Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное
образовательное учреждение высшего образования
«Уфимский государственный авиационный технический университет»

МАВЛЮТОВСКИЕ ЧТЕНИЯ

XV Всероссийская молодежная научная конференция

Том 4

Уфа 2021

Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное
образовательное учреждение высшего образования
«Уфимский государственный авиационный технический университет»

МАВЛЮТОВСКИЕ ЧТЕНИЯ

XV Всероссийская молодежная научная конференция

Том 4

Научное электронное издание сетевого доступа

ISBN 978-5-4221-1529-7
ISBN 978-5-4221-1533-4 (Т. 4)

Уфа 2021

Мавлютовские чтения : материалы XV Всероссийской молодежной научной конференции : в 7 томах [Электронный ресурс] / Уфимск. гос. авиац. техн. ун-т. – Уфа : УГАТУ, 2021.

Том 4. Уфимск. гос. авиац. техн. ун-т. – URL: https://www.ugatu.su/media/uploads/MainSite/Ob%20universitete/Izdateli/El_izd/2021-126.pdf

Содержатся статьи, включенные в программу XV Всероссийской молодежной научной конференции, состоявшейся в УГАТУ 26–28 октября 2021 г.

Организационный комитет конференции:

При подготовке электронного издания использовались следующие программные средства:

- Adobe Acrobat – текстовый редактор;
- Microsoft Word – текстовый редактор.

Материалы публикуются в авторской редакции

Ответственный за выпуск *Т. В. Разяпов*
Предпечатная подготовка *О. А. Соколова*
Программирование и компьютерный дизайн *О. М. Толкачёва*

Подписано к использованию: 19.10.2021
Объем: 27,01 Мб.

ФГБОУ ВО «Уфимский государственный авиационный технический университет»
450008, Уфа, ул. К. Маркса, 12.
Тел.: +7-908-35-05-007
e-mail: rik@ugatu.su

СЕКЦИЯ 5.1
АВТОМАТИЗИРОВАННЫЕ СИСТЕМЫ ОБРАБОТКИ ИНФОРМАЦИИ И УПРАВЛЕНИЯ

УДК 681.5

М. М. АКТУГАНОВА
aktuganovam@gmail.com
Науч. руководов. – зав. каф. АСУ, д-р техн. наук В. В. АНТОНОВ

Уфимский государственный авиационный технический университет

ОБУЧЕНИЕ ПОЛЬЗОВАТЕЛЕЙ КАК СПОСОБ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ ВНЕДРЕНИЯ СИСТЕМЫ SAP ERP

Аннотация. В данной статье описывается особая значимость обучения будущих пользователей новой системы, которая внедряется в рамках проекта. Ставится акцент на успехе внедрения системы при качественном обучении пользователей. Предлагается подход к обучению при внедрении системы SAP ERP. Обучение выделено в отдельный этап внедрения и представлены требования к обучению, которые позволят конечным пользователям понимать работу программы.
Ключевые слова: обучение; пользователь; успех внедрения; SAP ERP; стратегия обучения.

Введение

При внедрении любой системы пользователь не всегда готов к новым технологиям. При это зачастую руководители проектов не уделяют достаточного внимания обучению персонала и считают данную часть не столь значимой. Однако, успех внедрения системы во многом зависит и от того, насколько понятно была объяснена работа системы будущим пользователям и как быстро они найдут «общий язык» с ней на практике. Следовательно, необходимо организовать и провести качественное обучение персонала до того, как им придется непосредственно работать в новой внедренной системе, в противном случае вероятность ошибок и некорректной работы возрастает, что ведет к очевидным финансовым потерям.

SAP является довольно известным поставщиком программного обеспечения, дающим возможность предприятиям внедрять и включать ПО в свои бизнес-процессы. Данное действие позволит автоматизировать работу в компании путем соединения в единое целое всех процессов и подразделений.

SAP ERP – самый известный продукт компании, позволяющий объединить процессы производства, финансов, закупок, кадров и сбыта продукции предприятия. Система SAP ERP состоит из отдельных модулей, что позволяет использовать как отдельные компоненты системы, так и их различные комбинации.

Система SAP ERP является достаточно сложным для понимания продуктом, поэтому на ее обучение требуется немного больше времени, чем, например, на всеми известную 1С: ERP.

Основной задачей любого проекта является его успех. Для того, чтобы повысить вероятность успеха, необходимо правильно обучить пользователей.

Актуальность данной проблемы обосновывается тем, как повысить эффективность внедрения SAP ERP с целью реинжиниринга.

Представление о внедрении

Системы SAP позволяют выполнять конфигурацию системы абсолютно с всеми потребностями заказчика. Компании приобретают подобные готовые к использованию системы, как SAP вследствие того, что эти программные продукты способны настраиваться с любыми требованиями компании и обладают достаточной гибкостью для данных операций.

По статистике 80% реинжиниринга предприятий оборачивается неудачей, а внедрение ERP-систем – 50%. Причин данного следствия достаточно много: проектирование системы ERP без учета стратегии развития компании, проектирование системы ERP "снизу-вверх", избыточный реинжиниринг бизнес-процессов, неверная оценка экономической эффективности внедрения ERP-системы.

Довольно часто после внедрения корпоративной информационной системы пользователи компании недовольны качеством программ, а руководство, анализируя трудозатраты подчиненных, не обнаруживают сокращение времени на выполнение рутинных операций. Помимоэтого сохраняются все недостатки, которые были в ранее сложившейся практике осуществления производственной

деятельности предприятия. Нередко спроектированная ERP-система настолько сложна, что будущие пользователи системы не готовы к работе с такой многозадачной программой. На этот факт я бы хотела обратить внимание.

В процессе реинжиниринга в компании происходит масса изменений, к которым бывает сложно быть готовым. Особенно, при внедрении новой системы у пользователей возникают проблемы с пониманием работы программного обеспечения, что в дальнейшем сказывается на настроении сотрудников и эффективности их работы. SAP ERP-система не является «элементарной» программой, доступной для восприятия любому пользователю, возникают проблемы с ее «принятием», ведь не так много людей, готовых к изучению и познанию нового. Для того, чтобы избежать данную проблему предлагается уделить особое внимание к подходу внедрения системы SAP ERP.

Внедрение SAP ERP происходит в 5 этапов: подготовка проекта, разработка концептуального бизнес-проекта, на основании которых строятся в дальнейшем все бизнес-процессы, реализация и проведение технических работ, окончательная подготовка системы к промышленной эксплуатации, запуск и поддержка.

Необходимо вынести в отдельный этап внедрения системы SAP ERP - обучение пользователей (таблица 1).

Таблица 1

Этапы внедрения SAP ERP

№	*Название этапа*	*Описание*
1	Подготовка проекта	Разработка различных планов: календарный, план коммуникационных связей и управления рисками и др.
2	Разработка концептуального бизнес-проекта	Разработка проекта эффективных концепций, на основании которых строятся в дальнейшем все бизнес-процессы
3	Реализация	Проведение технических работ, которые включают в себя продуктивный старт системы и интеграционный тест.
4	Окончательная подготовка	Подготовка системы к промышленной эксплуатации. Решение исключительных ситуации и устранение нестыковок.

Окончание табл. 1

5	Обучение и тестирование	Проведение обучения пользователей в тестовой системе совместно со специалистами поддержки, тестирование на реальных данных.
6	Запуск и поддержка	Проверка готовности системы к запуску, устранение возможных проблемы. Запуск. Осуществление поддержки пользователей консультантами SAP, устранение ранее скрытых ошибок и несоответствий в системе.

SAP ERP-система вносит значительные изменения в уже существующие на предприятии бизнес-процессы, и сотрудникам приходится выполнять помимо своих основные обязанности, функции, "навязанные" новой системой. Поэтому очень важно руководству подготовить персонал.

Насколько будет успешно внедрение системы во многом зависит от заранее продуманной политики обучения персонала. Комплекс ERP-систем -- эффективно эксплуатировать может только хорошо обученный и замотивированный персонал. Одной из задач обучения является то, чтобы сотрудники увидели систему как полезный инструмент.

Ниже представлены требования в обучении пользователей:

1. Создание одного информационного пространства, чтобы разъяснить всем сотрудникам цели, которые преследует предприятие при внедрении информационной системы;

2. Выделение ключевой группы пользователей и осуществление их постоянной коммуникации с проектной командой;

3. Обучение конечных пользователей на реальных данных в тестовой системе;

4. Проведение практических заданий в нестандартных ситуациях.

Поскольку обучение выделено в отдельный этап внедрения, то на него затрачивается больше времени и соответственно увеличивается период внедрения системы. Если обычно внедрение может занять от 1 до 3 лет, то в данном случае вместо привычного обучения в 1 месяц, необходимо выделять минимум 4

месяца, чтобы пользователи смогли протестировать всевозможные случаи работы системы.

Для того, чтобы обучение было действенным, необходимо проводить промежуточную проверку практических знаний, полученных пользователями. После изучения блока или раздела системы, необходимо давать пользователям практические задания, затем снова закреплять тот же теоретический материал. Таким образом эффективность обучения возрастает за счет повторения материала после практического использования, так как у пользователей возникают дополнительные вопросы, ответы на которые они могут получить после практики.

Результаты

В результате исследования выявлено, что проект, уделивший внимание обучению персонала не столкнулся с проблемой пользователей при работе системы после запуска в промышленную эксплуатацию. Пользователи были готовы к работе, выполняли свои прямые обязанности, обращались к поддержке меньшее количество раз, чем другие компании, что можно увидеть на рисунке 1.

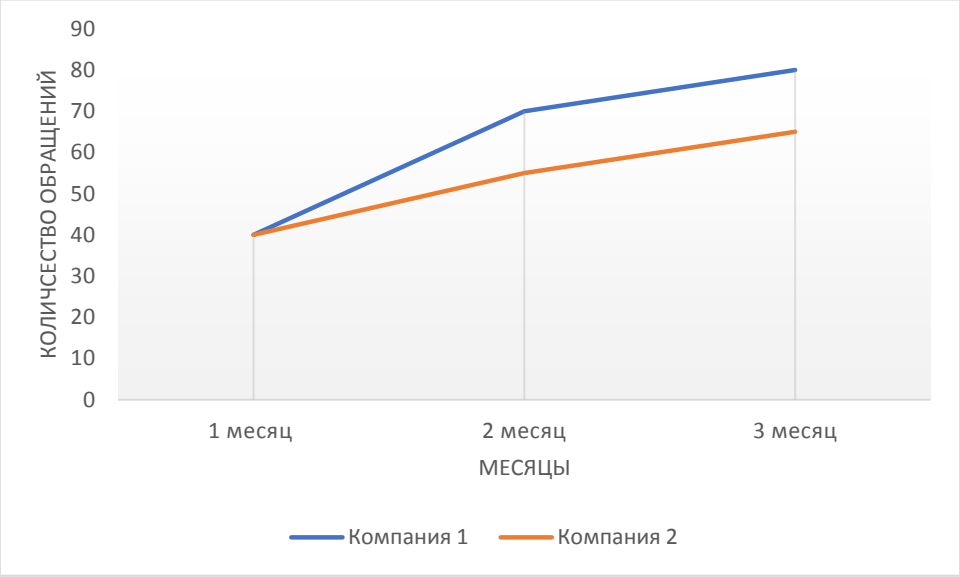


Рис. 1. Количество обращений в поддержку после внедрения системы

Компания 1 использовала старый подход в обучении персонала, Компания 2 использовала новый метод, уделив особое внимание обучению сотрудников. Количество обращений в службу поддержки пользователей от Компании 2 в первые месяцы после внедрения системы и запуска меньше, чем у Компании

1 так как пользователи обращались с вопросами не по работе в системе, а по работе самой системы.

На рисунке 2 показана разница в причинах неудачного внедрения двух компаний, которые возникли после запуска системы.

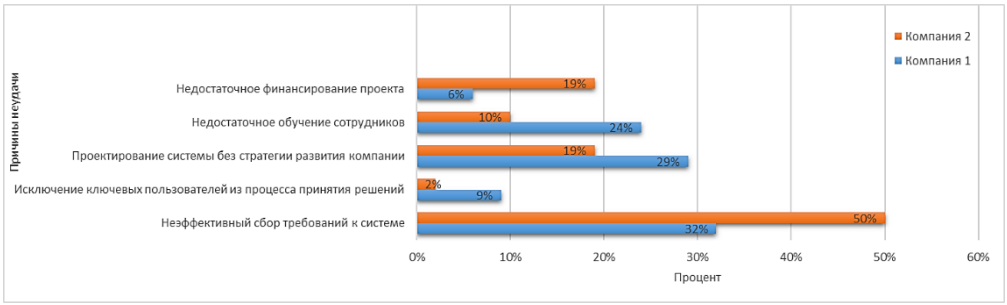


Рис. 2. Причины неудачного запуска

Значительно заметно уменьшение процента с 24% до 10% по причине «Недостаточное обучение сотрудников».

Выводы

SAP — это одна из лучших ERP-систем на рынке. Она обладает прогрессивным дизайном, который позволяет сочетать масштабность и гибкость. Для того, чтобы внедрение данной системы было более эффективным, необходимо включить в этапы внедрения обучение персонала, объяснить логику работы системы, повысить качество знаний сотрудников, благодаря чему свести к минимуму ошибки пользователей, в результате которых могут возникать финансовые потери компании.

В результате исследования описан подход к обучению пользователей новой системе на этапе внедрения – необходимо увеличить период обучения пользователей, выделив данный этап как самостоятельный, а также разработать стратегию обучения, в которой пользователи поэтапно знакомятся с определенным разделом системы и проходят тестирование у консультантов поддержки системы. Приведены сравнительные результаты успеха двух проектов компаний, эффективность внедрения которых отлична по пункту «обучение пользователей». Можно сделать вывод о том, что подход к качественному обучению чрезвычайно важен и влияние на результат проекта не следует недооценивать.

СПИСОК ЛИТЕРАТУРЫ

1. Джесутасан Р., Будро Дж. Реинжиниринг бизнеса. Москва: «Альпина Паблишер», 2019. 278 с.
2. Хаммер М., Чампи Д. Реинжиниринг корпорации. Манифест революции в бизнесе. Москва: «Манн, Иванов и Фербер», 2011. 288 с.
3. Колин К.К. Информационная культура в информационном обществе //Открытое образование. 2006. № 6. С. 50-57.
4. Павлюк А.К., Меркушева Н.И., Применение реинжиниринга бизнес-процессов на предприятиях // Молодой ученый. 2015. №1. С. 265-267.
5. Григорьев В.К., Аксенов О.А. Модель системы обучения кадров большой территориально-распределенной корпорации//Труды ТГТУ. 2002. С. 81-85.
6. Обучение персонала фирм в бизнес-школах: проблемы и реалии// Управление персоналом. 2001. № 5. С.16-21.
7. Норенков И.П. Синтез индивидуальных маршрутов обучения в онтологических обучающих системах // Информационные технологии. 2009. № 3. С. 74.
8. Rahman A.A, Abdullah M., Alias S.H. The architecture of agent-based intelligent tutoring system for the learning of software engineering function point metrics // 2nd International Symposium on Agent, Multi-Agent Systems and Robotics. 2016. P. 139-144.
9. Рожков, И.В. Информационные системы и технологии в маркетинге. Москва: «Русайнс», 2017. 320 с.
10. Краус М. Измерительные информационные системы. Москва: «Мир», 2016. 310 с.
11. Сенкевич Г. Е., Информационная система малого предприятия "с нуля". Самое необходимое. Москва: «БХВ-Петербург», 2016. 400 с.
12. Мезенцев К. Н. Автоматизированные информационные системы. Москва: «Академия», 2016. 176 с.
13. Шёнталер, Ф. Бизнес-процессы. Языки моделирования, методы, инструменты / Ф. Шёнталер. - М.: Альпина Паблишер, 2019. 264 с.
14. Gharaibeh N., Soud S.A. Software development methodology for building intelligent decision support systems // Doctoral Consortium on Software and Data Technologies. 2008. P. 3-14.
15. Макарычев П. П., Денисова И. Ю. Информационные обучающие системы. Пенза: «ПГУ», 2008. 160 с.
16. Markin S., Sinha A. SAP Integrated Business Planning Functionality and Implementation. Quincy: «Rheinwerk Publishing Incorporated», 2018. 504 P.
17. Ефремова Л.И., Курганов А.Н. Методологические подходы к совершенствованию бизнес-процессов предприятия // Системное управление. 2016. № 2 (31). С. 3-5.
18. Евдокимова А.Б., Ильин И.В. Реинжиниринг бизнес-процессов в организации как инструмент антикризисного управления // Научно-технические ведомости СПбГПУ. Экономические науки. 2016. № 3 (245). С. 15-21.

УДК 004.057.5

М. И. БЕЛОВ, А. Д. МЕРКИН, Е. Ю. КИРШИНА
belov.maksim.i@yandex.ru, arsen.merkin@gmail.com, kirshina.elena.yu@yandex.ru
Науч. руководитель – ст. преп. О. В. КОНДРАТЬЕВА

Уфимский государственный авиационный технический университет

РАЗРАБОТКА МОБИЛЬНОГО ПРИЛОЖЕНИЯ ДЛЯ АЛГОРИТМИЧЕСКОЙ ТОРГОВЛИ НА ФОНДОВОЙ БИРЖЕ

***Аннотация*.** Рассмотрен проект создания симулятора алгоритмического трейдинга в форме приложения на фреймворке *ReactNative*.
***Ключевые слова*:** мобильная разработка; разработка приложений; *ReactNative*; фондовая биржа

Стремительное развитие технологий позволяет совершенствовать наши гаджеты, делая их меньше, легче, мощнее и полезнее. Уже сейчас мобильные устройства едва уступают по характеристикам персональным компьютерам и ноутбукам. Каждый год выходят новые изобретения, которые становятся все мощнее и совершеннее. Сейчас невозможно представить учебу, работу и просто повседневную жизнь без мобильных телефонов.

Используя мобильные технологии, появляется возможность управлять своим банковским счетом, производить онлайн оплату услуг или, используя технологию NFC, оплачивать покупки в магазинах, отслеживать расписание и местонахождение транспорта и т.д.

Многие брокерские компании стремятся автоматизировать процесс торговли на фондовой бирже, используя для этого различные инструменты для программирования. Самые распространенные оперативные системы для мобильных устройств это *Android* и *IOS*.

В статье рассматривается разработка мобильного приложения, с помощью которого пользователь может симулировать торговлю на бирже, используя алгоритмы для автоматизации покупки и продажи акций.

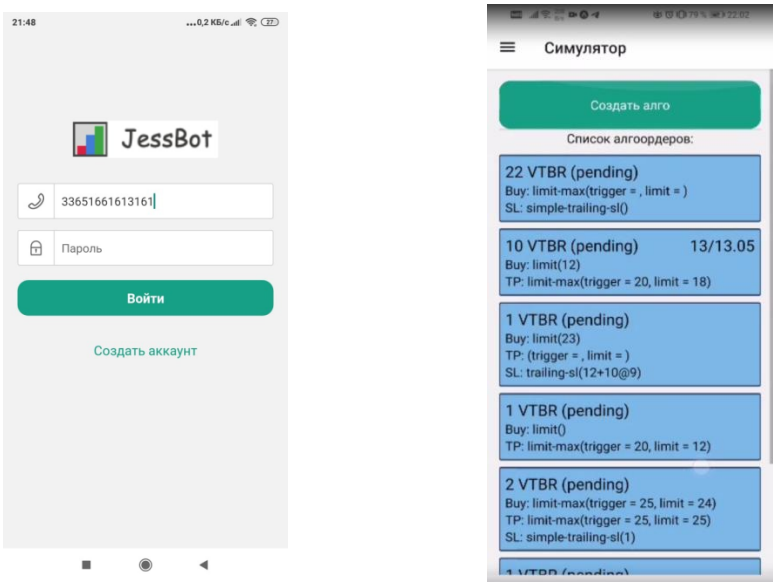
Мобильное приложение разрабатывалось для компании *JessBot* [1], которая хотела автоматизировать процесс торговли на фондовой бирже, а существующее решение в виде сайта не позволяло это делать.

Приложение создавалось с помощью *JavaScript* с фреймворком *ReactNative* [2]. Выбор пал на данный инструмент, так как он позволяет создавать кроссплатформенные приложения, которые работают на операционных системах *Android* и *IOS*.

При разработке были учтены современные тенденции дизайна и технического оснащения мобильных приложений с учетом индивидуального дизайна компании.

В ходе работы над мобильным приложением было сделано "окно авторизации" при первом запуске приложения, в котором пользователь может зарегистрировать новую учетную запись или войти в уже существующую. Главное окно отображено в соответствии с рисунком 1 (а).

В соответствии с рисунком 1 (б) отображено окно списка алго-ордеров (готовых алгоритмов), в которое пользователь попадает после авторизации. Здесь он может просмотреть свои раннее созданные алго-ордера или создать новые. Создание новых алго-ордеров показано в соответствии с рисунком 2.

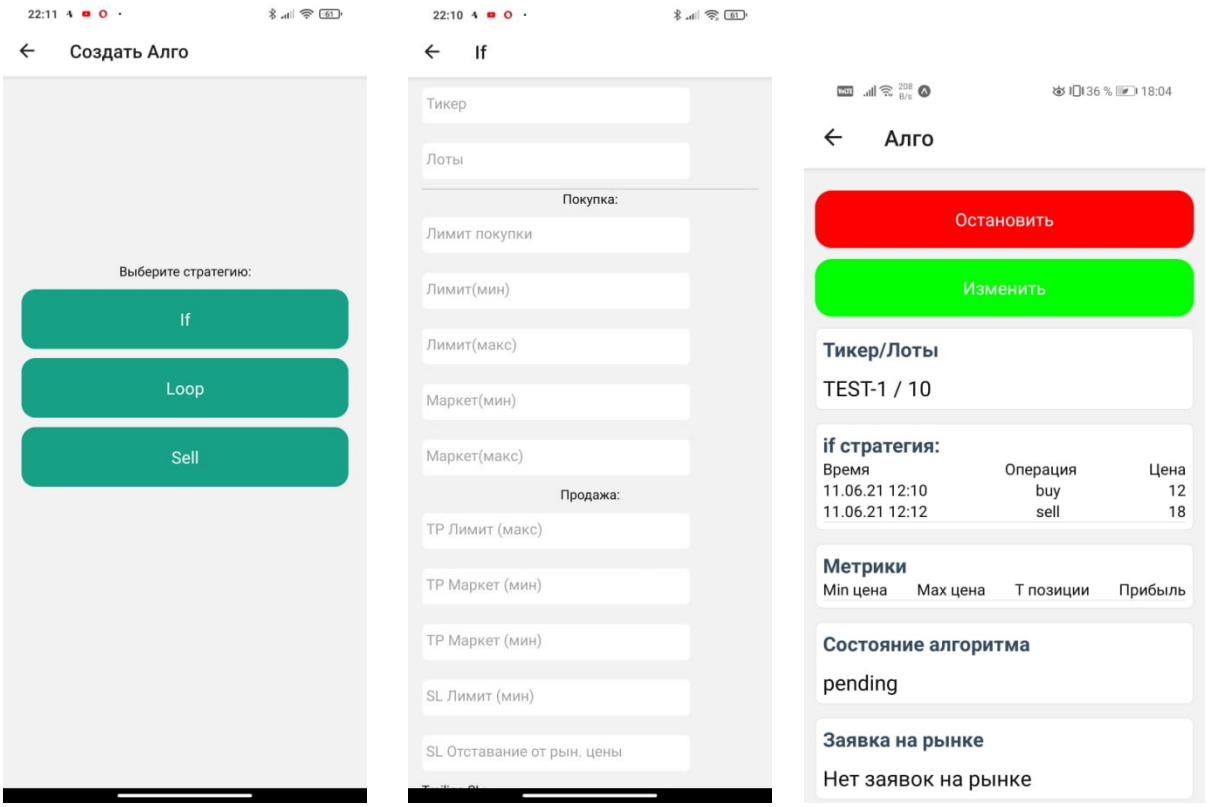


а *б*

Рис. 1. Окна мобильного приложения *JessBot*:
а – окно авторизации; б – главное окно

При создании новых алго-ордеров необходимо выбрать стратегию торговли (варианты стратегии представлены в соответствии с рисунком 2 (а)). При выборе той или иной стратегии пользователь попадает в настройки алгоритма торговли, где может задать минимальные и максимальные значения, при которых система будет продавать или покупать ту или иную валюту/акцию. Окно настроек алгоритма показан в соответствии с рисунком 2 (б).

После задания желаемого алгоритма пользователь возвращается в окно со списком готовых алго-ордеров и может следить за ходом их работы. При желании пользователь может изменить ордер. Нажав на него, он попадет в окно изменения алго-ордера (рисунок 2 (в))



а *б* *в*

Рис. 2. Создание алго-ордера:
а – выбор стратегии; б – настройки стратегии; в – изменение стратегии

Плюсом такого мобильного приложения является то, что пользователь может задать алгоритм его работы и не следить за движениями графиков и тенденций. Программа будет всегда соблюдать заданный алгоритм работы и мгновенно реагировать на изменения на рынке [3].

Такие приложения уже показали свою эффективность и все передовые компании по торговле на фондовой бирже переходят на мобильные приложения, чтобы позволить своим пользователям в любой момент времени отследить свой алгоритм, изменить его или создать новый.

В ходе разработки мобильного приложения для компании *JessBot* были получены навыки работы с *JavaScript* и с фреймворком *ReactNative* для создания кроссплатформенного приложения. Весь функционал работы сайта компании был перенесен в мобильное приложение и протестирован. В ходе тестирования было выявлено, что приложение работает корректно.

СПИСОК ЛИТЕРАТУРЫ

1. JessBot (сайт). URL: https://jess-bot.ru/docs/ (дата обращения 13.06.2021).
2. Что такое биржевой робот: принцип работы, виды, плюсы и минусы, то 5 лучших (сайт). URL: https://greedisgood.one/robot-dlya-torgovli-na-birzhe (дата обращения 27.07.2021).
3. Руководство по React Native для начинающих Android-разработчиков (сайт). URL: https://habr.com/ru/company/plarium/blog/458118/ (дата обращения 27.07.2021).

УДК 543.27

Э. Ф. ВАЛИЕВА[1], В. И. САФАРОВА[2], Р. М. ХАТМУЛЛИНА[2]
[1] ***Башкирский государственный университет***
[2] ***ГБУ РБ УГАК***

Науч. руководитель – д-р хим. наук, проф. В. И. САФАРОВА
ГБУ РБ УГАК

ПРИМЕНЕНИЕ АВТОМАТИЗИРОВАННЫХ СИСТЕМ МОНИТОРИНГА АТМОСФЕРНОГО ВОЗДУХА ПРИ АВАРИЙНЫХ СИТУАЦИЯХ

Аннотация. В статье приводятся результаты контроля атмосферного воздуха с помощью автоматизированных систем мониторинга при аварийной ситуации, связанной с разливом газового конденсата. Представлены результаты определения сероводорода и серосодержащих органических соединений в атмосферном воздухе.
Ключевые слова: автоматические системы контроля; передвижная экологическая лаборатория; газоанализатор; атмосферный воздух; аварийные и чрезвычайные ситуации.

Важнейшим объектом окружающей среды является атмосферный воздух, загрязнение которого приводит к серьезным экологическим проблемам и представляет серьезную угрозу для здоровья населения.

Поступление загрязняющих веществ в атмосферный воздух происходит не только при штатном режиме работы предприятий, но и при аварийных и других нештатных ситуациях. Часто возникают ситуации, связанные с разливом нефтепродуктов, приводящие к поступлению в окружающую среду токсичных соединений серы (диоксид серы, сероводород, сульфиды, меркаптаны и др.)

Так как воздушная среда представляет собой динамичную систему, где перемешивание и рассеивание веществ происходит за достаточно короткий промежуток времени, то необходимы методы, позволяющие в режиме «on-line» определять концентрации примесей. Поэтому в условиях нештатных ситуаций одним из наиболее оптимальных решений является внедрение автоматических систем контроля с применением современных технических и программных средств, позволяющих осуществлять анализ на месте расположения источника загрязнения [1, 2]. Одним из вариантов автоматизированного контроля компонентов окружающей среды, в частности атмосферного воздуха, являются передвижные экологические лаборатории (ПЭЛКАВ), оснащенные газоанализато-

рами различного принципа действия. Эти лаборатории могут осуществлять как выполнение определенных задач, так и проводить оценку состояния окружающей среды в целом.

В данной статье представлены результаты анализа проб атмосферного воздуха, загрязненного серосодержащими компонентами в результате поступления газового конденсата в окружающую среду. Анализ воздуха осуществлялся на ПЭЛКАВ непрерывно в дневное и ночное время. Для измерения сероводорода применялся газоанализатор флуоресцентного принципа действия с принудительным отбором пробы с помощью встроенного побудителя расхода. Принцип работы прибора основан на окислении сероводорода до диоксида серы, с последующей регистрацией характерного излучения диоксида серы в диапазоне длин волн 220-240 нм.

В ходе мониторинга атмосферного воздуха в поставарийный период было установлено, что содержание сероводорода в атмосферном воздухе в разное время суток превышало предельно допустимые концентрации (ПДК). В некоторых случаях уровень загрязненности воздуха соответствовал высокому и экстремально высокому. При этом максимальное превышение концентрации сероводорода зафиксировано в ночное время. Только использование для контроля атмосферного воздуха в зоне загрязнения автоматических средств измерений позволило оперативно за максимально короткий промежуток времени получить информацию, на основании которой были приняты природоохранные и другие меры. Таким образом, применение автоматизированных систем мониторинга атмосферного воздуха является чрезвычайно важным в условиях возникновения аварийных ситуаций. Так, передвижные экологические лаборатории позволяют в режиме реального времени обследовать территории, подверженные загрязнению и выявить наиболее загрязненные участки. Кроме того, использование средств измерений непрерывного действия дает возможность оперативно связать получаемые данные с метеорологическими параметрами, такими как скорость и направление ветра, температура воздуха, влажность, что является

немаловажным, так как от этих параметров зависит накопление и дальнейшее распространение загрязненных воздушных масс.

СПИСОК ЛИТЕРАТУРЫ

1. Москвин А.Л., Хромов-Борисов С.Н. / Внелабораторный химический анализ (Проблемы аналитической химии. Т. 13). Под ред. Золотова Ю.А. М.: Наука, С. 47.
2. Разяпов А.З. Проблемы аналитической химии. Т. 13. Внелабораторный химический анализ. Под ред. Золотова Ю.А. М.: Наука, 2010. С. 470.

УДК 004.9

А. И. ВАХИТОВА
vahitova98@bk.ru
Науч. руководов. – канд. техн. наук, доц. Т. К. ГИНДУЛЛИНА

Уфимский государственный авиационный технический университет

ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИЙ «ИНДУСТРИИ 4.0» В ПРОВЕДЕНИИ ПРОФОРИЕНТАЦИИ ШКОЛЬНИКОВ

Аннотация. Статья посвящена проблеме проведении профориентации школьников. Рассматриваются ключевые компоненты цифровой трансформации промышленного производства в контексте Индустрии 4.0 и как они могут помочь будущим выпускникам с определением будущей профессии. В частности, рассматриваются технологии, используемые в рекламе, как возможность узнать увлечения пользователя системы для составления общей картины интересов. Также доказывается мысль об необходимости использования новейших технологий обзором принадлежности школьников к поколению зумеров.
***Ключевые слова*:** профориентация; школьник; индустрия 4.0; теория поколений; цифровые технологии; тестирование.

Проведение профориентации с получением эффективного результата задача не из легких. При использовании обычных тестов можно получить определенные выводы, но не будет полной картины. Как дополнение необходимо также проведение беседы с психологом. Но в таком случае возникает проблема в нехватке специалистов для каждого пользователя, так как программа должна быть рассчитана как минимум для всех выпускников региона. В данном случае необходимо использовать что-то, что позволит помочь каждому, например современные информационные технологии.

Основным материалом исследования будет та часть общества для кого необходима система профориентационных работ – будущие абитуриенты ВУЗов и ССУЗов. Для понимания как она должна быть построена необходимо изучить характерные особенности данной группы. В данную категорию попадают люди, родившиеся в 2004 и в последующие годы. Исходя из адаптированной для России американской теории поколений, можно сделать вывод, что мы имеем дело с поколением Z (рожденные 2000–2011 гг.) и всем известный факт, что такие дети «рождаются со смартфоном в руках».

Необходимо выделить важные особенности для этого поколения:

– для них не существует шаблонов и ограничений, принципов и устойчивых взглядов

– некоторые из них уже пытались открыть свой бизнес.

– в воспитании принимают участие не только родители, но, и различные блогеры из YouTube, Tik Tok, Instagram

– привычного для прошлого поколения детства с друзьями во дворе, у них нет.

Для поколения Z уже с самого рождения общение с компьютером происходит «на ты». Имена Маруся, Алиса, Олег они ассоциируют не с какими-то конкретными людьми (приятелями, друзьями), а с более знакомыми для них роботами-помощниками. А ведь такой инструмент как голосовой помощник может помочь решить некоторые вопросы, связанные с проблемой проведения тестирования среди будущих абитуриентов.

Человечество живет во время бурного развития информационных и коммуникационных технологий, вследствие чего часто сталкивается с изменениями и в обычной жизни. Все эти изменение связанные с широким распространением всемирной сети Интернет вызванные четвертой промышленной революцией. Индустрия 4.0, начавшая во второй половине двадцатого века, вызвала новые явления и процессы – цифровизацию и цифровую экономику, что находит отражение в изменении промышленности.

В Индустрии 4.0 основными направлениями выделяют:

– Аддитивное производство;

– Большие данные, облачные вычисления;

– Виртуальная реальность;

– Искусственный интеллект.

Последний пункт особенно выделяют как одно из самых перспективных направлений цифровых технологий

Революция не обошла стороной и сферу образования. Во многих школах привычные для всех бумажные дневники уже потеряли свою актуальность, так как идет переход на электронные. Также никого не удивишь тестирующими программами. Большое влияние цифровых технологий на процесс обучения весь мир прочувствовал, столкнувшись с пандемией в 2020 году. Как ученикам младших классов, так и преподавателям с высоким стажем работы выпал шанс опробовать возможности компьютерных технологий. Даже после того, как все постепенно вернулись на учебу в офлайн режиме, задания для проверки знаний, которые проверяет компьютер, не потеряли своей актуальности.

Возникает вопрос: необходим ли искусственный интеллект для проведения профориентации школьников. Ведь, казалось бы, в таком нелегком вопросе как выбор будущей профессии, вряд ли может помочь бездушный робот.

Такое явление, как реклама в Интернете, появилось не так давно, но при этом используемые технологии имеют высокий темп в усовершенствовании. Многие пользователи сети замечают, что получают рекламу того, в чем заинтересованы. Происходит ощущение, что кто-то подслушивает за человеком и специально высылает то, что ему надо. Если этот феномен рассматривать простым взглядом, то да – за нами следят, но происходит это намного сложнее. Здесь используется инструмент ремаркетинга. Из справочного раздела Google можно узнать, что он способствует в воспроизведении нужной рекламы тем, кто уже посещал сайт или пользовался приложением. Пользователи могут получить рекламное объявление при просмотре иных сайтов, или по запросам схожих товаров.

Дело в том, что мы оставляем «цифровой след». «Цифровой след» – это совокупность информации, размещаемой пользователем о себе в сети Интернет. Т. е. когда люди оставляют комментарии под фотографиями звезд, делают заказ в интернет-магазинах, заводят страницу в социальной сети, указывая персональные данные (имя, фамилия, дата рождения, номер телефона, место работы и т. д.), то не задумываясь вносят в интернет крупицы информации. Но если

это как-то можно контролировать, например, уменьшить активность во всемирной сети, то феномен «цифровая тень» обыграть не получится. «Цифровая тень» – информация, которая накапливается неявно: маршруты передвижений, видеозаписи камер наблюдений и т. д. Сбор информации продолжается и тогда, когда мы не взаимодействуем с телефоном. Наш гаджет сам подключается к роутерам заведений и организаций, встречающихся на пути.

Такие технологии нас пугают. Но в современном мире мы имеем один выход – успокоиться и свыкнуться с мыслью, что это норма для жизни в цифровой эпохе.

Для чего нужен сбор информации? Ответ прост: для того, чтобы угодить покупателям. Ведь главная задача рекламы – помочь в выборе. Каждый сайт, который мы посещаем, создает небольшие текстовые документы, в которых записываются наши действия. Эти документы называются cookies. Затем все это собирается на веб-сервер. Алгоритмы машинного обучения анализируют собранные материалы и выдает рекламу, которая вероятнее всего заинтересует пользователя.

Почему бы данную способность роботов не использовать и для проведения профориентации? С помощью cookie-файлов можно собрать информацию о школьнике в течение определенного времени. Затем также с помощью машинного алгоритма выявить его интересы и предпочтения.

Плюсами такой системы будут следующие:

– при прохождении теста школьник может задуматься и дать ошибочный ответ, но в случае, когда используется подобная система, вероятность ошибки уменьшается;

– система рассчитана на большое количество пользователей;

– система имеет меньше затрат для результата;

– система использует больше информации.

Но в такой системе есть и минусы:

– как и в случае с рекламой, может произойти утечка информации из-за злоумышленников;

– есть вероятность использования интересов не только тестируемого, но и членов семьи или того, кто также пользуется роутером;

– для анализа нужна выборка, собранная за большое количество времени.

Как же тогда будет работать система? Школьники будут как можно раньше получать свой личный кабинет. Далее система будет собирать cookie-файлы. Также пользователь системы должен будет проходить несколько видов тестирования на профориентацию. После сбора всей информации система начнет подбирать специальности. Вдобавок в некоторых случаях будет использоваться помощь экспертов. Как результата ученики школ получат специальный набор, который включает: профессии, которые наиболее подходят; учебные заведения, в которых можно получить необходимое образование; список предметов, которые изучается в определенном учебном заведении; список дополнительных курсов; олимпиады. Хорошим дополнением будет ролик от каждого предложенного учебного заведения, в котором будет рассказываться об направлении подготовки от трех лиц: преподавателя, студента, выпускника. Это все необходимо для того, чтобы будущий абитуриент мог наглядно представить результаты теста. Все это будет находиться на портале электронного образования Республики Башкортостан (Рис. 1).

Рис. 1. Модель системы профориентации

Предлагаемая модель имеет множество преимуществ. Но так ли она хороша в использовании? Если попытаться систематизировать все действия, то

можно обойтись без использования информационных систем, сам школьник может без тестов и помощи от взрослых выбрать нужную специальность. В таком случае не стоит забывать, что существует множество направлений и даже в рамках Уфимских университетов специальности с одинаковыми названиями имеют разные учебные планы. Так, не имеющий полного представления абитуриент может запутаться и выбрать неверный путь. Система же поможет и подберет именно нужный ВУЗ (ССУЗ), кроме того предложит ту специальность, которая не была рассмотрена из-за непонятного наименования.

Таким образом в ходе исследования была построена модель проведения профориентации, которая включает в себя привычные виды анкетирования и тестирования. Вдобавок была рассмотрена технология, используемая в рекламах, которая поможет дополнить общую картину внутреннего мира выпускника, от чего выбор профессионального пути будет наиболее точной. Следовательно, появиться специалист, который ценит свою работу. В свою очередь если он окончил учебное заведение на бюджетном месте, то государственное финансирование получит положительный результат.

СПИСОК ЛИТЕРАТУРЫ

1. Бояркина Л.А. Бояркин В.В. Цифровой след и цифровая тень как производные персональных данных [Электронный ресурс] // Сборники конференций ниц социосфера. 2016. № 62.
2. Дугар-Жабон Т. З., Симакина М. А. Таргетинг и ретаргетинг как инструменты маркетинга // Научные труды Московского гуманитарного университета. 2019. № 4.
3. Зверева Екатерина Анатольевна Особенности медиапотребления "поколения Y" и "поколения Z" // Социально-гуманитарные знания. 2018. №8.
4. Московченко В.М., Столяров Д.О., Горбунов А.А., Белянин В.И. Анализ технологий защиты от идентификации веб-браузеров // NBI-technologies. 2018. №1.
5. Шишкунова В.А. Теория поколения: понятие и характеристика // Актуальные проблемы авиации и космонавтики. 2017. №13.

УДК 004.9

Э. Ю. ГИБАДУЛЛИНА
Gibadullia.elina@inbox.ru
Науч. руководв. – канд. техн. наук, доц. Т. К. ГИНДУЛЛИНА

Уфимский государственный авиационный технический университет

К ВОПРОСУ ИСПОЛЬЗОВАНИЯ ПО BIZAGI MODELER В ПРОЦЕССЕ ИССЛЕДОВАНИЯ ПРЕДМЕТНОЙ ОБЛАСТИ

Аннотация. В статье рассматривается то, как происходит изучение предметной области с помощью Bizagi Modeler, инструмента для графического описания процессов в нотации BPMN 2.0. Описано, что такое модель, для чего ее необходимо изучать и как это делается с помощью моделирования. Также в статье отражены преимущества Bizagi и нотации BPMN.
***Ключевые слова*:** изучение предметной области; Bizagi Modeler; модель; моделирование бизнес-процессов; бизнес-процесс; BPMN-модель; имитационное моделирование.

Введение

Актуальность темы обусловлена тем, что изучение предметной области является неотъемлемым этапом проектирования информационных систем (ИС), а также их сопровождение. Одним из методов изучения предметной области является процесс создания модели предметной области, анализируя которую возможно определить требования к ИС в соответствии с информационными потребностями пользователя.

Для получения соответствующего предметной области проекта ИС в виде системы правильно работающих программ, необходимо иметь целостное, системное представление модели, которое отражает все аспекты функционирования будущей информационной системы. Предварительное моделирование предметной области позволяет сократить время и сроки проведения проектировочных работ и получить более эффективный и качественный проект.

Основная часть

Предметная область – это часть реального мира, которая подлежит изучению. Также можно сказать, что предметная область определяет совокупность объектов (предметов), свойства и отношения которых представляют интерес для разработчиков и пользователей будущей системы.

Предметной областью в данной статье будет пониматься часть реального мира, рассматриваемая в пределах процесса (бизнес-процесса) «Участие в олимпиаде». Конкретнее изучению подлежит процесс «Подготовка к олимпиаде».

Моделирование - процесс создания формализованного описания системы, предполагающий представление различных характеристик поведения физической или абстрактной системы см помощь другой системы.

Моделирование бизнес-процессов. При анализе существующего и разработке нового бизнеса важную роль играет построение моделей компании и протекающих в ней бизнес-процессов. Модели могут различаться степенью детализации процессов, формой их представления, учетом только статических или также динамических факторов и др. Следует отметить, что все известные подходы к моделированию бизнеса принадлежат к семейству методов моделирования сложных информационных систем.

Case (Computer Aided Software Engineering) технологии - совокупность методов проектирования систем, а также набор инструментальных средств, позволяющих в наглядной форме моделировать предметную область. Case-технологии реализуются при помощи Case-средств. Примеры Case-средств: ARIS, IBM Rational Rose, IBM WebSphere Business Modeler, Bizagi.

В данной статье для моделирования процесса будет рассмотрена система Bizagi - это BPM-система, разработанная одноименной компанией, и направленная на моделирование, исполнение, автоматизацию и анализ бизнес-процессов.

BPMN (Business Process Model and Notation) - «Нотация и модель бизнес-процессов» - нотация для моделирования бизнес-процессов, включающая систему условных обозначений и их описание в XML.

Модель отображает процесс подготовки студента к олимпиаде с помощью либо преподавателя, либо репетитора на курсах. С помощью Bizagi разработана простейшая модель процесса (рис. 1).

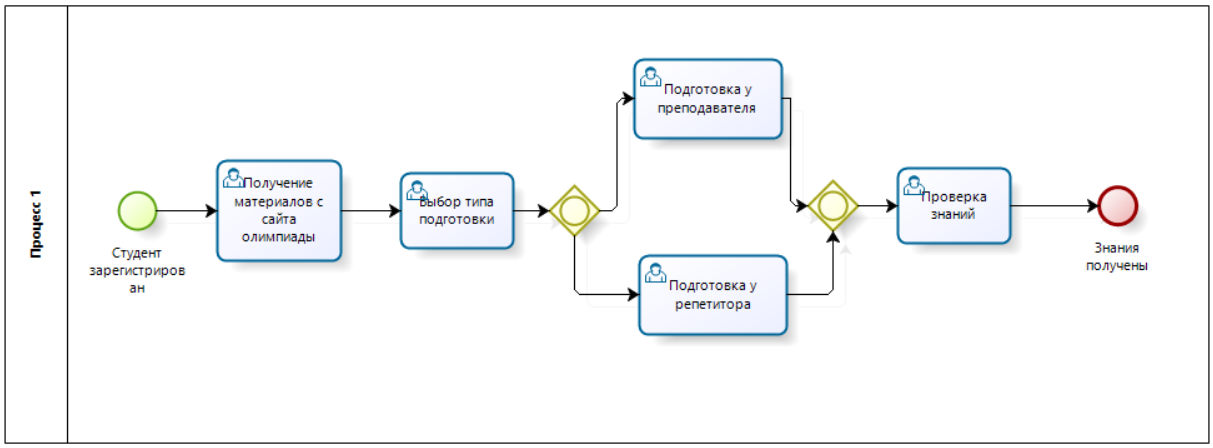


Рис. 1. Простейшая модель процесса

Описание простейшей модели

Начальное событие «Студент зарегистрирован» и конечное событие «Необходимые знания получены». Задачи процесса: «Получение материалов с сайта олимпиады», «Выбор типа подготовки», «Подготовка у преподавателя», «Подготовка у репетитора», «Проверка знаний».

В модели задачи связаны потоками операций, а логику их взаимодействия демонстрируется при помощи шлюзов. Студент получает задания с сайта олимпиады, далее выбирает вид подготовки. Он может заниматься у преподавателя или у репетитора. Либо вообще посещать оба вида занятий, поэтому был выбран шлюз «И/ИЛИ» для разветвления и слияния потоков операций.

Далее модель усложняется при помощи добавления дополнительных элементов. Происходит преобразование задач «Подготовка у преподавателя» и «Подготовка у репетитора» в подпроцессы (локальный процесс в терминологии IBM). Подпроцессы показаны на рис. 2-3.

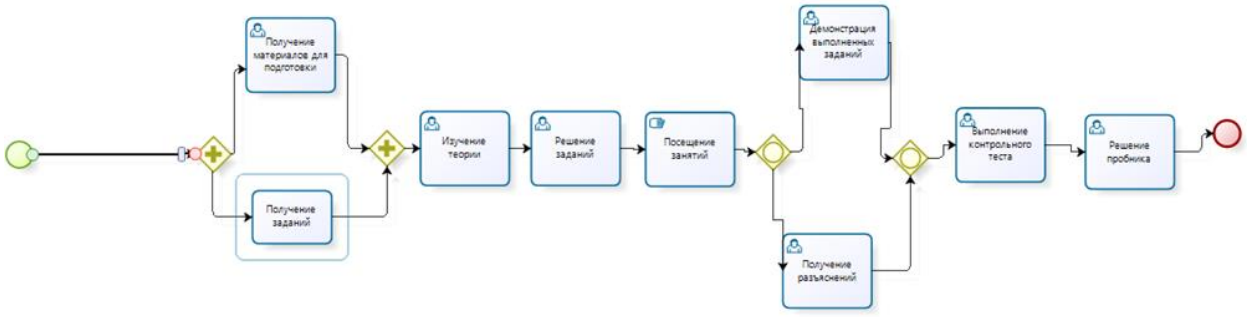


Рис. 2. Подпроцесс «Подготовка у преподавателя»

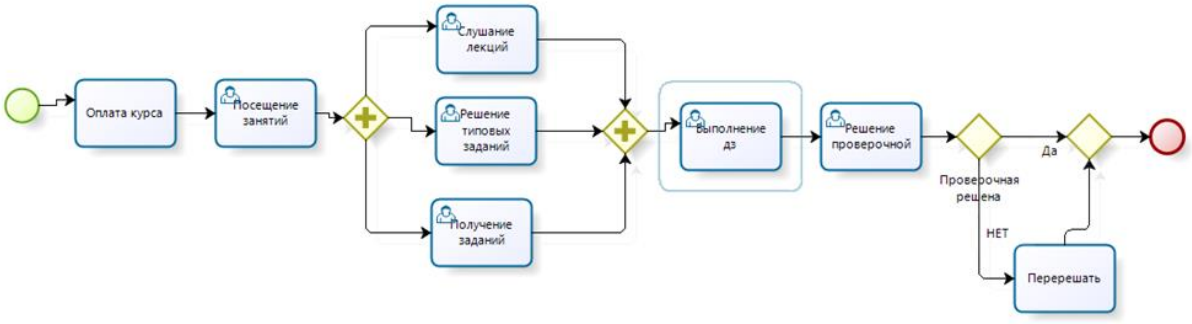


Рис. 3. Подпроцесс «Подготовка у репетитора»

Благодаря Bizagi есть возможность создания вложенных процессов. В процессе принимают участие некоторое количество исполнителей: Студент-участник, Преподаватель и т.д. Чтобы изучить предметную область в Bizagi есть возможность создания и добавления Дорожек. После добавления дорожек, вложенных процессов получаем готовую модель предметной области (рис.4)

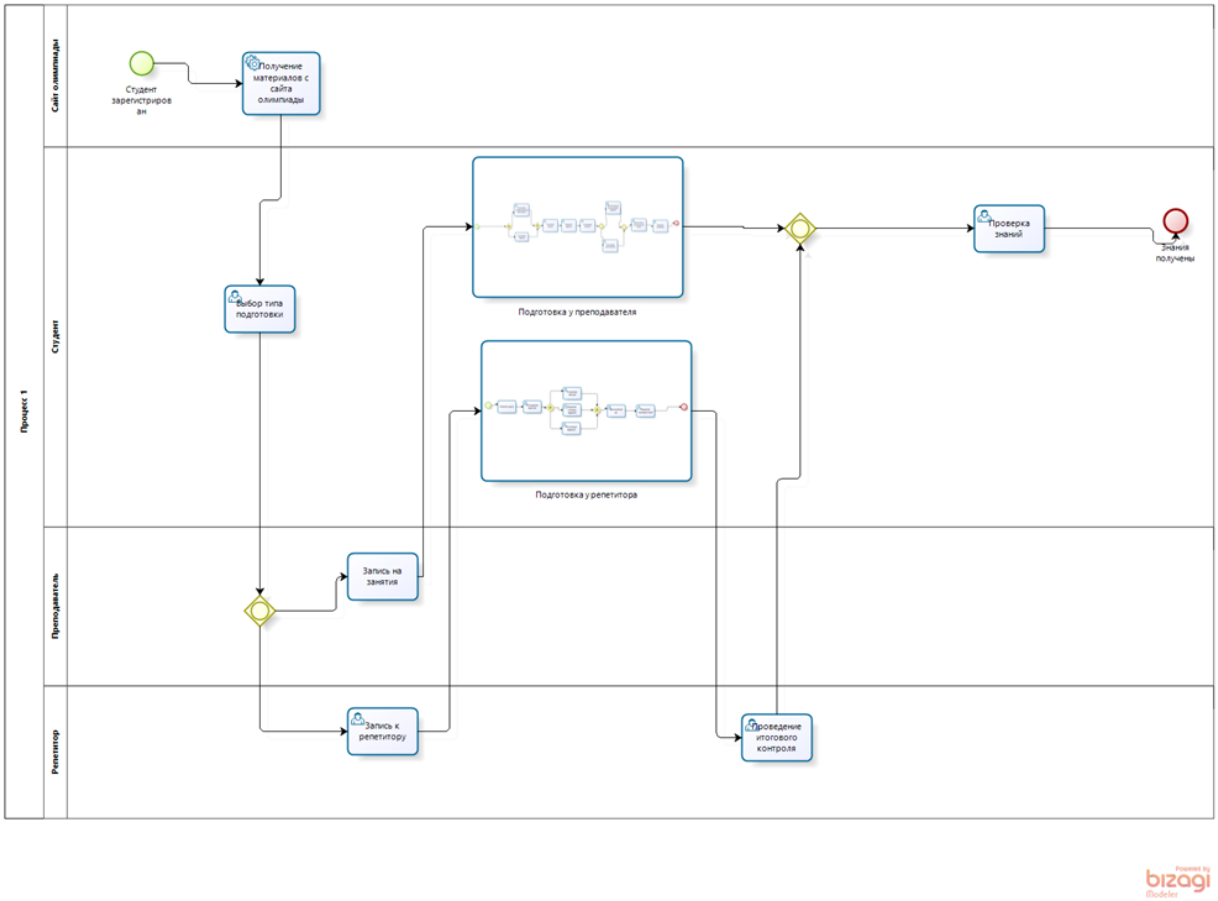


Рис. 4. Готовая модель процесса

Такие диаграммы бизнес-процессов помогают читателям быстро понимать процесс и легко ориентироваться в его логике, что способствует лучшему

изучению предметной области. С помощью Дорожек демонстрируется, кто выполняет ту или иную задачу, что упрощает понимание процесса. Вложенные процессы показывают два сценария развития событий, при которых Студент-участник выбирает способ подготовки к Олимпиаде.

Имитационное моделирование

Имитационное моделирование — один из наиболее эффективных методов оптимизации процессов, который позволяет спроектировать процесс и проанализировать его работу до того, как процесс будет опубликован или передан в разработку.

Bizagi Modeler позволяет выполнить имитационное моделирование (или, так называемую, симуляцию) процесса, в ходе которого есть возможность провести временной и стоимостной анализ бизнес-процесса.

Временной анализ позволяет увидеть время обработки запущенных процессов, представленное как минимум, максимум, среднее значение и сумма (общее время обработки). Аналогичные результаты могут быть представлены для отдельных задач.

Для выполнения симуляции процесса необходимо задать общие параметры сценария имитации во вкладке Properties. Так в рассматриваемом примере, общая длительность процесса назначена 30 дней, денежные единицы USD. Для данного сценария на стартовом событии количество запускаемых процессов равно 100 (Допускается, что подготовку проходят 100 студентов). Для шлюзов определяются возможные варианты отклонения. Далее было задано время выполнения каждой отдельной задачи модели бизнес-процесса (настройка типа параметра, примеры: Duration - Время в формате - сколько дней, часов, минут, секунд);

В процессе имитации процесса симулятор отображал, какое количество экземпляров процесса прошло через каждую операцию, сколько было затрачено временных ресурсов в среднем и в целом (рис.5-6).

Имитация прошла успешна, количество запущенных процессов соответствует количеству завершенных. Общее время запуска сценария - 4497 дней, 6 часов, 27 минут, 11 секунд.

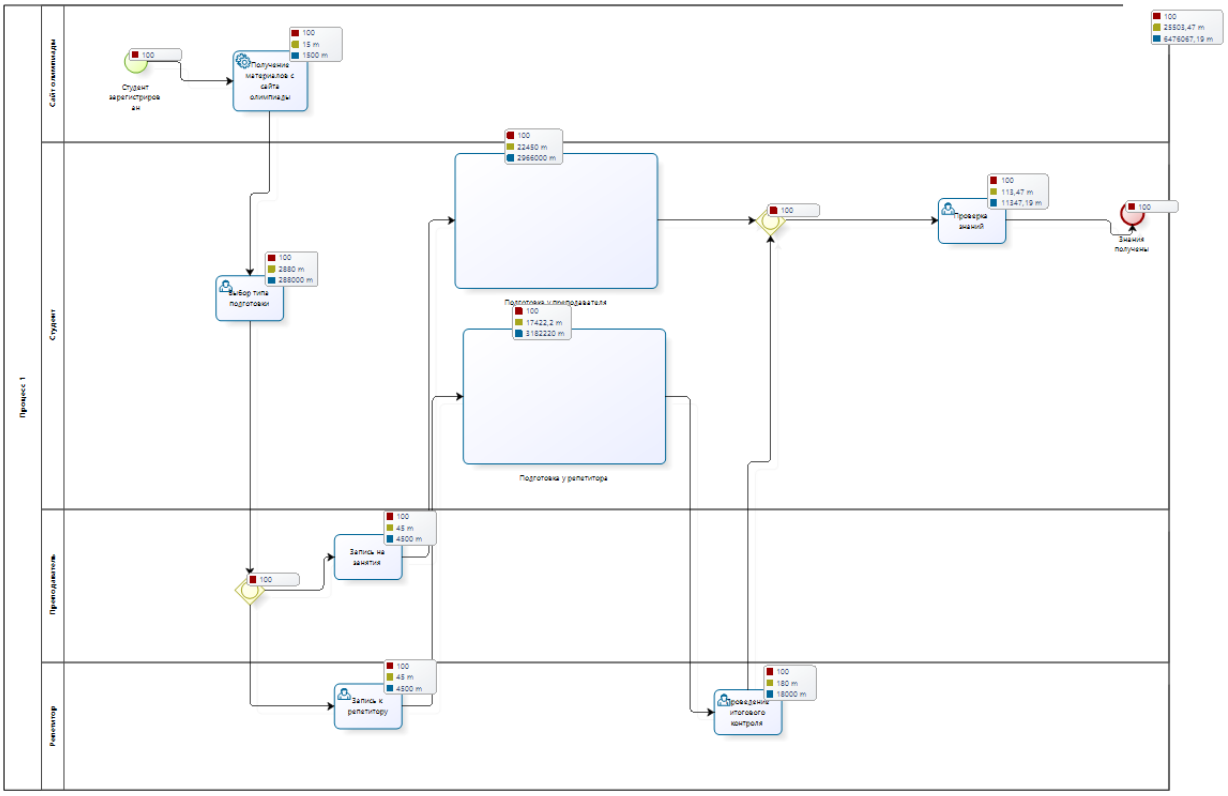


Рис. 5. Имитация процесса на втором уровне (Time Analysis)

Name	Type	Instances completed	Instances started	Min. time	Max. time	Avg. time	Total time
Процесс 1	Process	100	100	17d 16h 10m 40s	17d 18h 9m 58s	17d 17h 3m 28s	4497d 6h 27m 11s
Выбор типа подготовки	Task	100	100	2d	2d	2d	200d
Знания получены	End event	100					
Подготовка у репетитора	Process	100	100	12d 2h	12d 3h	12d 2h 22m 12s	2209d 21h
Подготовка у преподавателя	Process	100	100	15d 14h 10m	15d 14h 10m	15d 14h 10m	2059d 17h 20m
InclusiveGateway	Gateway	100	100				
Проверка знаний	Task	100	100	1h 40s	2h 59m 58s	1h 53m 28s	7d 21h 7m 11s
Проведение итогового контроля	Task	100	100	3h	3h	3h	12d 12h
Студент зарегистрирован	Start event	100					
Запись на занятия	Task	100	100	45m	45m	45m	3d 3h
InclusiveGateway	Gateway	100	100				
Запись к репетитору	Task	100	100	45m	45m	45m	3d 3h
Получение материалов с сайта олимпиады	Task	100	100	15m	15m	15m	1d 1h

Рис. 6. Результат имитации

What-If-Analysis в Bizagi предлагает создание всевозможных сценариев имитационного моделирования с уникальными настройками для анализа процесса при заданных условиях. Используя различные сценарии, существует возможность проводить реалистичный анализ процессов, не подвергая риску, например, свою бизнес-деятельность.

Преимущества использования Bizagi Modeler

BPMN позволяет при моделировании бизнес-процессов опускать на определенном уровне те или иные реальные процессы. Так, в нашем случае мы оставляем «за скобками» Регистрацию студента. Благодаря чему изучению и анализу подлежит только процесс «Подготовка к олимпиаде».

В Bizagi Modeler есть возможность декомпозиции, поддержка нотации моделирования бизнес-процессов, проверка построения нотаций, возможность групповой работы в приложении.

Заключение

В результате проделанной работы были изучены такие понятия, как: предметная область, модель, моделирование бизнес-процессов, а также изучена предметная область «Участие в олимпиаде» - процесс «Подготовка к олимпиаде» с использованием Bizagi. Определены преимущества данной системы и нотации BPMN.

СПИСОК ЛИТЕРАТУРЫ

1. Кравченко, А. В. Моделирование бизнес-процессов : учебное пособие / А. В. Кравченко, Е. В. Драгунова, Ю. В. Кириллов. — Новосибирск : НГТУ, 2020. — 136 с. — ISBN 978-5-7782-4159-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/152364 (дата обращения: 28.09.2021). — Режим доступа: для авториз. пользователей.
2. Business Process Modeling Notation Specification / Графический язык моделирования бизнес-процессов BPMN : спецификация (избранные главы)/ EleWise, 2006-2009. - 121 с.
3. Зуева, А. Н. Моделирование бизнес-процессов в нотации BPMN 2.0 : учебное пособие / А. Н. Зуева. — Москва : РТУ МИРЭА, 2021. — 105 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/176564 (дата обращения: 28.09.2021). — Режим доступа: для авториз. пользователей.
4. Зуева, А. Н. Бизнес-процессы: анализ, моделирование, управление : учебное пособие / А. Н. Зуева. — Москва : РТУ МИРЭА, 2020. — ISBN 978-5-7339-1550-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/163874 (дата обращения: 28.09.2021). — Режим доступа: для авториз. пользователей. — С. 69.
5. Яблочников, Е.И., Молочник, В.И., Фомина, Ю.Н. Реинжиниринг бизнес-процессов проектирования и производства [Электронный ресурс]: Учебное пособие. - СПб: СПбГУ ИТМО, 2008. - 152 с. Загл. с экрана. - Режим доступа: http://window.edu.ru

УДК 5.1

К. С. ГУРОВА
gurova2067@yandex.ru
Науч. руководв. – канд. техн. наук, проф. А. М. СУЛЕЙМАНОВА

Уфимский государственный авиационный технический университет

АНАЛИЗ ДАННЫХ НА ПРОИЗВОДСТВЕ С ПОМОЩЬЮ НЕЙРОННЫХ СЕТЕЙ

Аннотация. В данной статье речь идет об актуальности использования нейронных сетей, и о применении метода использования нейронных сетей с долгой краткосрочной памятью в сфере бюджетирования. В статье приведено описание принципа работы данной сети и процесс обучения нейронной сети. Также в данной статье говорится о результатах, которые будут достигнуты после обучения нейронных сети с долгой краткосрочной памятью.
***Ключевые слова*:** анализ; данные; информация; метод; нейрон; нейронная сеть; обучение; подход.

Введение

На сегодняшний день развитие различных сфер жизни человека связано с накоплением и обработкой полученных данных, которые содержат очень важную информацию. Для хранения такой информации требуются хранилища, способные вмещать большие объемы данных. Таким образом, сначала появилась потребность в технологии, которая позволит анализировать, хранить и обрабатывать огромное количество данных.

Целью исследования является повышение эффективности анализа большого массива данных в сфере бюджетирования.

Для достижения цели были решены следующие задачи:

1. Формирование обучающего набора данных
2. Разработка модели нейронной сети для анализа данных и их прогнозирования
3. Проведение обучения нейронной сети
4. Сравнение показателей точности анализа до и после применения метода

Материалы и методы

С помощью искусственного интеллекта решается такие задачи, как принятие решений, теория игр, обучение нейросетей и т.д [5]. В рамках данной диссертации рассматривается метод обучения нейронных сетей. Учитывая объемы данных в сфере бюджетирования, возникают трудности с принятием управленческих решений. Целью данной работы является обучение нейросети для работы с данными в сфере бюджетирования.

Объектом исследования являются нейронные сети.

Предметом исследования является разработка методов использования нейронных сетей с долгой краткосрочной памятью для принятия управленческих решений в сфере бюджетирования. Новизна этого подхода заключается в том, что данный метод будет использован для анализа и прогнозирования бюджетирования Республики Башкортостан.

Нейронная сеть — это последовательность нейронов, соединенных между собой синапсами. Структура нейронной сети в программировании была заимствована из биологии[1]. Данная структура позволяет машине анализировать и даже запоминать различную информацию[4]. Также это дает возможность нейросетям воспроизводить информацию из своей памяти.

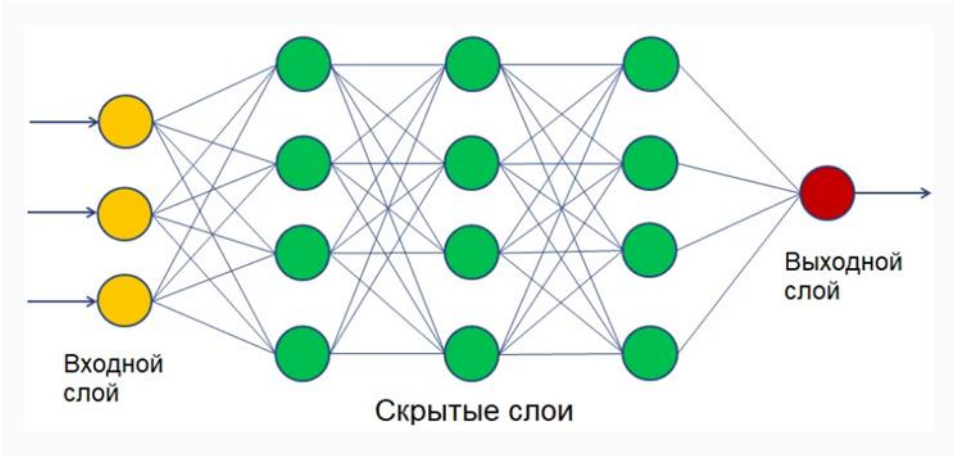


Рис. 1. Графическое представление нейронной сети

Основной принцип нейронной сети с долгой краткосрочной памятью заключается в том, что входной элемент определяет, какая входная информация

будет использоваться для обновления информации и какую информацию можно добавить в долгосрочную память. Выходной элемент определяет содержание выходной информации в блоке памяти[3]. Также в сети присутствует элемент «забывания». Данный элемент определяет какую информацию необходимо удалить из блока, а какую оставить[7].

В данной статье рассматривается пример обучений нейронной сети для распределения ЦСР в бюджетном планировании на основе программных продуктов предприятия НПО «Криста».

ЦСР – целевая статья расходов. Данная статья добавляется в систему под определенным кодом и имеет принадлежность к определенному бюджету, поэтому для каждого региона Республики Башкортостан данные статьи добавляются по отдельности. Пример отображения ЦСР в системе представлен на рисунке 2.

04 0 01 02030	Глава муниципального образования
20 0 00 98210	Государственная поддержка на проведение капитального ремонта общего имущества в м
20 2 01 00000	Детские дошкольные учреждения
04 0 02 00000	Дополнительное профессиональное обучение муниципальных служащих
21 0 00 03150	Дорожное хозяйство
02 0 00 74000	Иные безвозмездные и безвозвратные перечисления
20 0 00 74000	Иные безвозмездные и безвозвратные перечисления
20 0 00 74040	Иные межбюджетные трансферты на финансирование мероприятий по благоустройству
21 0 00 74040	Иные межбюджетные трансферты на финансирование мероприятий по благоустройству
20 9 00 03560	Мероприятия в области коммунального хозяйства
20 9 00 00000	Мероприятия в области коммунального хозяйства
20 0 00 03560	Мероприятия в области коммунального хозяйства

Рис. 2. Коды ЦСР

Данные статьи в систему должны добавлять финансовые органы районов, но бывает так, что пользователи изначально заводят в систему не все необходимые ЦСР. И в дальнейшем, в ходе работы у пользователей возникает множество ошибок, например, в консолидации отчетности или при составлении бюджетных обязательств, так как система пытается сослаться на ЦСР, которая изначально не была заведена.

Предлагаемая нейронная сеть будет на начальном этапе анализировать необходимую информацию и сообщать пользователям, какие ЦСР им необходимо добавить именно на их бюджет.

Для примера, в программе Deductor была построена таблица где было выбрано 5 рандомных ЦСР и 5 рандомным регионов РБ. После обучения построенной нейронной сети с помощью карт Кохонена были получены изображения, на которых видно, какая ЦСР на бюджете какого района отсутствует. Данные изображения представлены на рисунке 3.

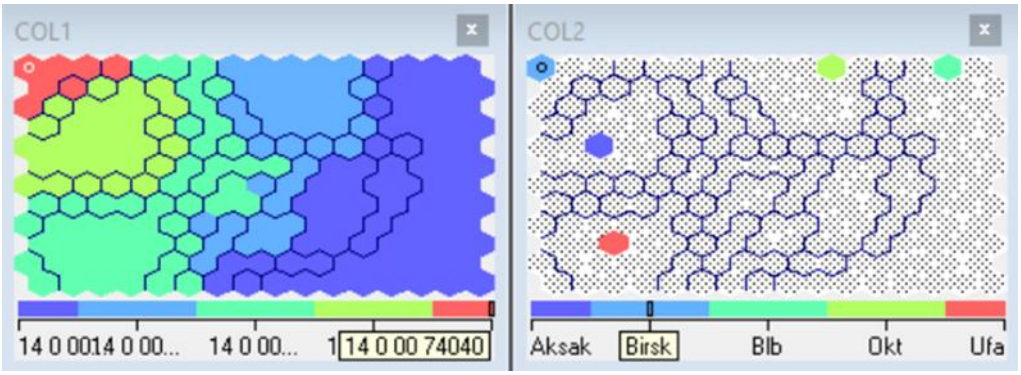


Рис. 3. Карты Кохонена

После обучения нейронная сеть будет способна обрабатывать новые данные по заданному алгоритму без участия человека.

Результаты и обсуждения

Благодаря данной нейросети сокращается время анализа данных. Устраняются ошибки, связанные с добавлением ЦСР. Данная нейросеть позволяет проводить анализ на всех уровнях иерархии от бюджета Республики Башкортостан до бюджетов муниципальных образований.

Выводы

Таким образом, в заключении можно сказать, что внедрений нейронных сетей на производство значительно облегчает процесс обработки информации, а также экономит временной и денежный ресурс. Данный метод удобен тем, что не требует глубоких знаний программирования для внедрения его на предприятии. Нейронная сеть может использоваться в любой сфере производства, помогая планировать и прогнозировать дальнейшую деятельность предприятия.

СПИСОК ЛИТЕРАТУРЫ

1. Айзерман М. А. Браверман Э. М., Розоноэр Л. И. Метод потенциальных функций в теории обучения машин: «Наука» 1970. 384с.
2. Бирюков А.Н. Нейросетевое моделирование в бюджетно-налоговой системе регионального и муниципального уровней: дис. … канд. техн. наук. Уфа 2012. 130 с.
3. Дюк В. А. Флегонтов А. В., Фомина И. К. Применение технологий интеллектуального анализа данных в естественнонаучных, технических и гуманитарных областях // Известия РГПУ им. А.И. Герцена. 2017. Том 9. №138. С. 77–84.
4. Ерофеева В.А. Обзор теории интеллектуального анализа данных на базе нейронных сетей: дис. … канд. тех. наук: 08.05.2021. Санкт-Петербург. 2018. 103 с.
5. Лабусов М. В. Нейорнные сетидолгой краткосрочной памяти и их использование для моделирования финансовых временных рядов// Инновации и инвестиции. 2020. Том 4. №3 С. 3-10.
6. Николаева Ю.В. Методы и алгоритмы интеллектуальной системы поддержки принятия решений трейдеров финансовых рынков: дис. … канд. техн. наук. 07.05.2021. Ижевск 2018. 127 с.
7. Кратович П.В. Нейросетевые модели для управления инвестициями в финансовые инструменты фондового рынка: дис. … канд. техн. наук. 08.05.2021. Тверь 2017. 165 с.
8. Тарик Р. Создаем нейронную сеть: «Вильямс» 2018. – 5-10 с.
9. Транкс Э. Глубокое обучение: «Библиотека программиста» 2019. – 4-9 с.
10. Ширяев В. И. Финансовые рынки. Нейронные сети, хаос и нелинейная динамика: «Либроком» 2009. 232 с.
11. Фаустова К. И. Нейронные сети: применение сегодня и перспективы развития// Территория науки. 2017. №4. С. 2-7.
12. Хайкин С. Нейронные сети: полный курс, 2-е издание: «Вильямс» 2008. 18с.
13. Schmidhuber J. Deep Learning in Neural Networks: «IDSIA» 2016. P. 85–87.
14. Nielsen M. Neural Networks and Deep Learning: «Scopus» 2019. P.13-16.
15. Simon O. Haykin Neural Networks and Learning Machines, 3rd Edition: «Scopus» 2018. P. 3-6

УДК 681.5

Э. Р. КАРИМОВ
eemcha@mail.ru
Науч. руководитель – канд. техн. наук, доц. Е. А. ДРОНЬ

Уфимский государственный авиационный технический университет

ВНЕДРЕНИЕ ИНФОРМАЦИОННОЙ СИСТЕМЫ ДЛЯ ХРАНЕНИЯ ДАННЫХ ПРОЕКТОВ ЭЛЕКТРОСНАБЖЕНИЯ

Аннотация. В статье выносится решение по выбору системы среди имеющихся на рынке готовых решений, которая обеспечит хранение сложной технической документации внутри отдела. В работе указано, что готовое решение необходимо доработать для конкретной работы по рассмотрению проектов электроснабжения. Для наглядности ожидаемых результатов был смоделирован бизнес-процесс в BPMN-нотации и приведены примеры экранных форм. В дальнейшем автор статьи рассчитывает внедрить данную систему на предприятие.
***Ключевые слова*:** электроэнергетика; техническая документация; электронный документооборот; хранение документов; поиск документов; регистрационная карточка.

Введение

Электроэнергетические предприятия в рамках своей деятельности используют проекты электроснабжения. Такие проекты содержат различные электронные чертежи линий передач, номера технических условий, информацию о договорах, а также техническую документацию о замечаниях и проверки документов. Речь пойдет о процессе рассмотрения и согласования проектов электроснабжения.

В рамках фирмы из области электроэнергетики подобные проекты передаются из одного отдела в другой при помощи различных систем электронного документооборота (СЭД). Данные проектов вносятся в систему, а после рассмотрения и результат проверки. Однако, электроэнергетика – специфическая область. Хранение данных проектов электроснабжения зачастую не предусмотрено настройками СЭД. Выходом в таком случае, например, может служить хранение самих данных проекта в другой системе и обращаться к ним при необходимости.

Сотрудникам отдела, занимающимся согласованием проектов электроснабжения, приходится проделывать двойную работу при проверке проектной документации, т.к. СЭД, выполняющая функции хранения и передачи техниче-

ской документации проектов, не позволяет сохранить все необходимые параметры данных проекта электроснабжения [9, 11]. Таким образом, данные проектов электроснабжения хранятся сразу в двух местах. Это неудобно как при сохранении данных проекта, так и с последующим его поиском.

Цель исследования: разработать проект системы, избавляющей от необходимости записи и хранения информации о проектах электроснабжения сразу в двух местах.

Задачами исследования являются: выбор готового решения, моделирование бизнес-процесса с учетом доработки, разработка эскиза экранных форм.

Основная часть

1. Анализ существующих решений

Когда люди обращаются в компании, предоставляющие услуги по передачи и распределению электрической энергии, они приносят с собой проекты электроснабжения, требующие согласования. Сотрудники компании перед согласованием занимаются рассмотрением и проверкой этих проектов. В случае нахождения ошибок, проект возвращается на доработку, а затем снова проверяется при повторном обращении клиента [2]. В этом случае удобно, если в отделе будут сохраняться данные этих проектов электроснабжения, т.к. при дальнейших проверках можно будет корректировать изменения, а не сохранять документацию заново.

Одним из методов решения проблемы хранения и поиска технической документации проектов электроснабжения может стать продукт «Directum».

«Directum» – эта система, в которой отличное реализовано управление цифровыми документами, а также их обработка и хранение. Благодаря технологии Workflow в данной системе электронного документооборота реализованы возможности согласования документов, а также обработка сложной технической документации. В «Directum» можно хранить документы в неструктурированном виде, а можно их структурировать и назначить права доступа к различным папкам и фалам. В системе присутствует возможность как полнотекстово-

го поиска документов, так и поиск по различным атрибутам. Хорошо реализованы процессы обработки документов, их согласования, а также функции контроля и взаимодействия между сотрудниками. Данная платформа хорошо обеспечивает надежность данных, а также позволяет обращаться к системе при помощи мобильных решений, например, устройства на операционных системах Andoid или iOS [4, 7]. Также «Directum» обладает отличной гибкостью и масштабируемостью системы, что позволит в дальнейшем без проблем расширить круг решаемых задач. Стоимость такого решения обойдется в 167200 рублей. Здесь учитываются и серверные, и клиентские лицензии.

Другим методом решения проблемы хранения и поиска технической документации проектов электроснабжения может стать продукт «1С:Документооборот» [8].

«1С:Документооборот 8» – отличная система, позволяющая организовать электронный документооборот. В системе отлично реализован контроль исполнения документов, что позволяет увидеть состояние документа, на котором он находится, например, согласован он или не согласован, утвержден или нет, уже исполнен или все еще на исполнении. Для того, чтобы удостовериться в целостности документа, есть поддержка электронной подписи. Усиленная электронная подпись, при необходимости, может использоваться для шифрования файла. В программе также отлично реализован поиск документов, что обеспечивает быстрый поиск даже при большом количестве документов в системе. В модуле поиска имеются возможности простого поиска, точного поиска и полнотекстового поиска, что позволяет искать документы и по индексам, и по реквизитам, и по содержанию самих файлов. Для быстрого сохранения файла в нужную папку или карточку в системе реализовано штрихкодирование документов. Это также обеспечивает распознавание и быстрый поиск документов по штрих-коду. Стоимость такого решения обойдется в 78000 рублей. Здесь учитываются только клиентские лицензии, так как лицензия на сервер уже имеется на предприятии.

Также методом решения проблемы хранения и поиска технической документации проектов электроснабжения может стать продукт «Docsvision». «Docsvision» – система электронного оборота с приятным интерфейсом. Данный продукт позволяет провести комплексную автоматизацию управления. Также в системе присутствуют специализированные отраслевые решения. Компания обеспечивает курсами для подготовки специалистов к работе в системе. В плане масштаба система универсальна, поэтому может подойти как для большого предприятия, так и для небольшого отдела внутри предприятия. В качестве особенности можно выделить то, что в систему можно также подключаться и с мобильных устройств. В «Docsvision» есть схожие готовые решения для промышленности, например, нефтегазовая промышленность, т.к. здесь тоже используется огромное количество технической документации с чертежами. Обеспечить структурированное хранение документации помогут инструменты архива, у которых есть функции сканирования и распознавания текста и штрихкодов. В системе можно вести реестр договоров, что обеспечивает быстрый доступ к нужному документу при поиске. Модуль управления документами позволяет проводить согласование документации, а также проводить контроль по выдаче и выполнению поручений. Стоимость такого решения обойдется в 154000 рублей. Здесь учитываются и серверные, и клиентские лицензии.

2. Материалы и методы

Для выполнения поставленной задачи был решено разработать регистрационную карточку в информационную систему (ИС) «1С:Документооборот» [3, 6]. В ней будут храниться данные проекта, ранее записываемые в Excel-документе. Это позволит не делать двойную работу при записи данных проекта электроснабжения в систему, а также ускорит поиск проекта в дальнейшем, т.к. все данные будут храниться в одной системе.

Для оценки результатов был выбран параметр «время». В условиях, когда за год через отдел проходит порядка 2000-3000 проектов, время сохранения и поиска данных проектов играет важную роль. Поэтому решение внедрения ре-

гистрационной карточки должно сократить временные затраты на регистрацию проекта внутри отдела и на дальнейший поиск данных проекта электроснабжения, а также повысить удобство работы с данными, так как теперь информация о проектах будет храниться в одном месте.

Для понимания и визуализации бизнес-процесса после внедрения регистрационной карточки было решено смоделировать его в нотации BPMN. Для того была выбрана программа Bizagi Modeler [1]. Эта программа позволяет строить модели, проводить их валидацию и симуляцию. Симуляция позволяет провести анализ процесса, времени и ресурсов, затраченные на процесс [5, 8]. В рамках симуляции программа позволяет выставить максимальный подсчет прибытия. Данный параметр, показывающий количество запускаемых итераций процесса во время симуляции, указывается на стартовом событии BPMN-модели. На рисунке 1 показано, что в рамках процесса было выставлено 100 итераций.

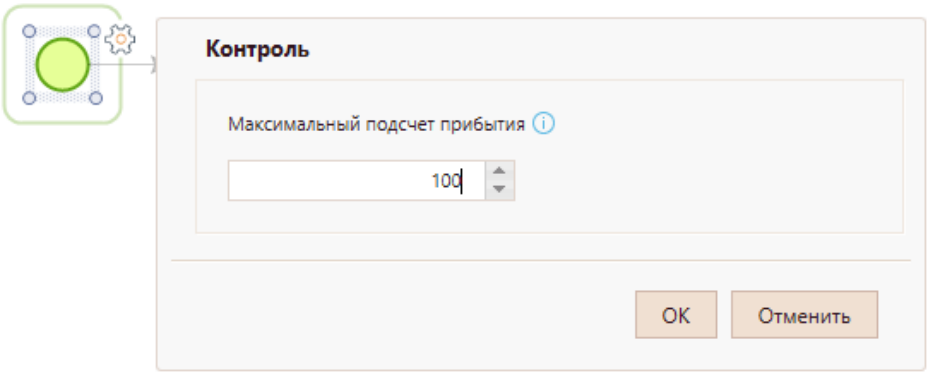


Рис. 1. Задание количества запускаемых процессов

Для сравнения на рисунке 2 представлена модель текущего процесса согласования проекта электроснабжения, а на рисунке 3 представлена модель предлагаемого процесса с учетом регистрационной карточки. В рамках данных моделей показывается, что начальник производственно-технического отдела (ПТО) получает проектную документацию для согласования, затем выдает сотрудникам указания по работе. В зависимости от типа проекта электроснабжения им занимаются либо ведущий инженер, либо инженер первой категории. После выполнения указаний, инженер отчитывается перед начальником в виде

отчета о выполнении работ, а также в текущем процессе переписывает данные проекта электроснабжения в Excel-документ, а в предлагаемом процессе фиксирует их в регистрационной карточке внутри системы. Далее начальник ПТО проводит проверку согласованности проекта и подписывает необходимую техническую документацию.

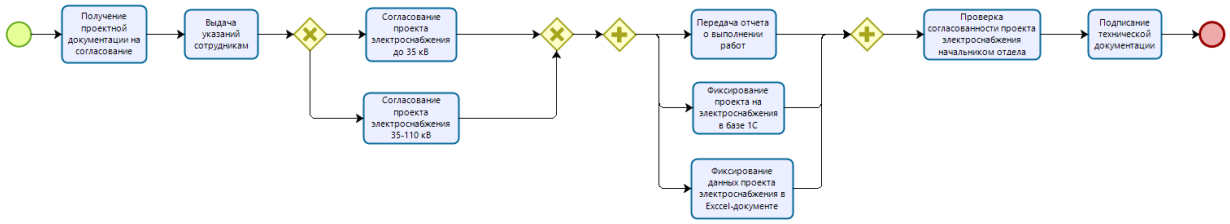


Рис. 2. Модель текущего процесса согласования проекта электроснабжения

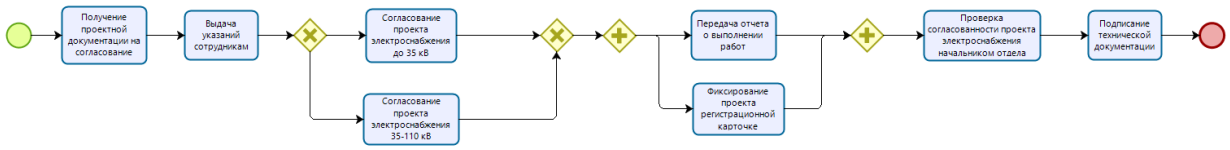


Рис. 3. Модель предлагаемого процесса согласования проекта электроснабжения

На рисунке 4 представлена модель текущего процесса поиска данных проекта электроснабжения, а на рисунке 5 представлена модель предлагаемого процесса с учетом регистрационной карточки.

В рамках текущего процесса показано, что для поиска данных проекта начальнику ПТО приходится искать данные проекта сначала в Excel-документе, а затем в базе 1С. На это уходит большое количество времени.

В рамках предполагаемого процесса показывается, как начальник ПТО, получивший запрос на поиск, производит его в регистрационной карточке. В сравнении с существующим процессом видно, что уменьшилось количество действий для поиска нужного проекта электроснабжения. Это сокращает как временные ресурсы, так и значительно повышает удобство самого процесса поиска. После того, как начальник производственно-технического отдела нашел

нужный проект, он подписывает необходимую техническую документацию, а затем отправляет всю эту документацию на утверждение главному инженеру.

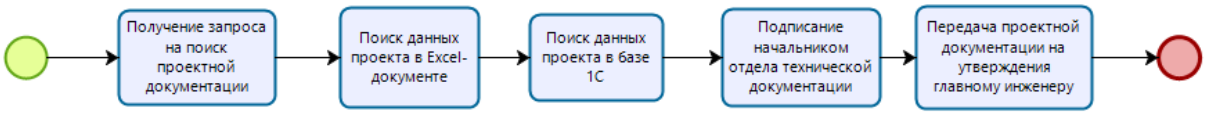


Рис. 4. Модель текущего процесса поиска проекта электроснабжения

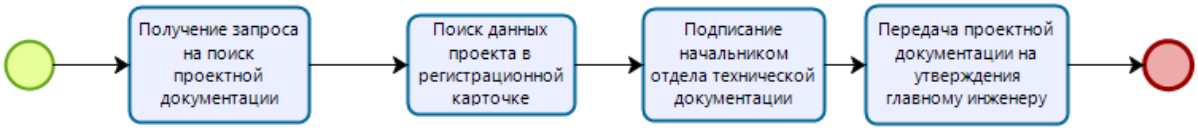


Рис. 5. Модель предлагаемого процесса поиска проекта электроснабжения

3. Результаты и обсуждения

Было проведено сравнение существующего процесса рассмотрения проекта и предлагаемого с использованием регистрационной карточки, путем симуляции на основе 100 итераций.

В таблице 1 представлен результат проведения симуляции.

Таблица 1

Результаты симуляции

	Тип	Существующий процесс	Предлагаемый процесс
Согласование проекта электроснабжения	Процесс	1 дн. 3 ч. 17 мин.	1 дн. 1 ч. 51 мин.
Поиск проекта электроснабжения	Процесс	1 ч. 19 мин.	14 мин.
Сравнение времени	–	1 дн. 4 ч. 36 мин.	1 дн. 2 ч. 5 мин.

На основе данных симуляции, представленных в таблице 1 можно сделать вывод о том, что время выполнения существующего процесса рассмотрения проекта превышает время выполнения предлагаемого процесса с использованием регистрационной карточки.

Для визуального представления готового результата были разработаны примеры экранных форм. На рисунке 6 представлен пример регистрационной

карточки. На нем видно, что в регистрационной карточке имеются записи, содержащие данные проектов электроснабжения.

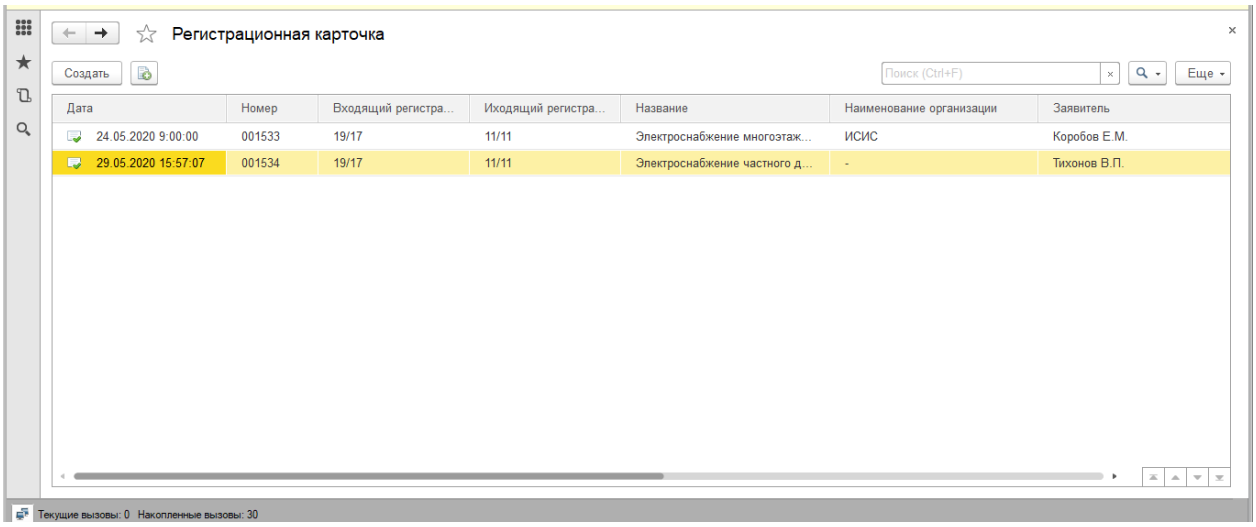


Рис. 6. Регистрационная карточка

На рисунке 7 представлен пример записи в регистрационной карточке. Он показывает данные проекта электроснабжения многоэтажного дома.

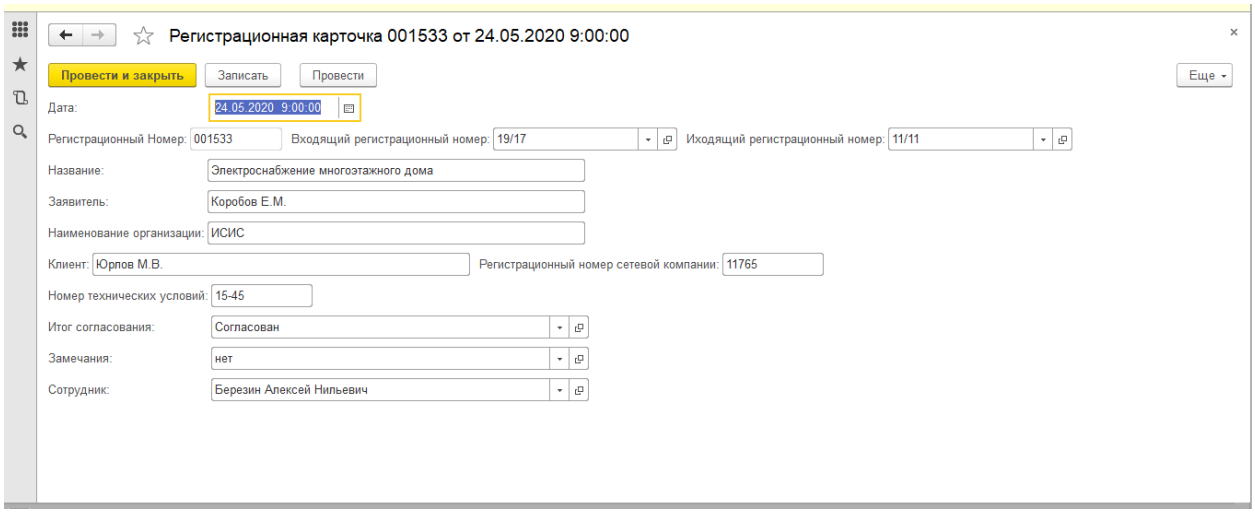


Рис. 7. Запись в регистрационной карточке

Выводы

Был проведен анализ программных решений, которые популярны на рынке и обладают хорошим функционалом. У некоторых готовых решений уже есть готовые шаблоны для электроэнергетической промышленности, у некоторых нужно дорабатывать имеющиеся шаблоны под свой процесс. По итогу бы-

ли определены методы для поставленной задачи исследования, а также определены их особенности и преимущества.

Был разработан проект информационной системы с регистрационной карточкой, которая позволяет хранить в себе различные параметры технической документации проектов электроснабжения. Результаты проекта были представлены в виде смоделированного бизнес-процесса и примеров экранных форм.

СПИСОК ЛИТЕРАТУРЫ

1. Александров Д.В. Инструментальные средства информационного менеджмента. CASE-технологии и распределенные информационные системы: Учебное пособие / Д.В. Александров. – М.: ФиС, 2017.
2. Варфоломеева, А.О. Информационные системы предприятия: Учебное пособие / А.О. Варфоломеева, А.В. Коряковский, В.П. Романов. – М.: НИЦ ИНФРА-М, 2018.
3. Гагарина, Л.Г. Автоматизированные информационные системы: учебное пособие / Л.Г. Гагарина. – М.: МИЭТ, 2016.
4. Большев В.Е., Виноградов А. В. Обзор зарубежных источников по применению информационных сетей в инфраструктуре интеллектуальных сетей // Вести высших учебных заведений Черноземья. 2019. Т. 55. № 1. С. 8-18.
5. Исаев Е.А., Первухин Д.В., Рытиков Г.О., Филюгина Е.К., Айрапетян Д.А. Оценка эффективности информационных систем с учетом рисков // Бизнес-информатика. 2021. №1. С. 19-29.
6. Абдулаева А.Д., Гашимова Л.Г. Особенности реинжиниринга бизнес-процессов на современных предприятиях // РППЭ. 2019. №5 (103). С. 143-148.
7. Kuzlu M., Pipattanasomporn M., Rahman S. Communication network requirements for applications in HAN, NAN and WAN // Computer Networks. 2016. Vol. 67. pp. 74-88.
8. Kabalci Y. A survey on metering communication // Renewable and Sustainable Energy Reviews. 2016. Vol. 57. pp. 302-318.
9. Старр, М. Управление производством / М. Старр. - М.: Прогресс, 2020. - 400 с.
10. Корнева, Л. В. 1С:Документооборот + склад. Версия 8.0 / Л.В. Корнева. - М.: Феникс, 2020. - 272 с.
11. Ильина, О.П. Служба информационного обеспечения / О.П. Ильина, И.А. Смирнов, В.Ф. Юровский. - М.: Лениздат, 2016. - 151 с.

УДК 004.9

Н. А. КОНОНОВ
knnv.nkt@gmail.com
Науч. руководов. – д-р техн. наук, проф. В. В. АНТОНОВ

Уфимский государственный авиационный технический университет

ПРОТОТИПИРОВАНИЕ ИНФОРМАЦИОННЫХ СИСТЕМ НА ПРИМЕРЕ ИНФОРМАЦИОННОЙ СИСТЕМЫ ВЕДЕНИЯ ПРИЕМНОЙ КАМПАНИИ ВОЕННОГО УЧЕБНОГО ЦЕНТРА

***Аннотация*.** В рамках данной статьи определено понятие прототипа и сущность прототипирования; рассмотрен один из подходов к прототипированию информационных систем на примере разработки прототипа информационной системы ведения приемной кампании военного учебного центра.
***Ключевые слова*:** системный анализ; системное моделирование; CASE-технологии; прототипирование; прототип информационной системы; ВУЦ; военный учебный центр.

Определение сущности прототипирования

Согласно международному стандарту практик бизнес-анализа BABOK Guide 3.0 [1], прототипирование используется для определения требований и неподтвержденных предположений путем демонстрации того, как продукт выглядит и как она работает.

Прототипы можно разделить на одноразовые (Throw-away) и развиваемые (EvolutionaryorFunctional) прототипы.

Одноразовые прототипы разрабатываются с помощью примитивных инструментов (бумага и карандаш или графический редактор). В ходе работы такой прототип может быть многократно доработан, однако он не становится работоспособным кодом и не поддерживается в качестве конечного результата после реализации системы.

Развиваемые прототипы требуют специализированных инструментов. Прототипы, разработанные по данному подходу, являются работающими решениями и могут быть использованы в качестве финального продукта.

Таким образом, прототип информационной системы — это частичная или возможная реализация предлагаемой концепции информационной системы.

Исследование предметной области

Для разработки прототипа информационной системы необходимо предварительно выполнить:

– изучение предметной области (контекст предмета исследования);

– исследование существующего бизнес-процесса;

– определение недостатков существующего бизнес-процесса и особенностей предметной области;

– определение цели преобразования системы;

– анализ возможных путей улучшения и формирование предложений по усовершенствованию существующего бизнес-процесса.

В результате исследования существующего бизнес-процесса и формализации предложений по его преобразованию должны быть разработаны комплексы функциональных и динамических моделей бизнес-процесса. Структура моделей (количество уровней рассмотрения и нотация) определяется методологией проектирования.

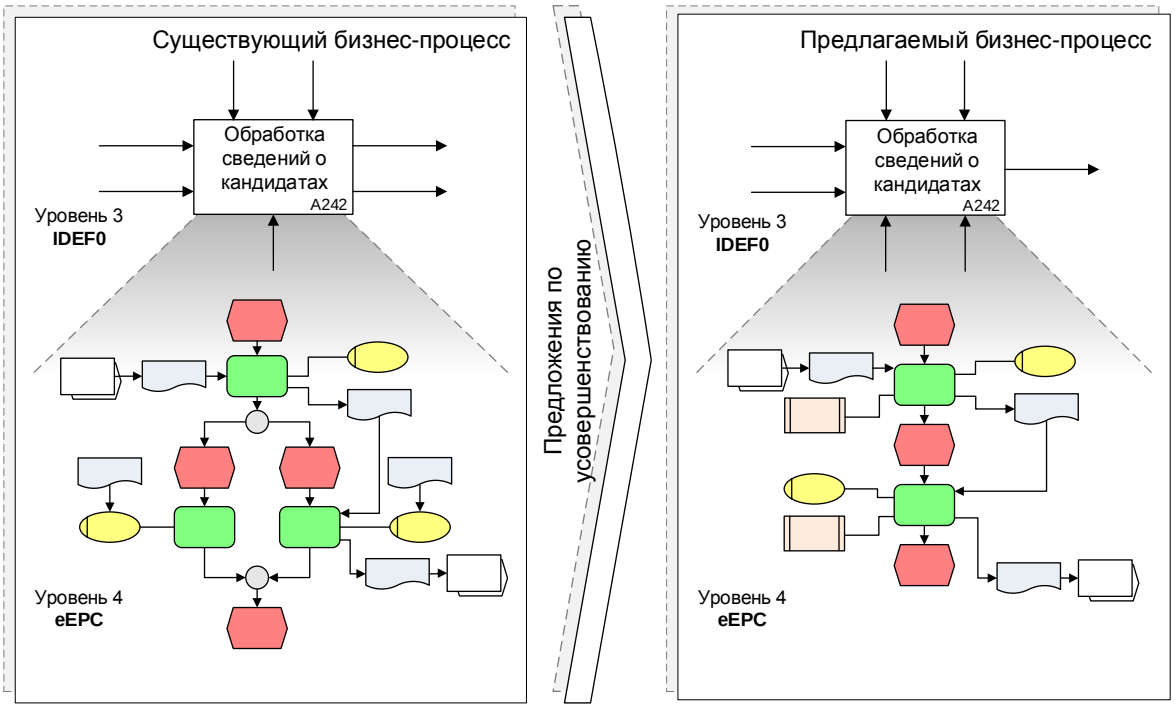


Рис. 1. Фрагменты архитектуры уровней модели

На рисунке 1 представлен фрагмент структуры уровней одного из вариантов структуры модели, где применяется методология структурного анализа и проектирования[2]: на верхних уровнях используются функциональные диаграммы в нотации IDEF0, а нижний уровень детализируются с помощью динамических диаграмм в нотации eEPC [3].

В рамках данной работы рассматривается разработка прототипа фрагмента информационной системы ведения приемной кампании военного учебного центра. Функционально фрагмент соответствует задаче «A242 Обработка сведений о кандидатах» [4]. Предполагается, что остальные фрагменты информационной системы разрабатываются аналогично.

Для поставленной задачи, было принято решение о рассмотрении бизнес-процесса на 5 уровнях.

На рисунках 2-4 представлена диаграмма декомпозиции функционального блока «A242 Обработка сведений о кандидатах» в нотации eEPC модели существующего бизнес-процесса «Проведение конкурсного отбора».

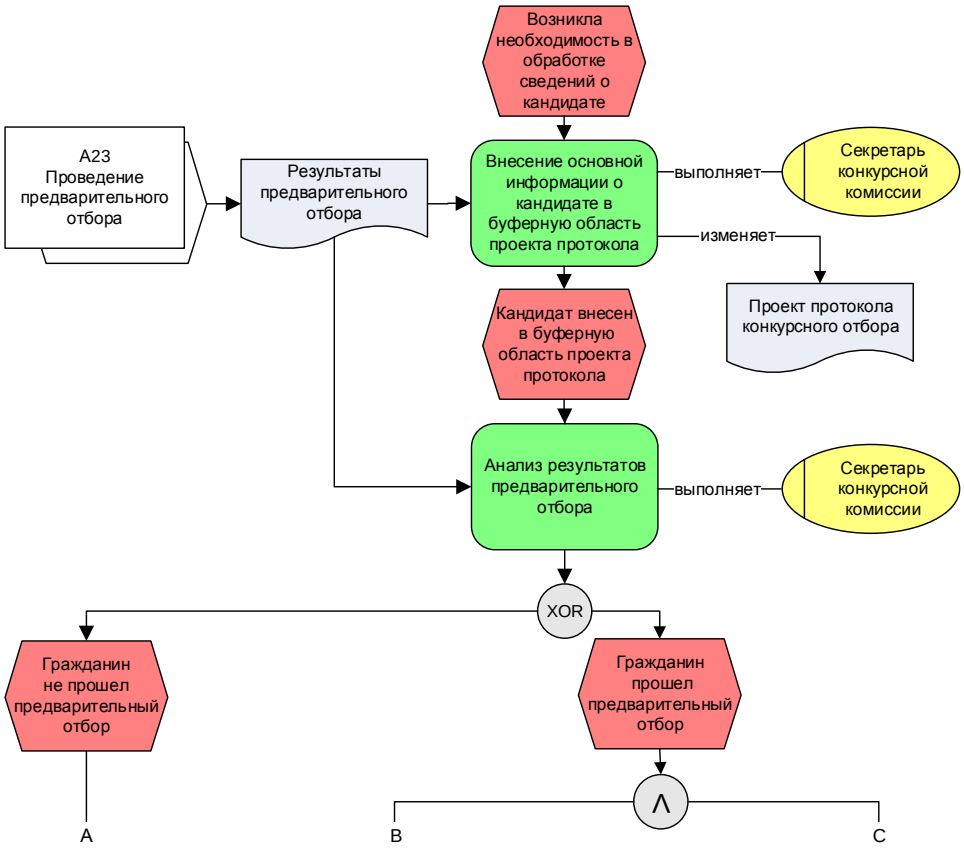


Рис. 2. Декомпозиция функционального блока «A242 Обработка сведений о кандидатах» модели существующего бизнес-процесса в нотации eEPC, фрагмент 1

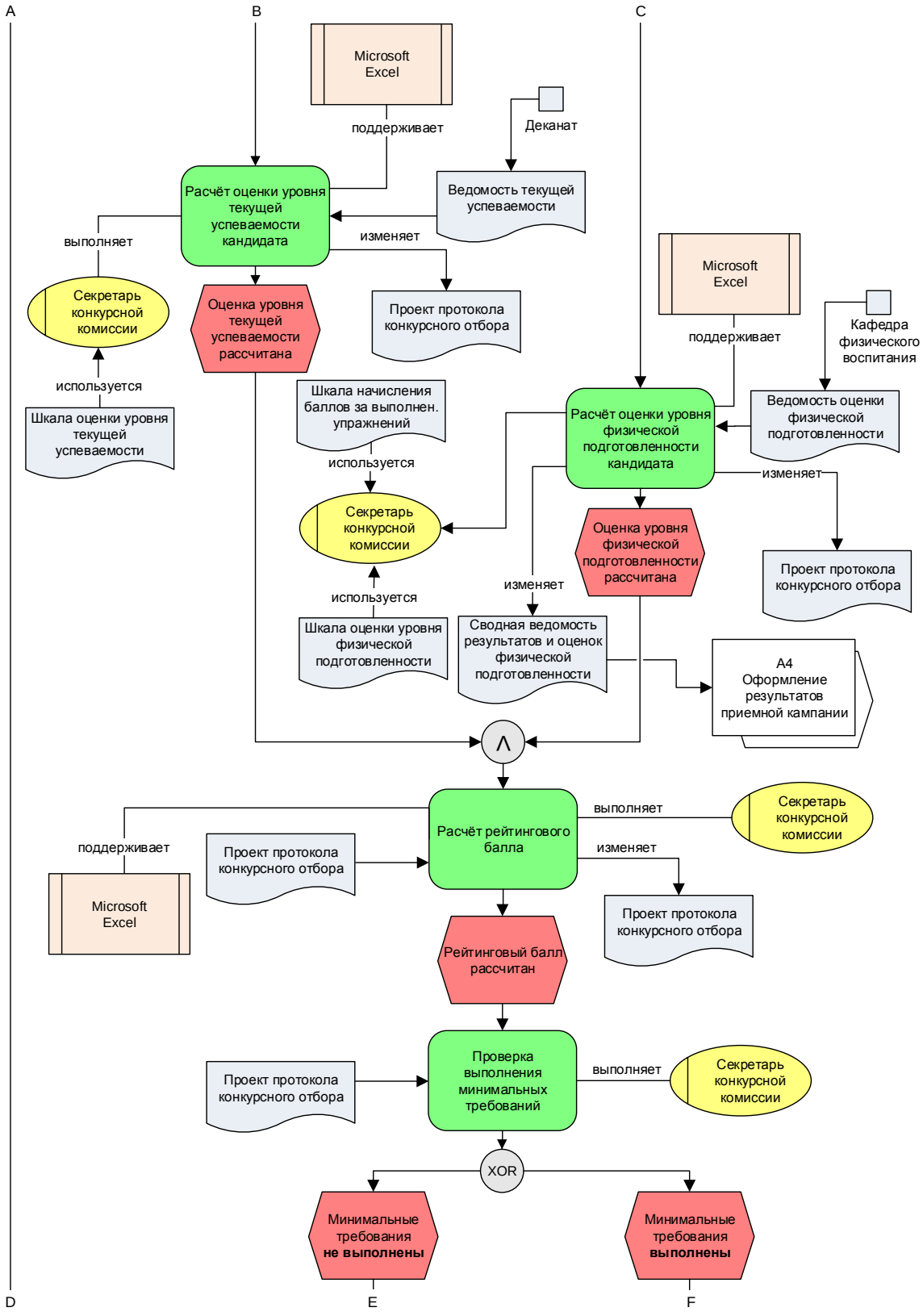


Рис. 3. Декомпозиция функционального блока «A242 Обработка сведений о кандидатах» модели существующего бизнес-процесса в нотации eEPC, фрагмент 2

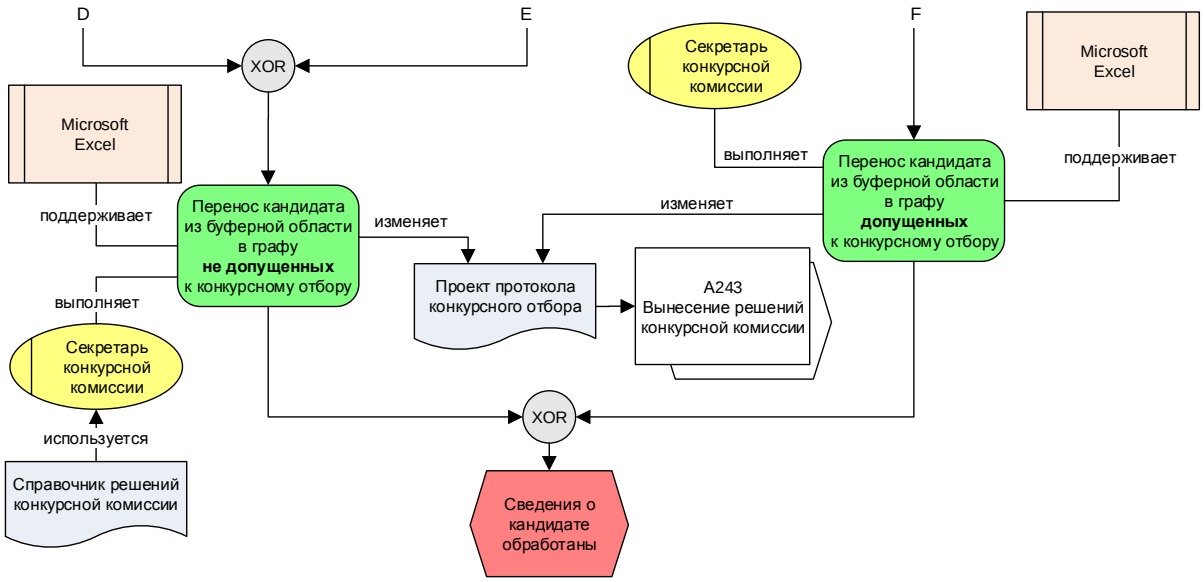


Рис. 4. Декомпозиция функционального блока «A242 Обработка сведений о кандидатах» модели существующего бизнес-процесса в нотации eEPC, фрагмент 3

Поскольку этап перестройки бизнес-процесса не входит в область обозрения данной работы модели предлагаемого бизнес-процесса представлены без пояснения их происхождения. Тем не менее, при построении модели предлагаемого бизнес-процесса рекомендуется определить подход к преобразованию системы. М. Хаммер и Дж. Чампи в книге «Реинжиниринг корпорации. Манифест революции в бизнесе» определяют следующие подходы в зависимости от использования информационных технологий и организационных изменений: системная интеграция, постепенные улучшения, инновация процессов, реорганизация и реинжиниринг бизнес-процессов.

Разработанные предложения по усовершенствованию существующего бизнес-процесса «Проведение конкурсного отбора граждан» были формализованы в виде комплекса функциональных и динамических моделей предлагаемого бизнес-процесса.

На рисунке 5 представлена декомпозиция функционального блока «A242 Обработка сведений о кандидатах» модели предлагаемого бизнес-процесса в нотации eEPC.

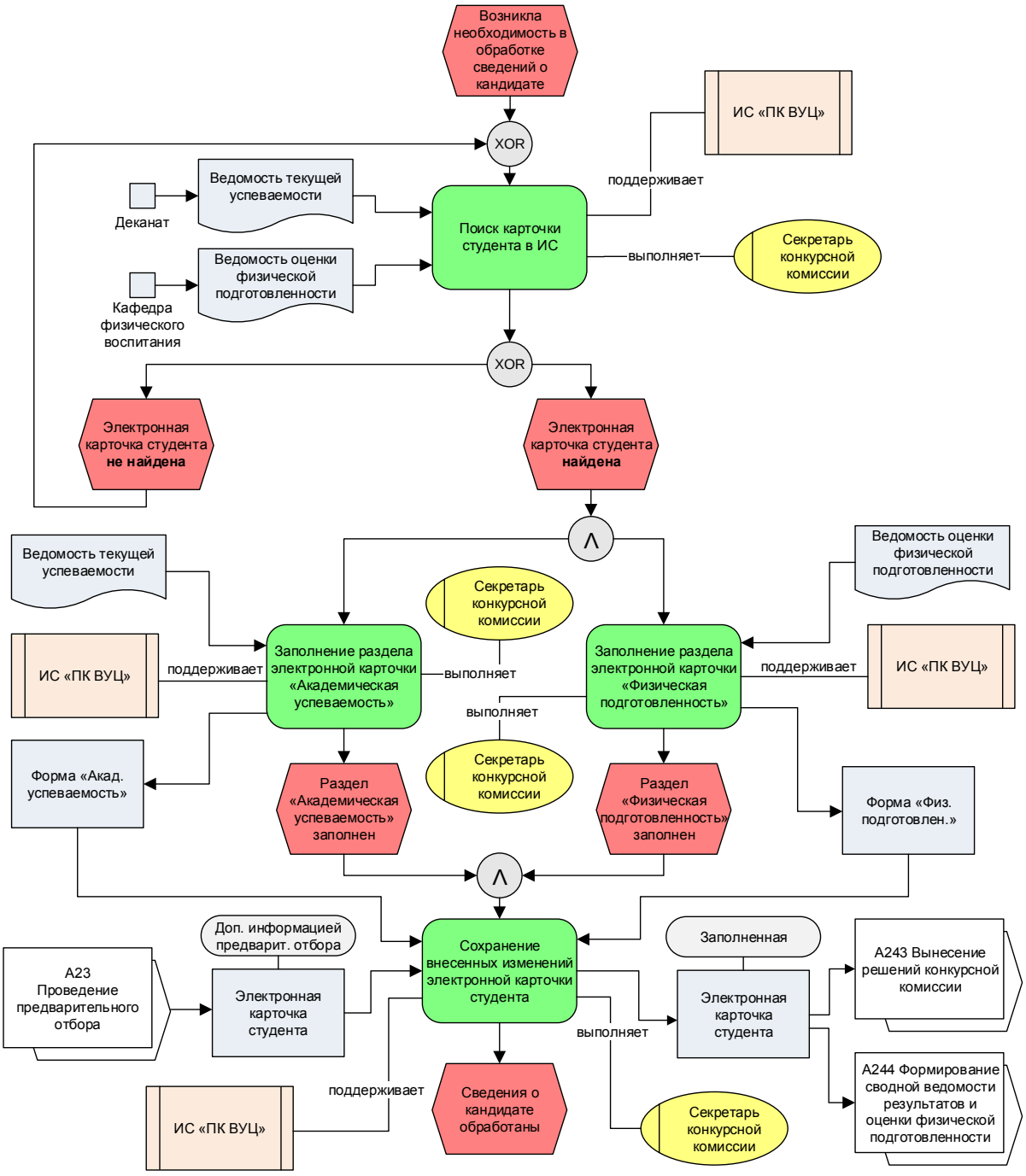


Рис. 5. Декомпозиция функционального блока «A242 Обработка сведений о кандидатах» модели предлагаемого бизнес-процесса в нотации eEPC

Формирование требований к функциям фрагмента информационной системы

На основе модели предлагаемого бизнес-процесса были сформированы требования к функциям информационной системы.

Требования, предъявляемые к функциям информационной системы, разделяют на автоматизированные и автоматические. В таблице 1 представлены

примеры требований, которые могут быть предъявлены к информационной системе ведения приемной кампании военного учебного центра, в частности к фрагменту, отвечающему за осуществление обработки сведений о кандидатах.

Таблица 1

Примеры требований, предъявляемых к информационной системе ведения приемной кампании военного учебного центра

Автоматические	Автоматизированные
1. Система должна обеспечивать автоматический расчет рейтинговых баллов при заполнении всех необходимых данных о студенте. 2. Система должна обеспечивать автоматическую проверку выполнения минимальных требований по каждому упражнению. 3. Система должна обеспечивать автоматическую проверку выполнения минимального требования к суммарному баллу по всем упражнениям.	1. Система должна позволять выполнять поиск по уникальному идентификатору студента. 2. Система должна позволять выполнять ввод среднего балла студента. 3. Система должна позволять выполнять ввод результатов сдачи упражнений по физической подготовленности.

Информационное моделирование

Потоки информации, обеспечивающие функционирование рассматриваемого бизнес-процесса, должны быть исследованы, проанализированы и распределены по трем категориям: исходная (входная) информация, результатная (выходная) информация, условно-постоянная информация.

В таблице 2 представлен фрагмент перечня исходной (входной), результатной (выходной) и условно-постоянной информации, обеспечивающих решение задачи по обработке сведений о кандидатах.

Таблица 2

Фрагмент перечня исходной, результатной и условно-постоянной информации

Исходная (входная)	Результатная (выходная)	Условно-постоянная
Результаты предварительного отбора	Проект протокола конкурсного отбора	Шкала оценки уровня текущей успеваемости
Ведомость текущей успеваемости		Шкала оценки уровня физической подготовленности
Ведомость оценки физической подготовленности		Шкала начисления баллов за выполнение упражнений

Далее было выполнено описание структурных элементов исходной (входной), результатной (выходной) и условно-постоянной информации. Наборы структурных элементов информации должны быть представлены в объеме, достаточном для решения рассматриваемой задачи.

Основываясь на полученных результатах исследования информационных потоков, обеспечивающих решение задачи, должна быть сформирована информационная модель. На рисунке 6 представлен фрагмент информационной модели логического уровня в нотации IDEF1x [5].

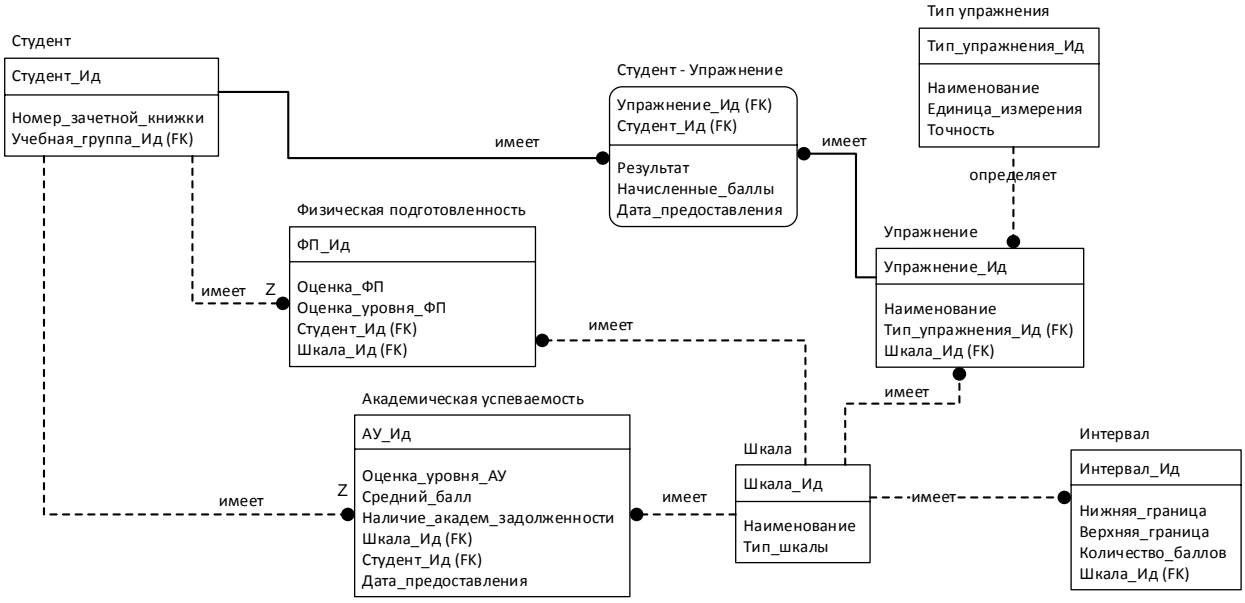


Рис. 6. Фрагмент информационной модели

Разработка алгоритма решения задачи

Преобразование входной информации в выходную можно представить в виде комплекса схем алгоритмов работы программы. Для рассматриваемого примера по разработке прототипа фрагмента информационной системы ведения приемной кампании военного учебного центра, представлен один из алгоритмов по расчету рейтингового балла студента (рисунок 7).

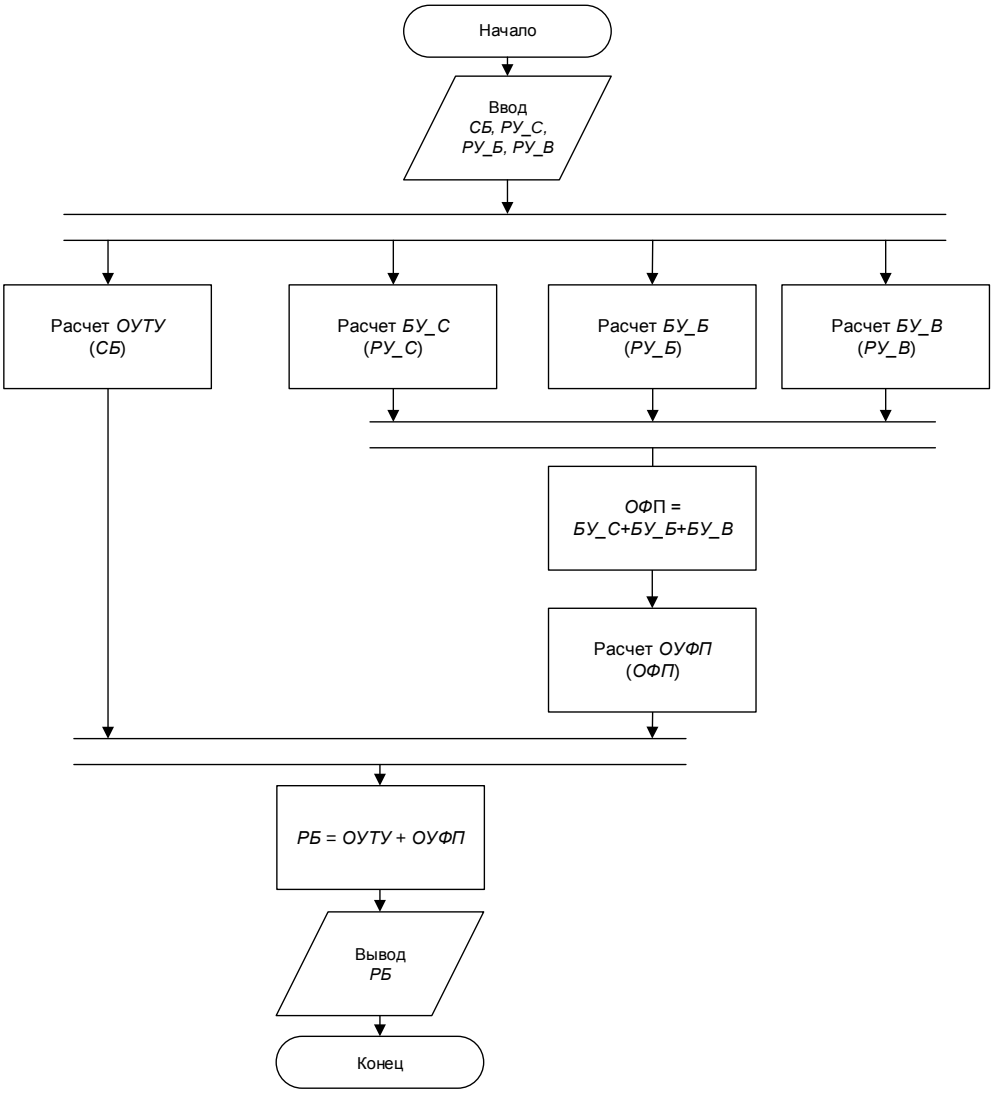


Рис. 7. Схема алгоритма расчета рейтинговых баллов студента

Разработка прототипа на языке PHP

Прототип может быть реализован на любом из известных языков программирования (VBA, Java, PHP и др.), технологической платформе 1С или системе управления бизнес-процессами, поддерживающей возможность прототипирования (Elma, BizagiStudio).

В рамках данной работы наиважнейшими критериями при выборе языка программирования для разработки прототипа информационной системы ведения приемной кампании ВУЦ являлись возможность технической поддержки разрабатываемой системы и возможность потенциальной интеграции в инфра-

структуру университета. Язык веб-программирования PHP был выбран как наиболее подходящий по данным критериям.

Программный продукт с продуманной архитектурой легче расширять и изменять, а также тестировать, отлаживать и понимать.При формировании архитектуры программного продукта на языке PHP был выбран архитектурный паттерн MVC.

Архитектурный шаблон проектирования MVC предполагает разделение данных (информации, состояния), пользовательского интерфейса и бизнес-логики приложения на три типа компонентов: Model (Модель), View (Представление) и Controller (Контроллер). Подобное разделение системы на компоненты позволяет модифицировать их независимо друг от друга.

На рисунке 8 представлена разработанная мнемосхема архитектуры приложения, реализующего паттерн MVC на языке PHP [6].

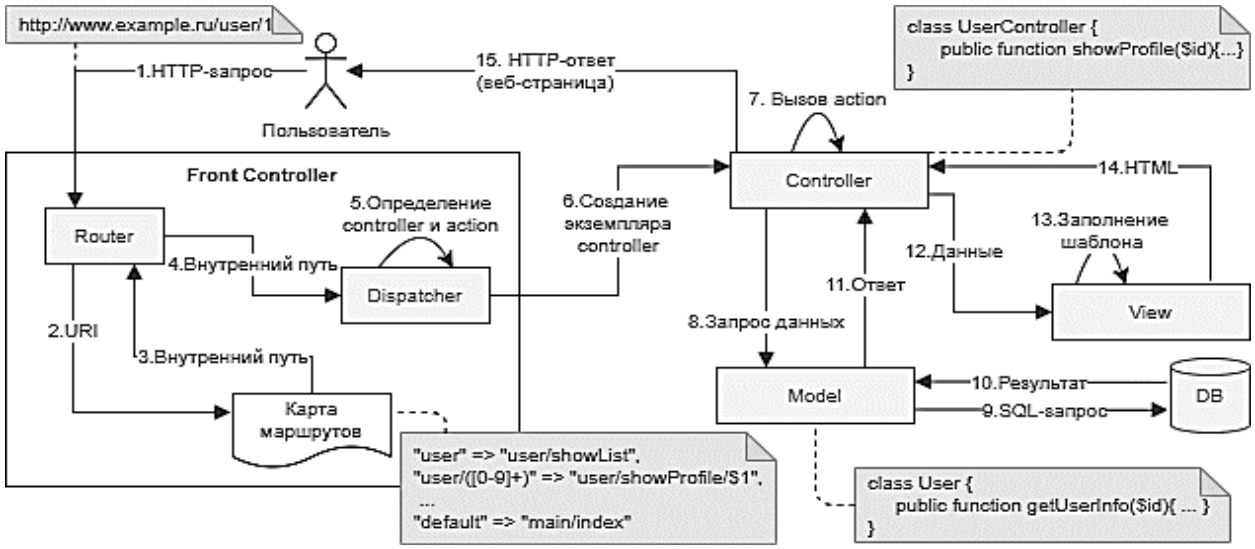


Рис. 8. Мнемосхема архитектуры приложения, реализующая паттерн MVC на языке PHP

На рисунке 9 представлена экранные формы разработанного прототипа информационной системы ведения приемной кампании военного учебного центра. Фрагмент, рассматриваемый в рамках данной работы ограничен красным контуром.

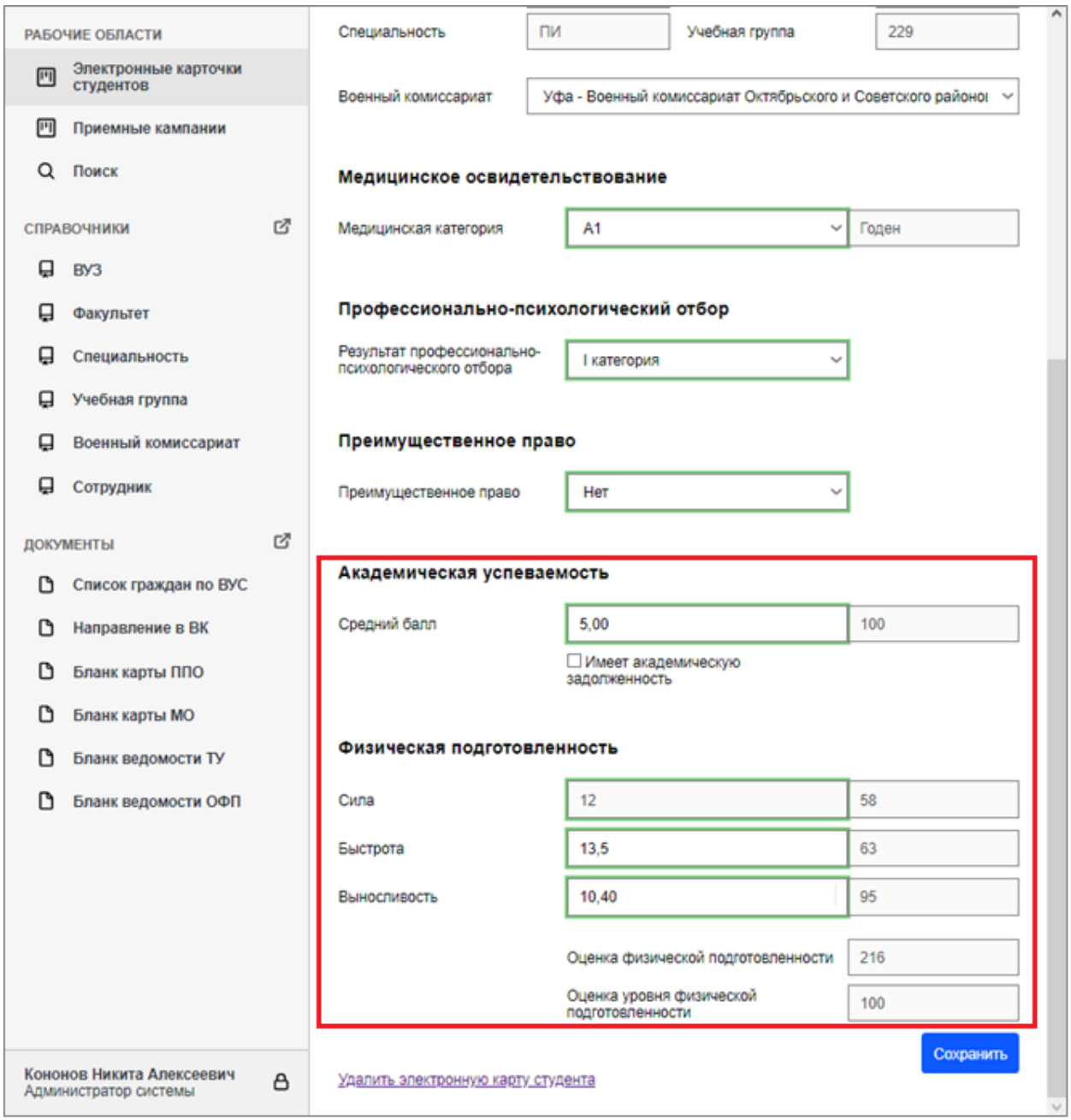


Рис. 9. Фрагмент заполненной электронная карточка студента

Заключение

Представленный в рамках данной работы подход к прототипированию информационных систем был применен для разработки прототипа информационной системы ведения приемной кампании военного учебного центра.Разработанный прототип является работающим программным решением и применяется в качестве финального программного продукта.

СПИСОК ЛИТЕРАТУРЫ

1.BusinessAnalysisinRussia// База знаний по бизнес-анализу URL: https://analytics.infozone.pro/babok/chapters-of-babok-version-3/(дата обращения: 20.09.2021)
2. Марка, Д.А. Методология структурного анализа и проектирования: [Пер. с англ.] / Дэвид А. Марка, Клемент Л. МакГоуэн; Предисл. Д. Т. Росса. - [М.] :Фирма "МетаТехнология", 1993. - 240 с.
3. Репин В. Business Studio, нотацияeEPC: границыпроцессов, события, стрелки // Business Studio URL: https://www.businessstudio.ru/articles/article/business_studio_notatsiya_eepc_granitsy_protsessov/ (датаобращения: 20.09.2021)
4.ГиндуллинаТ.К. Кононов Н.А. К вопросу применения компьютерных технологий в приемной кампании военного учебного центра / Гиндуллина Т.К. Кононов Н.А. // Мавлютовские чтения: материалы V Международной научно-технической конференции, посвященной 95-летию со дня рождения член-корр. РАН, д-ра техн. наук, профессора РыфатаРахматулловичаМавлютова: в 6 томах / Уфимск. гос. авиац. техн. ун-т. – Уфа : УГАТУ, 2021. – С. 42-47.
5. Дейт, К.Дж. Введение в системы баз данных [Текст] / К.Дж. Дейт ; пер. с англ. – 6-е изд. – Киев ; М. ; СПб. : Издательский дом «Вильямс», 1999. – 848 с.
6. Кононов Н.А. Проектирование архитектуры веб-приложения, реализующего паттерн MVC на языке PHP / Кононов Н.А. // Теоретический и практический потенциал современной науки: Сборник научных статей. Ч. VII. – М., 2019. – С. 92-94.

УДК 004.75

Г. Р. САФИНА
lafleur300997@gmail.com
Науч. руководитель – д-р техн. наук, проф. В. Е. ГВОЗДЕВ

Уфимский государственный авиационный технический университет

ФОРМИРОВАНИЕ СБАЛАНСИРОВАННОЙ СИСТЕМЫ ХАРАКТЕРИСТИК В МОДЕЛИ «ТРЕУГОЛЬНИК ПРОЕКТА»

Аннотация. Формирование характерной сбалансированной системы программного проекта является решающим фактором успешной реализации проекта. В этой статье описывается формальная процедура оценки значений бюджета и продолжительности реализации проекта, которые обеспечивают наилучшее соответствие между удовлетворенностью клиентов результатами проекта и участниками проекта. Проект представлен в виде многомерного объекта управления. Эмпирические функциональные зависимости соответствуют прямой и перекрестной связи многомерного объекта.
Ключевые слова: треугольник проекта; начальная стадия проекта; консолидированное решение; многосвязный объект управления; продолжительность проекта; реализация проектов.

Введение

Основываясь на информации, представленной в отчетах StandishGroup [1, 2], можем сделать вывод о том, что, несмотря на прогресс в области разработки проектов, технологий и инструментов, эффективность реализации проектов остается низкой. В [3] и других отмечается, что одной из причин инцидентов, возникающих в предметно-ориентированных системах, являются ошибки организационной системы. Одной из причин возникновения системных ошибок является дисбаланс в основных характеристиках проекта (бюджет проекта, продолжительность проекта, удовлетворенность участников проекта) [2, 7].

Концептуальной основой настоящей статьи является положение о том, что удовлетворенность потребителя результатами проекта, а исполнителя – организацией и ходом реализации проекта являются равнозначными факторами, определяющими успех проекта.

1. Положения и попущения подхода

Концептуальную основу подхода составляет следующее положение:результаты проекта и ход его реализации должны обеспечивать приемле-

мый уровень удовлетворенности всем акторам, причастным к реализации проекта.

В силу того, что программные системы относятся к классу субъектоцентрических систем при оценивании проектов нужно одновременно использовать как их измерительные данные, так и субъективные оценки потребителей и исполнителей. При оценивании качества хода проекта и потребительских свойств получаемого продукта в равной степени важно учитывать удовлетворенность исполнителей и заказчиков. В качестве входных параметров проекта рассматриваются бюджет и длительность реализации проекта. В качестве выходных – удовлетворенность представителей заказчика и исполнителей проекта. Содержание этого допущения является конкретизацией компонентов известной системной модели «треугольник проекта» в редакции 2015 года. Модель треугольника проектов представлена на рисунке 1.

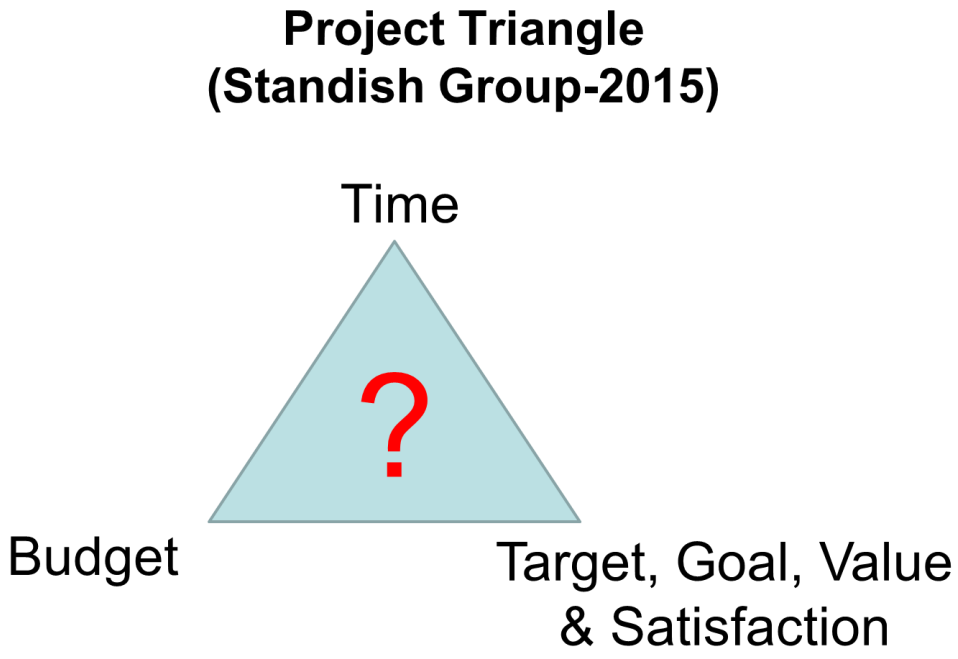


Рис. 1. Модель треугольника проектов

И хотя для проекта в равной степени важны все три элемента, как правило, только один из них в зависимости от приоритетов имеет наибольшее влияние на другие, и как правило, очень сложно подобрать необходимое количество

ресурсов, которые бы удовлетворяли участников проекта, таких как разработчик и заказчик программного проекта. Это связано с тем, что у разработчика и у заказчика имеются свои онтологии, свое видение окружающего мира и ценностей.

Изобразим предполагаемый процесс оценки сбалансированности характеристик проекта в виде мнемосхемы. Использование мнемосхемы для демонстрации исследуемого процесса обусловлена тем, что мнемосхема – наглядное, графическо-схематическое, условное представление системы или процессов системы в символьно-графической форме, наглядно отображающее исследуемую систему.

2. Представим проект как многосвязный объект управления

Проект как многосвязный объект управления поставлен на рис. 1.

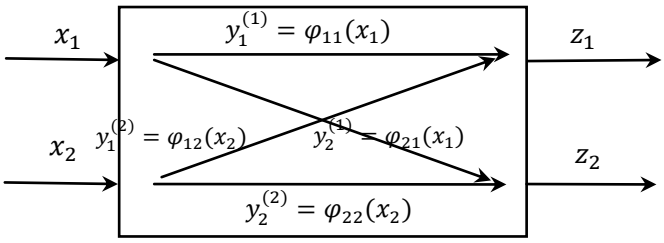


Рис. 2. Модель проекта как многосвязного объекта управления

Входными (управляемыми) параметрами модели являются x1 – бюджет и x2 –длительность реализации проекта соответственно. Выходными параметрами являются удовлетворенность заказчика - y1 и исполнителя y2 соответственно.

Совместное влияние входных характеристик x_i на выходные определяется на основе функциональных зависимостей, характеризующих прямые и перекрестные связи $y_j^{(i)} = \varphi_{ij}(x_i)$:

$$A^{(j)}: \left\{ y_j^{(i)} = \varphi_{ij}(x_i) \right\} \rightarrow z_j = \Phi_j(x_1, x_2), i, j = 1, 2 \qquad (1)$$

Здесь $A^{(j)}$– оператор свертки, соответствующий *j-му* выходному параметру модели.

Областью допустимых значений для характеристики удовлетворенности y_j будем считать интервал $y_j \in [0,1]$, $j = 1, 2$. Нижняя граница интервала

соответствует варианту, когда субъекты (потребитель/исполнитель) абсолютно не удовлетворены результатами /ходом проекта. Верхняя граница интервала соответствует их абсолютной удовлетворенности.

Удовлетворенность потребителя уменьшается по мере увеличения как бюджета x_1, так и длительности реализации проекта x_2. Поэтому функциональные зависимости $y_j^{(i)} = \varphi_{ij}(x_i)$ являются обратными. При этом возможна компенсация одного параметра другим. К примеру, компенсация изменения длительности реализации проекта за счет изменения бюджета проекта и наоборот.

С точки зрения заказчика возможна реализация проекта нулевой длительности, что фактически соответствует приобретению готового продукта. Исходя из вышеизложенного можно утверждать, что $\Phi_1(x_1, x_2)$ можно представить аддитивной функцией, т.е.

$$y_1 = \varphi_{11}(x_1) + \varphi_{21}(x_2) \quad (2)$$

Удовлетворенность исполнителей, напротив, растет с увеличением как бюджета x_1, так и длительности реализации x_2 проекта. Постулируется, что исполнитель отказывается от реализации проекта, если хотя бы одна из его характеристик x_i *(i=1,2)* равна нулю.

Исходя из этих соображений можно заключить, что в качестве $\Phi_2(x_1, x_2)$ можно использовать:

$$y_2 = \varphi_{12}(x_1) * \varphi_{22}(x_2) \quad (3)$$

т.е. мультипликативную функцию.

3. Постановка и схема решения задачи

Известен вид функциональных зависимостей $y_j^{(i)} = \varphi_{ij}(x_i)$, *i,j*=1, 2

Требуется оценить значения параметров проекта $x_i^{(OUT)}$ (*i=1,2*), при которых достигается наименьшее различие в удовлетворенности результатами проекта потребителей y_1 и исполнителей y_2.

Очевидно, что наименьшее различие в удовлетворенности результатами проекта потребителями и ходом проекта исполнителями достигается при $y_1=y_2$. Этому условию соответствует соотношение

$$\varphi_{11}(x_1) + \varphi_{21}(x_2) = \varphi_{12}(x_1) * \varphi_{22}(x_2) \quad (4)$$

При этом должны соблюдаться ограничения:

$$0 \le \varphi_{11}(x_1) + \varphi_{21}(x_2) \le 1 \quad (5)$$

$$0 \le \varphi_{12}(x_1) * \varphi_{22}(x_2) \le 1 \quad (6)$$

$$x_i 0 \ge 0, i = 1,2 \quad (7)$$

Рассмотрим случай, когда связи внутри многосвязного объекта управления, представленного на рисунке 1, представлены в виде нелинейных зависимостей, так что:

$$\varphi_{11}(x_1) = e^{\lambda_0 - \lambda_1 x_1} - k_1 \quad (8)$$

$$\varphi_{21}(x_2) = e^{\mu_0 - \mu_2 x_2} - k_2 \quad (9)$$

$$\varphi_{12}(x_1) = R_1 * \sqrt[n]{x_1} \quad (10)$$

$$\varphi_{22}(x_2) = R_2 * \sqrt[m]{x_2} \quad (11)$$

В этом случае совокупное влияние x_1, x_2 на y_1, y_2 определяются соотношениями:

$$y_1 = e^{\lambda_0 - \lambda_1 x_1} - k_1 + e^{\mu_0 - \mu_2 x_2} - k_2 \quad (12)$$

$$y_2 = R_1 * \sqrt[n]{x_1} * R_2 * \sqrt[m]{x_2} \quad (13)$$

Ограничения на входные и выходные параметры определены в постановке задачи (6) – (8).

Коэффициенты k_1 и k_2 необходимы для обеспечения условия:

$$y_1(x_1^*) = 0$$

$$y_2(x_2^*) = 0$$

Функция вида $z = e^{a+bt}$ при конечном t никогда не равна нулю.

Поэтому

$$y_1 = e^{\lambda_0 - \lambda_1 x_1^*} - k_1 = 0 \quad (14)$$

Отсюда

$$e^{\lambda_0 - \lambda_1 x_1^*} = k_1 \quad (15)$$

Или

$$\lambda_{0-}\lambda_1 x_1^* = \ln(k_1) \quad (16)$$

Откуда

$$\lambda_1 = \frac{\lambda_{0-}\ln(k_1)}{x_1^*} \quad (17)$$

Аналогичным образом находим μ_2:

$$\mu_{0-}\mu_2 x_2^* = \ln(k_2) \quad (18)$$

Откуда

$$\mu_2 = \frac{\mu_{0-}\ln(k_2)}{x_2^*} \quad (19)$$

Найдем значения функций при нулевом бюджете и нулевой длительности реализации проекта, то есть при $x_1 = 0$ и $x_2 = 0$

$$\varphi_{11}(0) = e^{\lambda_0} - k_1 \quad (20)$$

$$\varphi_{21}(0) = e^{\mu_0} - k_2 \quad (21)$$

Постулируя равную степень влияния на y_1 как x_1, так и x_2, получаем

$$e^{\lambda_0} - k_1 = 0{,}5 \quad (22)$$

$$e^{\mu_0} - k_2 = 0{,}5 \quad (23)$$

Выражаем из (28) и (29) λ_0 и μ_0:

$$\lambda_0 = \ln(0{,}5 - k_1) \quad (24)$$

$$\mu_0 = \ln(0{,}5 - k_2) \quad (25)$$

С учетом (30) и (31) соотношения (23) и (25) преобразуются к виду

$$\lambda_1 = \frac{\ln(0{,}5-k_1)-\ln(k_1)}{x_1^*} = \frac{\ln(\frac{0{,}5-k_1}{k_1})}{x_1^*} \quad (26)$$

$$\mu_2 = \frac{\ln(0{,}5-k_2)-\ln(k_2)}{x_2^*} = \frac{\ln(\frac{0{,}5-k_2}{k_2})}{x_2^*} \quad (27)$$

С учетом того, что $y_j \leq 1$, из (18), (19) получаем:

Для y_2:

$$0 \leq y_2 = R_1 * \sqrt[n]{x_1} * R_2 * \sqrt[m]{x_2} \leq 1 \quad (28)$$

Пусть:

$$R_1 * R_2 = R_\Sigma$$

Отсюда:

$$x_1^{\frac{1}{n}} * x_2^{\frac{1}{m}} \leq \frac{1}{R_\Sigma} \tag{20}$$

Таким образом,

$$x_2 \leq (\frac{1}{R_\Sigma} * \frac{1}{x_1^{\frac{1}{n}}})^m \tag{30}$$

В частном случае при $R_1 = R_2$=1, n=m=0, получим:

$$x_2 \leq \frac{1}{x_1} \tag{31}$$

Для y_1:

$$0 \leq y_1 = e^{\lambda_0 - \lambda_1 x_1} - k_1 + e^{\mu_0 - \mu_2 x_2} - k_2 \leq 1 \tag{32}$$

В частном случае при k_i=1 при i=1,2, $x_j^* = 1$ при j=1,2, получим

$$x_2 \leq \frac{x_1}{3x_1 - 1} \tag{33}$$

Соотношения (37) и (39) определяет область, которой возможен поиск $x_1^{(OUT)}$ и $x_2^{(OUT)}$. Эта область на рисунке 11 выделена штриховкой.

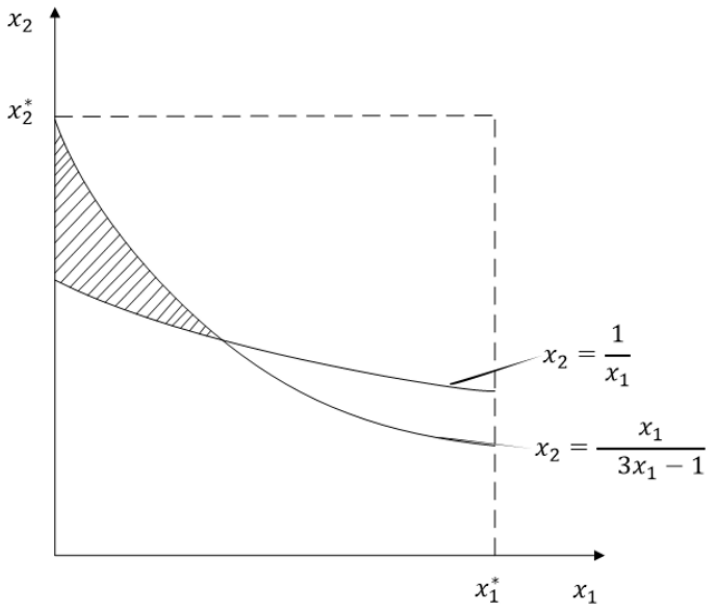


Рис. 3. Область поиска $x_i^{*(OUT)}$, при $i = 1, 2$

В таблице 1 приведены значения $y_1^{(OUT)}$ и $y_2^{(OUT)}$ при различных значениях коэффициентов нелинейных зависимостей и с заданными максимальными значениями $x_i^{*(OUT)}$, при $i = 1,2$.

Таблица 1

Значения x_1^* и x_2^* и соответствующие им значения $y_j^{(OUT)} = \Phi_{ij}(x_1^*, x_2^*)$

k_1	k_2	λ_0	μ_0	λ_1	μ_2	R_1	R_2	$x_1^{(OUT)}$	$x_2^{(OUT)}$	$y_1^{(OUT)}$	$y_2^{(OUT)}$
0,1	0,1	-0,9	-0,9	1,4	1,4	1	1	0,1	1,8	0,2	0,2
0,05	0,05	-0,8	-0,8	2,2	2,2	1	1	0,1	3	0,3	0,3
0,01	0,01	-0,7	-0,7	1,9	1	1	1	0,1	4	0,4	0,4
0,1	0,1	-0,9	-0,9	0,5	0,5	1	1	0,1	3	0,3	0,3
0,05	0,05	-0,8	-0,8	0,5	0,5	1	1	0,1	4	0,4	0,4
0,01	0,01	-0,7	-0,7	0,6	0,6	1	1	0,1	5	0,5	0,5
0,01	0,01	-0,7	-0,7	0,5	0,4	1	1	0,1	5	0,5	0,5

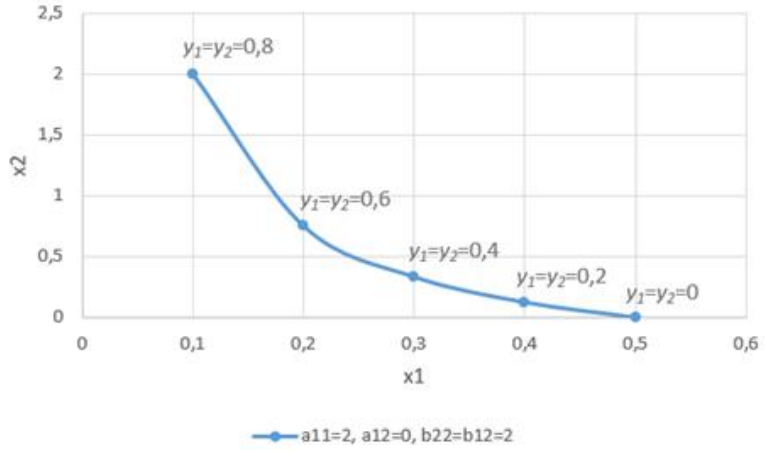


Рис. 3. Пример зависимости степени удовлетворенности от$x_i^{(OUT)}$, $i = 1, 2$ при фиксированных значениях параметров k_1, k_1 и x_1^*, x_2^*

На основании полученных зависимостей с учетом реальных ограничений на бюджет x_1^* и длительность реализации проекта x_2^* на ранних стадиях проекта можно оценить предполагаемое качество результатов (выражаемое степенью удовлетворенностиакторов) с учетом прежнего опыта взаимодействия исполнителя и заказчика.

Заключение

Предлагаемый подход делает возможным оценить предполагаемую удовлетворенность заказчика результатами проекта, а исполнителей – ходом проекта в зависимости от бюджета и ограничений на длительность проекта на ранних стадиях его разработки с учетом опыта, полученного от ранее реализованных проектов.

Предложена формальная модель проекта как многосвязного объекта управления, использование которой делает возможным повысить обоснованность принятия стратегических решений по организации проекта основными заинтересованными сторонами.

СПИСОК ЛИТЕРАТУРЫ

1. CHAOS MANIFESTO. The Standish Group International, Inc., 2013. https://larlet.fr/static/david/stream/ChaosManifesto2013.pdf
2. CHAOS Report. The Standish Group International, Inc., 2015. https://www.standishgroup.com/sample_research_files/CHAOSRepor t2015-Final.pdf
3. BowTieXP. The next generation BowTie methodology tool. BowTie Methodology Manual Revision 15 (27 Mar-2015), 64p.
4. Rick Kazman, Claus Nielsen, Klaus Schmid. Understanding Patterns for system-of-system integration//Software Engineering Institute and Acquisition Practices, Technical Node. CMU/SET-2013-TR-017, December 2013, 25p.
5. Roderic Gray. Projects and Projects Management. A review of literature, 1998, 27p.
6.CHAOS Report. The Standish Group International, Inc., 2013.
7. S. Hastie, S. Wojewoda. Standish Group 2015 Chaos Report - Q&A with Jennifer Lynch, //https://www.infoq.com/articles/standish-chaos2015/

УДК 65.11

А. А. СОМОВ
qsomov@gmail.com
Науч. руководит. – канд. физ.-мат. наук, доц. Р. Д. МУРТАЗИНА

Уфимский государственный авиационный технический университет

АВТОМАТИЗИРОВАННЫЙ АНАЛИЗ ДИНАМОГРАММЫ НИЗКОЙ И ВЫСОКОЙ ПОСАДОК ПЛУНЖЕРА

Аннотация. Автоматизация контроля и анализа возможной неисправности глубинного насоса штангового типа по динамограмме.
***Ключевые слова*:** автоматизированный анализ; обработка данных, динамограмма, глубинный насос.

Большинство действующих нефтеносных скважин оборудованы глубинными насосами штангового типа для искусственного подъема нефти.

Для оперативного контроля и анализа работы штанговых насосов используют динамограммы (графики изменения нагрузки на устьевой шток во время хода вверх-вниз).

Анализирующий компонент программы может определить низкую (см рис. 1) и высокую посадок плунжера (см. рис. 2), описать возможные неисправности оборудования, показывает график утечки и визуализирует историю измерений.

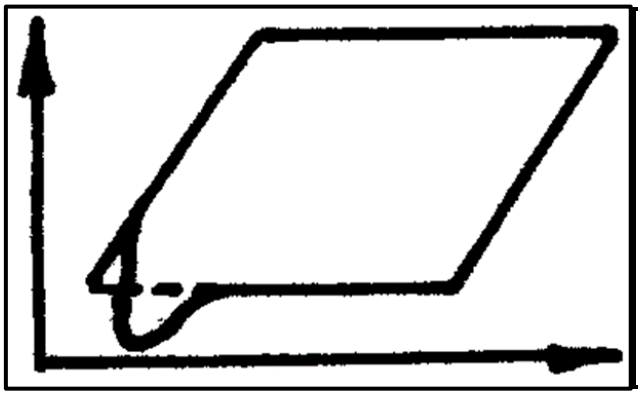


Рис. 1.

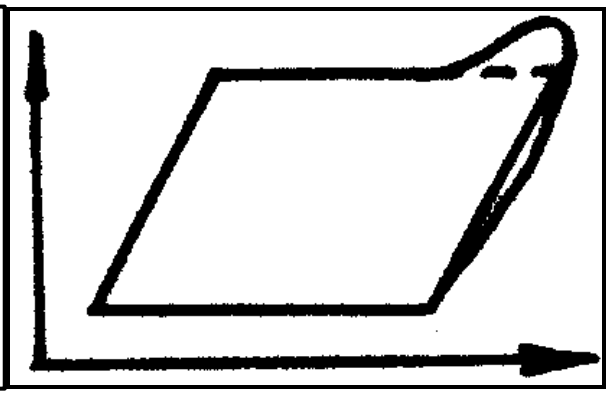


Рис. 2.

СПИСОК ЛИТЕРАТУРЫ

1. Беглов И.Г. Исследование работы глубинных насосов динамографом // Москва: Гостоптехиздат. 1960.
2. Воронцов К. В. Машинное обучение // https://bit.ly/1bCmE3Z.

УДК 004

Н. В. ХАМИНА
nadyushkakhamina@gmail.com
Науч. руководитель – канд. техн. наук, доц. Л. А. КРОМИНА,
канд. техн. наук, доц. Л. Е. РОДИОНОВА

Филиал ФГБОУ ВО «Уфимский государственный авиационный технический университет» в г. Кумертау

РЕАЛИЗАЦИЯ ТЕХНОЛОГИИ «УМНЫЙ ДОМ» В ВУЗЕ, НА ОСНОВЕ ПРИМЕНЕНИЯ КОНЦЕПЦИИ ИНТЕРНЕТ-ВЕЩЕЙ

Аннотация. Статья рассматривает применение концепции интернет-вещей, реализующих технологию «Умный дом» в вузе, а также раскрывает пользу разработки прототипа приложения и внедрения в специализированную систему для взаимодействия Вуза и Управляющей компании.
Ключевые слова: интернет-вещей; умный дом; прототип приложения; информационно-коммуникационные технологии; контроллер; графический интерфейс; функции прототипа.

В современном мире информационно-коммуникационные технологии встраиваются в механизмы обслуживания людей, а также технологии умной экономики стремительно проявляются проектными решениями, внедряемыми на предприятиях. Применение систем автоматизации, реализующих технологию «Умный дом» используется как в частных домах, так и в умных нежилых зданиях.

Реализация технологии «Умный дом» в вузе, на основе применения концепции интернет-вещей, то есть передачи данных между физическими объектами, оснащенными встроенными средствами и технологиями для взаимодействия друг с другом или с внешней средой, направлено на достижение значительной экономии финансовых и трудовых ресурсов, поскольку вуз включает в себя учебные корпуса, общежития, спорт залы. Сотрудникам периодически приходится контролировать расходование электроэнергии, воды и газа в помещениях.

В процессе исследования разработана специализированная система для управления устройствами представленная на схеме ниже. Метод обработки входных данных, глубокого обучения / нейронной сети.

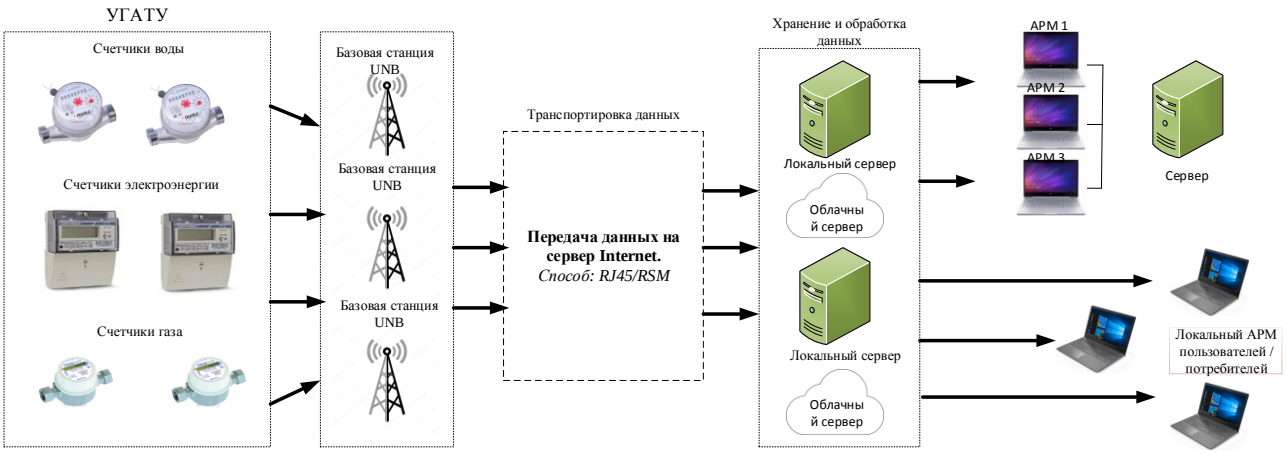


Рис. 1. Схема поступления данных- с датчиков в систему

Основываясь на изучение и обобщение теоретического и практического материала открытых источников ставится, задача разработать прототип мобильного приложения для взаимодействия Вуза и Управляющей компании.

Исследование актуально так, как на сегодняшний день, у большинства производителей, взаимодействующих с данной технологией, есть свои собственные приложения, но нет единой системы для них. Основываясь на выше перечисленных данных предполагается разработка прототипа мобильного приложения, создание проекта и разработка специальной системы управления устройствами. Учитывая это наборы данных будут соответствовать обучению модели системы.

Основой прототипа разрабатываемого приложения является отображение показаний приборов учета энергоресурсов (ХВС, ГВС, тепловая энергия, газ, электроэнергия), передаваемых по беспроводному стандарту LPWAN на центральный сервер системы.

В разрабатываемой системе предполагается контроллер, производящий вычисления в соответствии с измерениями датчиков и заложенной логикой, выдающий команды для исполнительных устройств. Серверный процесс в рассматриваемом контроллере умного дома реализован как многопоточное приложение, разработанное на языке C++ и запускаемое как отдельный сервис операционной системы.

Графический интерфейс контроллера предполагает разработку на языке PHP 7. За работу прототипа приложения отвечает веб-сервер. Одной из основных функций графического интерфейса выступает подключение интеллектуальных датчиков к контроллеру. Веб-приложение считывает его текущее состояние и конфигурацию подключенных устройств из БД SQLite.

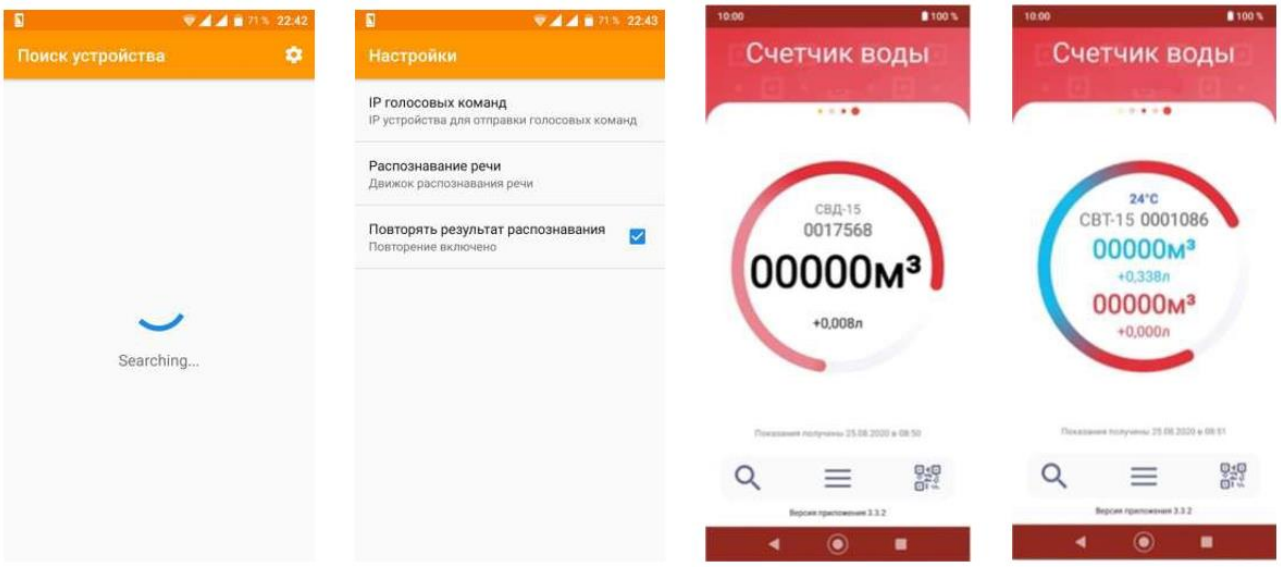


Рис. 2. Графический интерфейс прототипа приложения

Функции разрабатываемого прототипа приложения предусматривают:

1. Работа в офлайн и онлайн режиме.

2. Вход по логину и паролю, выданному при первичной регистрации пользователя в системе.

3. Сброс пароля по номеру телефона или email.

4. Для пользователя с ролью «управляющая компания»:

4.1. Выбор адреса.

4.2 Выбор абонента.

5. Отображение показаний приборов учета в личном кабинете абонента:

5.1. Отображение адреса абонента.

5.2 Отображение ФИО абонента.

6. Отображение всех контролируемых в системе приборов учета с указанием их заводских номеров и текущих показаний статистики по каждому прибору учета:

6.1 Отображение наименования прибора учета, заводского номера прибора и текущего показания.

6.2 Графическое отображение (диаграмма) отчета по расходу за выбранный период времени с возможностью группировки по часам, дням, месяцам.

Табличное отображение отчета по расходу за выбранный период времени с возможностью группировки по часам, дням, месяцам.

В заключении стоит отметить что преимущества разработанного прототипа мобильного приложения для взаимодействия Вуза и Управляющей компании заключаются в сборе данных без GSM, энергоэффективности, высокой проникающей способности, легкой интеграции данных, а также невозможности заглушить сигнал.

За счет минимизации потерь водоснабжения, исключения некорректного учета, повышения благонадежности потребителей и снижения затрат на контролеров и обходы, повышение собираемости оплаты и ответственности потребителей достигается экономия энергоресурсов.

СПИСОК ЛИТЕРАТУРЫ

1. Wikipedia [Электронный ресурс]: официальный сайт – URL: https://ru.wikipedia.org/wiki/ (дата обращения: 03.03.2021)
2. Облачный Умный Дом. Часть 1: Контроллер и датчики [Электронный ресурс]: информационный источник – URL: https://habr.com/ru/post/467219/

УДК 681.5

В. В. ЯКОВЛЕВА
Yakovleva.vv@mail.ru
Науч. руководит. – канд. техн. наук, доц. В. А. СУВОРОВА.

Уфимский государственный авиационный технический университет

К ВОПРОСУ ОБ АДМИНИСТРИРОВАНИИ ПРОЕКТОВ В КОНСАЛТИНГОВОЙ КОМПАНИИ

Аннотация. В данной работе исследуются процессы работы консалтинговой компании над проектами по внедрению корпоративной информационной системы. Целью исследования является выявление закономерностей процесса управления проектами по внедрению корпоративной информационной системы. Рассматриваются процессы работы над проектами по внедрению корпоративной информационной системы.
***Ключевые слова*:** консалтинг; консалтинговая компания; консультант; заказчик; решения; проекты; задачи.

Введение

Каждая компания, фирма, малый, средний или большой бизнес – любое предприятие стремится занять на рынке свое место, стать востребованным, иметь большой спрос, за которым последуют высокие доходы. Чтобы вырваться вперед и занять лидирующее место, компании уделяют внимание применению информационных технологий в различных процессах. Но ввести в компанию информационные системы и обучить сотрудников работе с ними недостаточно, также важно понимать, насколько эффективным является применение данной системы. В условиях постоянно развивающегося современного мира для владельцев предприятий становится актуальным обращение к консалтинговым услугам сторонних компаний.

Суть IT–консалтинга заключается во введении проектов по внедрению и поддержке информационных технологий с целью автоматизации и усовершенствования бизнес-процессов предприятия-заказчика, а также консультировании заказчика на всех этапах проекта. Эффективность проекта по внедрению корпоративной информационной системы тем выше, чем теснее сотрудничество между заказчиком и разработчиком на всех этапах работы над проектом. Для достижения наилучшего результата внедрения систем требуется качественно

выстроенная система управления. В связи с этим мы считаем актуальным для решения проблем по управлению проектами построение адекватной модели процессов администрирования проектов по внедрению корпоративной информационной системы.

Целью исследования – формализация и построение модели процессов администрирования проектов. Задача исследования – обзор существующих решений, изучение этапов процесса работы над проектом по внедрению корпоративной информационной системы, построение модели.

Анализ существующих решений

Понятие администратор проекта не является новым. В интернет- ресурсах достаточно описаний того, какой функционал у администратора проекта, предлагаются различные курсы по обучению управлению проектами, даже указываются конкретные инструменты для управления проектами. Многообразие средств и методик по администрированию проектами объясняется отсутствием единой идеальной системы управления. При выборе средств управления проектом учитывается область применения, детализированность, самодостаточность и формализация.

Например, предлагается такой способ управления проектами, как Asana. Это онлайн-сервис для командной работы над проектами, отслеживанием задач, выстраивания коммуникации в команде и обмена документами. Asana включает в себя многофункциональный набор инструментов, позволяющий вести проекты, не отвлекаясь на сторонние сервисы. В Asana у участников проекта есть дашборд, где они могут просматривать задачи, которые им надо выполнить или уже выполненные, могут просматривать статистику, а также добавлять необходимые для них диаграммы и виджеты. Руководство имеет возможность просмотра плана проекта в виде диаграмм, возможность отслеживания загруженности сотрудников для выстраивания дальнейших действия.

На образовательной платформе Skillbox предлагается курс «Менеджмент IT-проектов», который представляет собой двухгодичную магистерскую про-

грамму подготовки специалистов по управлению в сфере высоких технологий. Согласно описанию на сайте, выпускники смогут работать на стыке информационных технологий и бизнеса: сопровождать разработку и запуск проектов на всех этапах, анализировать данные, управлять проектной командой и в результате выводить на рынок коммерчески успешные продукты.

Easy Projects — это онлайн-система для управления проектами для IT-проектов, контроля операций и маркетинговых команд. Руководители проектов могут использовать инструмент для визуализации всей проектной деятельности и прогресса. К возможностям Easy Projects относится управление проектом и задачами, дашборды, планирование проекта и ресурсов, моделирование загрузки ресурсов, шаблоны проектов, генератор отчетов Ad-Hoc, уведомления по электронной почте.

В основном администрирование IT-проектами рассматривается как консалтинговая услуга заказчикам конкретных предприятий. В данной статье идет речь о необходимости внедрения процесса администрирования проектов IT-консалтинговой компании, занимающейся внедрением корпоративной информационной системы.

Этапы работы над проектом по внедрению корпоративной информационной системы

В настоящее время управление проектами – одно из наиболее востребованных направлений для достижения эффективного менеджмента. Эффективность менеджмента – сложное и многообразное понятие, смысл которого заключается в том, что весь процесс управления, начиная с постановки цели и заканчивая конечным результатом деятельности, должен производиться с наименьшими издержками или с наибольшей результативностью. Результатом работы консалтинговой IT-компании является внедренная корпоративная информационная система, отвечающая требованиям заказчика.

Каждый проект закреплен за конкретным руководителем, который контролирует всех сотрудников, привлеченных к работе над проектом. Проект со-

держит в себе множество задач, для выполнения которых привлекаются консультанты различных категорий: консультант-эксперт, ведущий консультант, старший консультант, младший консультант, консультант-разработчик. Промежуточным звеном между руководителем и консультантами являются архитектор проекта и администратор проекта, которые регулируют работу консультантов и обеспечивают взаимодействие с заказчиком. На рисунке 1 представлена организационная структура сотрудников, участвующих в работе над проектом.

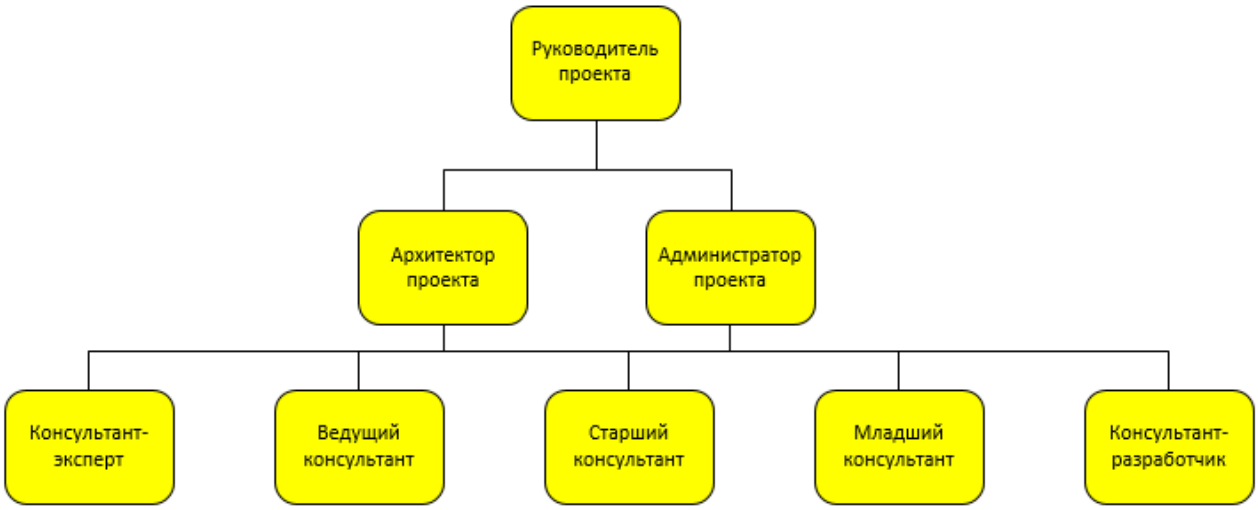


Рис. 1. Организационная структура проекта

Любая уважающая себя консалтинговая компания владеет набором компетенций, реализованных в виде различных методологий, референтных моделей. Накопленный опыт работы над предыдущими проектами позволяет приступать к каждому новому проекту, имея базу различных норм и решений, не изобретая каждый раз новый подход и методы работы.

Работа над проектом выполняется согласно составленному и утвержденному плану проекта, в котором указываются этапы проекта, ответственные лица, сроки сдачи. После обсуждения и согласования плана заказчиком приступают к исполнению проекта, что включает в себя разработку детального бизнес-сценария, технического задания, тестирование, программирование, обуче-

ние персонала компании-заказчика. По завершению работ оформляется акт сдачи-приемки проекта.

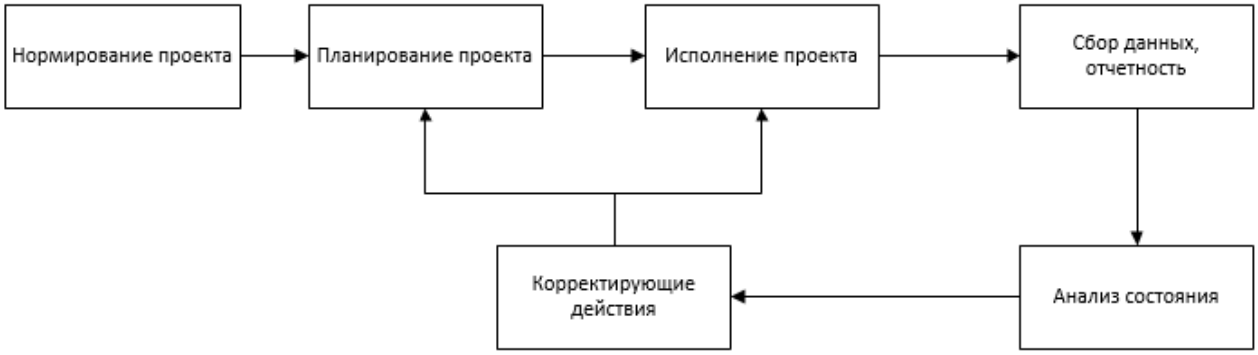


Рис. 2. Этапы работы над проектом

На рисунке 2 представлены в укрупненном виде этапы работ над проектом. По каждому из этапов формируется свой пакет документов. Администрирование каждого этапа является сложной многоуровневой задачей с итерациями на предыдущие этапы проекта.

Процесс разработки консалтингового проекта начинается с анализа первичных требований по конкретной задаче заказчика. Для определения контура проекта поставленной задачи, для четкого представления желаемого результата проводятся множественные совещания. В результате совещаний заказчик оформляет задание на оказание услуг, согласовывает предложенное решение, установку решения и подтверждает работоспособность и соответствие требованиям.

После оформления задания консультант приступает к работе: проводит анализ требований и в результате обсуждений с заказчиком деталей составляет техническое задание с описанием предлагаемого решения по проекту. Техническое задание направляется на согласование представителям заказчика и при необходимости корректируется консультантом согласно замечаниям заказчика. Именно на этом этапе появляется полная картина того, какой результат ожидает заказчик.

После согласования технического задания начинается этап разработки: документы передаются разработчикам исполнителя для программирования, после проводится тестирование, при обнаружении ошибок и недоработок вносятся соответствующие изменения в систему и технического задание, затем производится сборка предлагаемого решения и решение передается заказчику для установки и проведения тестирования системы с внедренным решением.

После успешного проведения тестирования наступает этап закрытия задачи: в задании на оказание услуг указывается дата начала и окончания работ, указывается перечень участников исполнителя, описываются результаты работ и критерии приемки работ, указываются трудозатраты, стоимость услуг. После согласования задания на оказание услуг заказчику выставляется счет за выполненные работы.

Заказчиком проекта обычно выступает руководитель одного из отделов компании, в интересах которого и реализуется проект. Как правило, решения, принимаемые в рамках одного проекта, могут влиять на другие проекты и процессы, протекающие в других отделах. Поэтому консультант учитывает взаимосвязи между процессами, протекающими в разных отделах, и обсуждения предлагаемого решения проводятся с руководителями различных бюро и отделов.

В рамках одного проекта выполняется множество задач, которые связаны и могут реализовываться параллельно друг с другом. Также консультант может заниматься несколькими задачами, относящимися к разным проектам. Каждой задаче выставляется своей приоритет, желаемые сроки реализации, которые зачастую не удается соблюдать из-за большого количества задач. Актуальным становится необходимость введения процесса администрирования проектов, что обеспечивает регулярный контроль работы над проектом, поддержание взаимодействия между консалтинговой компанией и заказчиком путем организации совещаний, ведение протоколов на совещании для фиксации обсуждаемых вопросов и принятых решений.

Заключение

В ходе исследования выявлены закономерности процесса управления проектами по внедрению корпоративной информационной системы, рассмотрен ход работы над проектом внедрения корпоративной информационной системы. Для повышения эффективности процессов работы консалтинговой компании определена актуальность и необходимость построения моделей, описывающих процесс администрирования проектов. Модели должны предусматривать варианты работы, отвечающие современным условиям как в режиме онлайн, так и в режиме офлайн. Предполагается, что администратор проекта обеспечит регулярный контроль работы над проектом на каждом этапе, назначая совещания с заказчиками, фиксируя принятые решения в протокол и дальнейшим согласованием, следя за соблюдением сроков исполнения и предоставляя отчетность руководителям.

СПИСОК ЛИТЕРАТУРЫ

1. Царев В. Е. Анализ видов управленческого консалтинга // Молодой ученый. — 2016. — № 7 (111). — С. 1029-1031.
2. Гюли Мухтарова. Внедрение ERP-систем. Основные ошибки // Директор-инфо. — 2018. — № 10 — С. 111-114.
3. Кривоносова, О. О. Аутсорсинг логистических функций провайдеру четвертого уровня как эффективный способ координации бизнес-процессов компании // Молодой ученый. — 2019. — № 4 (242). — С. 228-230.
4. Yana Bystrytska. Консалтинговые услуги – понятие, виды, преимущества // Компаньон Онлайн. — 2016. № 4. — С. 189-191.
5. Воронцова М. А. Маркетинговые коммуникации на рынке ИТ-консалтинга // Молодой ученый. — 2019. — № 5 (243). — С. 108-110.
6. Коптелов А.К. Зачем нужен ИТ-консалтинг // Корпоративное обучение в области ИТ. — 2016. — № 6 — С. 228-230.
7. Нестеренко, И. Н. Управленческий консалтинг: проблемы и перспективы развития на отечественном рынке // Молодой ученый. — 2019. — № 22 (260). — С. 560-562.
8. Хомутинникова К.С. Ключевые преимущества внешнего проектного офиса в развитии организационного управления проектами // Журнал о том, как управлять проектами, программами и портфелями проектов. — 2017. — № 11 — С. 307-310.
9. Холбутаева, Ш. А. Теоретико-методологический анализ консалтинга в современной экономической теории // Молодой ученый. — 2016. — № 11 (115). — С. 1052-1054.
10. Ишкина П. П. Рынок консалтинговых услуг по оптимизации производственных процессов: проблемы и особенности развития // Актуальные вопросы экономики и управления: материалы I Междунар. науч. конф., г. Москва, апрель 2011 г., 2011. С. 16-19.
11. Орлова Ю.А. Выбор и внедрение корпоративных систем // Организация внедрения корпоративных систем. — 2011. — № 7 — С. 102-104.

12. Bondaletov V.V., Medvedeva N.V., Senicheva L.V., Frolova E.V., Santos E. Local politics, business, people: issues and cooperation strategies // Journal of Advanced Research in Law and Economics. — 2014. — № 2. С. 63-73.
13. Ручкин А.В., Трофимова О.М. Управление проектами: Основные определения и подходы // Вопросы управления. 2017. №3 (46). URL: https://cyberleninka.ru/article/n/upravlenie-proektami-osnovnye-opredeleniya-i-podhody (дата обращения: 04.06.2021).
14. Сербская О.В. Современные методы управления проектами // Материалы Афанасьевских чтений. 2016. №2 (15). URL: https://cyberleninka.ru/article/n/sovremennye-metody-upravleniya-proektami (дата обращения: 09.05.2021).
15. Mudassir Iqbal. Organization Project Management (OPM – Project Management Seminars (PMP). 2018. [Электронный ресурс]. - https://mudassiriqbal.net/organizationprojectmanagement (дата обращения: 09.05.21)
16. https://www.iplc.ru/ru/

УДК 004.9

Р. Р. ЯЛИЛОВ
rmn.yalilov@gmail.com
Науч. руководитель – канд. техн. наук, доц. Н. Д. НАВАЛИХИНА

Уфимский государственный авиационный технический университет

ВЫБОР МЕТОДА МАШИННОГО ОБУЧЕНИЯ ДЛЯ ВЫЯВЛЕНИЯ СЕТЕВЫХ АТАК

Аннотация. В данной работе рассматривается использование машинного обучения для реагирования на атаки в компьютерных сетях, анализ сетевого трафика. Методом анализа иерархий осуществляется выбор алгоритма машинного обучения для анализа сетевого трафика.
***Ключевые слова*:** анализ сетевого трафика; машинное обучение, метод анализа иерархий.

В настоящее время в корпоративных компьютерных сетях существует необходимость обеспечения защиты информационных ресурсов от несанкционированного доступа. С каждым годом увеличивается объем сетевого трафика, а также размеры сетей и количество приложений. В результате огромное количество данных создается и передается в корпоративных сетях и за ее пределами. С ростом объемов передаваемой информации увеличивается и количество угроз безопасности, появляются новые способы атак.

Согласно ежегодной статистике Kaspersky Bulletin с 2019 г. по 2020 г. количество обнаруженных вредоносных объектов (скриптов, эксплоитов, исполняемых файлов и тд.) используемых в онлайн-атак выросло на 35,77%. [1]

Кроме вопросов безопасности существуют проблемы с производительностью и сбои в работе информационных систем, что оказывает значительное влияние на работу предприятий и бизнеса.

Традиционные методы выявления этих проблем, такие как сигнатурные методы, основанные на правилах и анализе статистики, становятся низко эффективными из-за сложности архитектурных решений современных систем и объема собираемой служебной информации. При большом объеме сетевого трафика обычные методы имеют проблемы с производительностью и масштабируемостью, кроме того они не могут самообучаться и находить новые атаки.

В данной работе рассматривается проблема анализа сетевого трафика с использованием машинного обучения (далее - ML). Машинное обучение является классом методов искусственного интеллекта (далее - ИИ) и нацелено на получение полезной информации из больших данных.

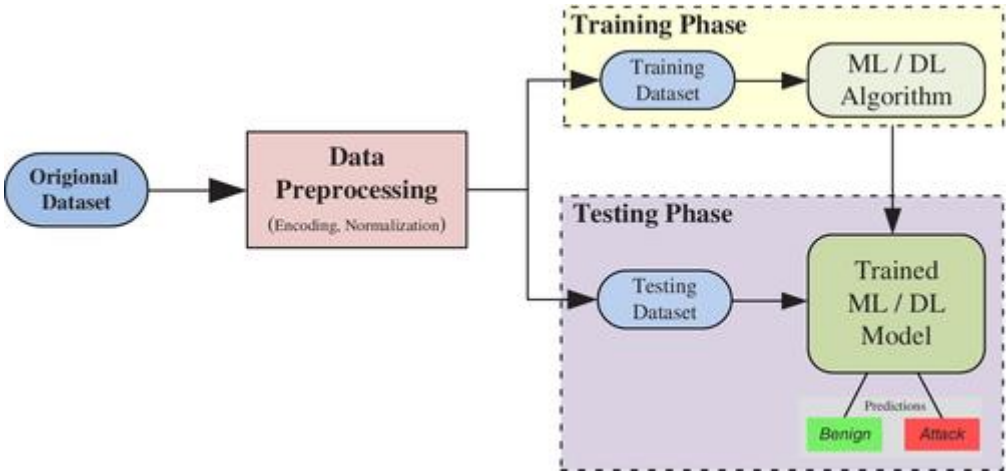


Рис. 1. Методология обнаружения атак с помощью машинного обучения, глубокого обучения

Общий подход к обнаружению аномальных данных в сетевом трафике содержит следующие этапы: этап предварительной обработки данных, этап обучения и этап тестирования. Для любого из методов ИИ требуется предварительная обработка данных, а именно нормализация и кодирование в подходящий для метода формат. Затем обработанные данные случайным образом разделяются на обучающих набор данных и тестируемый набор. [3] Алгоритм машинного обучения на следующем этапе проводит обучение с помощью первого набора. Время, затрачиваемое алгоритмом на обучение, зависит от размера набора данных и сложности предлагаемой модели. Как только модель обучена, она тестируется с использованием тестового набора данных и оценивается на основе сделанных ею прогнозов. В случае анализа сетевого трафика его экземпляр будет принадлежать либо к классу доброкачественных (нормальных), либо к классу атак.

Для анализа трафика в данный момент использую большое количество методов машинного обучения. Наиболее распространенными алгоритмами ма-

шинного обучения, являются: дерево принятия решений, метод k-ближайших соседей, искусственная нейронная сеть, машина опорных векторов, кластеризация K-средних, сеть быстрого обучения. В данном разделе статьи мы выберем наиболее эффективный метод с помощью оценки методом анализа иерархий.

Модель дерева принятия решений имеет обычную древовидную структуру с узлами, ветвями и листом. Каждый узел представляет атрибут или объект. Ветвь представляет решение или правило, в то время как каждый лист представляет возможный результат или метку класса. Алгоритм автоматически выбирает лучшие функции для построения дерева, а затем выполняет операцию обрезки, чтобы удалить ненужные ветви из дерева, чтобы избежать чрезмерной подгонки**.**

Метод k-ближайших, или kNN-классификации, является одним из самых изученных и высокоэффективны методов. На основании гипотезы классифицируемый объект относится к тому классу, к которому принадлежат k-ближайшие к нему объекты обучающей выборки.

Искусственные нейронные сети – системы, способные получать, хранить и использовать знания. Это совокупность искусственных нейронов. [6]

Метод машин опорных векторов – это класс методов машинного обучения может использоваться для решения задач классификации и для восстановления регрессии. Данный метод относится к категории универсальных сетей прямого распространения, как многослойный персептрон и сети на основе радиальных базисных функций. [7]

Кластеризация K-средних – это классический алгоритм, который находит центры масс кластеров, которые минимизируют расстояние между точками в евклидовом пространстве.

Для сравнения методов возьмем набор данных NSL-KDD, который эмулирует сетевую активность, и будем использовать метрики из данного набора данных. Набор данных от 2014 года NSL-KDD это пересмотренная и усовершенствованная версия набора данных KDD Cup'99, в которой устранены неко-

торые его проблемы, такие как повторения объектов. Этот набор данных содержит набор классов объектов с 41 сетевым параметром. Объекты разделены на четыре класса сетевых атак: DoS, U2R, R2L, Probe. [2]

Метрики из набора данных NSL-KDD будем использовать как критерии оценки для метода анализа иерархий. [4]

Погрешность: Определяется отношением правильно отсортированного трафика как положительный результат к общему количеству объектов являющихся положительными.

$$precision = \frac{TP}{TP+FP}. \quad (1)$$

Частота ложных срабатываний: Она также называется частотой ложных срабатываний и определяется как отношение неправильно предсказанных атак ко всем нормальным выборкам.

$$False\ Alarm\ Rate = \frac{FP}{FP+TN}. \quad (2)$$

Точность: Это отношение правильно классифицированных экземпляров к общему числу экземпляров. Это также называется точностью обнаружения и является полезным показателем производительности только в том случае, если набор данных сбалансирован.

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN}. \quad (3)$$

Скорость работы метода: Время затраченное на работу с набором данных, меньшее значение является лучшим.

На данном этапе решения проблемы методом анализа иерархий является формулирование и представление задачи. Для представления задачи используют иерархическую структуру. [5] Иерархическая структура образована посредством установления связи между целью, критериями оценивания и альтернативами – таблица 1.

Таблица 1

Уровни иерархий

1 уровень иерархии	Задача	Выбор метода ML для анализа сетевого трафика на предмет атак
2 уровень иерархии	Критерии оценивания	Погрешность, частота ложных срабатываний, точность, скорость работы метода
3 уровень иерархии	Альтернативы	Дерево принятия решений, метод k-ближайших соседей, искусственная нейронная сеть, машина опорных векторов, кластеризация K-средних, сеть быстрого обучения

После определения уровней и элементов иерархии критерии и альтернативы подлежат сравнению. Для этого строится шкала оценки предпочтений и матрица попарных сравнений – таблицы 2, 3.

Таблица 2

Шкала предпочтений

Степень важности	Определение	Описание
1	Равная значимость	Оба элемента имеют равный вес
3	Несильная значимость	Существует незначительный перевес в пользу одного элемента иерархии
5	Существенная значимость	Существует сильный перевес в пользу одного элемента иерархии
7	Очень сильная значимость	Существует явное превосходство одного элемента иерархии
9	Абсолютная значимость	Полное предпочтение одного варианта
2,4,5,6,8	Промежуточная значимость	Промежуточные значения веса

Таблица 3

Матрица попарных сравнений критериев

	Погрешность	Частота ложных срабатываний	Точность	Скорость работы метода
Погрешность	1	1/5	1/7	3
Частота ложных срабатываний	5	1	1/3	7
Точность	7	3	1	5
Скорость работы метода	1/3	1/7	1/5	1

Нормированный собственный вектор для матрицы попарных сравнений критериев: W=(0.123; 0.377; 0.453; 0.0474)

λ_{max}=4.795

$UC=\frac{4.795-4}{4-1}=0.265$

OC=0.265/0.9=0.294

Нормированный собственный вектор для матрицы парных сравнений «Погрешность»: W=(0.0712; 0.22; 0.236; 0.157; 0.118; 0.197)

λ_{max}=7.219

$UC=\frac{7.219-6}{6-1}=0.244$

OC=0.244/1.24=0.197

Нормированный собственный вектор для матрицы парных сравнений «Частота ложных срабатываний»: W=0.443; 0.0827; 0.0821; 0.17; 0.111; 0.111

λ_{max}=6.807

$UC=\frac{6.807-6}{6-1}=0.161$

OC=0.161/1.24=0.13

Нормированный собственный вектор для матрицы парных сравнений «Точность»: W=0.234; 0.117; 0.165; 0.248; 0.124; 0.11

λ_{max}=7.328

$UC=\frac{7.328-6}{6-1}=0.266$

OC=0.266/1.24=0.215

Нормированный собственный вектор для матрицы парных сравнений «Скорость работыметода»: W=0.245; 0.286; 0.0914; 0.163; 0.123; 0.0914

λ_{max}=6.707

$UC=\frac{6.707-6}{6-1}=0.141$

OC=0.141/1.24=0.114

Осуществляем иерархический синтез. Последовательно определяем век-

тора приоритетов альтернатив W_E^A относительно элементов E_j^i, находящихся на всех иерархических уровнях. Вычисление векторов приоритетов проводится в направлении от нижних уровней к верхним с учетом конкретных связей между элементами, принадлежащими различным уровням. Вычисление производится путем перемножения соответствующих векторов и матриц.

$$\begin{pmatrix} 0{,}0712 & 0{,}443 & 0{,}234 & 0{,}245 \\ 0{,}22 & 0{,}0827 & 0{,}117 & 0{,}286 \\ 0{,}236 & 0{,}0821 & 0{,}165 & 0{,}0914 \\ 0{,}157 & 0{,}17 & 0{,}248 & 0{,}163 \\ 0{,}118 & 0{,}111 & 0{,}124 & 0{,}123 \\ 0{,}197 & 0{,}111 & 0{,}11 & 0{,}0914 \end{pmatrix} \begin{pmatrix} 0{,}123 \\ 0{,}377 \\ 0{,}453 \\ 0{,}0474 \end{pmatrix} = \begin{pmatrix} 0{,}2933836 \\ 0{,}1247953 \\ 0{,}13905706 \\ 0{,}2034712 \\ 0{,}1183632 \\ 0{,}12024036 \end{pmatrix} \quad (4)$$

Максимальным элементом в матрице является 0.293. Следовательно, наиболее важным параметром при выборе будет являться Дерево принятия решений.

Исходя из критериев оценивания можно сделать вывод, что Дерево принятия решений показывает себя лучше остальных предложенных методов ИИ в совокупности по следующим показателям: погрешность, частота ложных срабатываний, точность и скорость работы метода.

Использование выбранного метода ИИ позволит решить поставленную проблему, а именно проводить анализ большого объема данных сетевой активности по сравнению с традиционными методами. Более того алгоритм дерева принятия решения предполагает выбор наилучшего решения по отношению к экземпляру трафика, уменьшив при этом количество ложных срабатываний и увеличив точность определения сетевых атак.

СПИСОК ЛИТЕРАТУРЫ

1. Kaspersky Security Bulletin 2020. Статистика [Электронный ресурс]: официальный сайт компании «Касперский». URL: https://go.kaspersky.com/rs/802-IJN-240/images/KSB_statistics_2020_ru.pdf (дата обращения: 23.09. 2021).
2. Кажемский М.А., Шелухин О.И. Многоклассовая классификация сетевых атак на информационные ресурсы методами машинного обучения // Труды учебных заведений связи. 2019. Т. 5. № 1. С. 107–115. DOI:10.31854/1813-324X-2019-5-1-107-115
3. Imamverdiyev Y, Abdullayeva F. Deep learning method for denial of service attack detection based on restricted Boltzmann machine. Big Data. 2018; 6(2): 159- 169.

4. Thomas R, Pavithran D. A survey of intrusion detection models based on NSL-KDD data set. Paper presented at: Proceedings of the 5th HCT Information Technology Trends (ITT). Dubai, United Arab Emirates: IEEE; 2018:286-291.
5. Саати, Т. Принятие решений. Метод анализа иерархий [Текст] / Пер. с англ. Р.Г.Вачнадзе - Москва «Радио и связь», 1993.
6. Васенков Д.В. Методы обучения искусственных нейронных сетей // КИО. 2007. №1. URL: https://cyberleninka.ru/article/n/metody-obucheniya-iskusstvennyh-neyronnyh-setey (дата обращения: 23.09.2021).
7. Китова О. В., Колмаков И.Б, Пеньков И.А.. "Метод машин опорных векторов для прогнозирования показателей инвестиций" Статистика и экономика, №. 4, стр. 27-30, 2016.

СЕКЦИЯ 5.2
МАТЕМАТИЧЕСКОЕ И ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

УДК 519

А. А. АХМАДУЛЛИН
akhmadullin.a@internet.ru
Науч. руководов. – д-р техн. наук, проф. Н. М. ШЕРЫХАЛИНА

Уфимский государственный авиационный технический университет

ЧИСЛЕННОЕ ИССЛЕДОВАНИЕ ИНТЕРПОЛЯЦИОННЫХ МЕТОДОВ

***Аннотация*.** В данной статье рассматриваются практические методы интерполяции и проводится численный эксперимент. В частности, сравниваются результаты, полученные различными методами интерполирования.
***Ключевые слова*:** интерполяция; численный метод; интерполяционный многочлен Лагранжа; интерполяционный многочлен Ньютона.

Интерполяция нам известна еще с древних времен. Ее использовали вавилонские и древнегреческие астрономы и математики. Описание линейной интерполяции можно найти в древнем китайском математическом тексте под названием «Девять глав математического искусства», датируемом с 200 г. до н.э. до 100 г. н.э. Дальнейшее развитие интерполяции обязано таким выдающимся математикам, как Ньютон, Лейбниц и Грегори. И их труды используются математиками всего мира до сих пор.

Сегодня у нас есть большой выбор различных методов интерполяции. К конкретным задачам мы можем выбрать тот способ решения, который лучше всего подходит. С появлением ЭВМ возникла потребность использовать численные методы решения задач интерполяции. Термин интерполяция — это отыскание промежуточных значений величины по некоторым известным ее значениям. В научных и инженерных расчетах довольно часто нужно оперировать наборами значений, полученных экспериментальным путем или методом случайной выборки. По этим наборам необходимо построить функцию, на которую могли бы с высокой точностью попадать другие получаемые значения. Такая задача называется аппроксимацией кривой. Интерполяцией называют

разновидность аппроксимации, при которой кривая построенной функции проходит точно через имеющиеся точки.

В данной работе мы рассмотрим интерполяционные формулы Лагранжа и Ньютона, а также проведем численный эксперимент.

Пусть некоторая функция $f(x)$ задана своими значениями $y_j=f(x_j)$ на дискретном множестве точек x_j, $j=0,..,m$. Требуется приближенно определить аналитический вид этой функции и тем самым получить возможность вычислить ее значения в промежуточных точках $x \in (x_j, x_{j+1})$. Интерполирующую функцию будем искать в виде алгебраического многочлена $P_n(x)=\sum_{i=0}^{n} a_i x^i$. Поскольку многочлен $P_n(x)$ в узловых точках должен совпадать с заданными значениями функции, то задача сводится к решению системы линейных алгебраических уравнений $\sum_{i=0}^{n} a_i x_j^i = y_j, \quad j=k,\ldots,k+n$ относительно неизвестных a_i.

Рассмотрим интерполяционный многочлен Лагранжа. Опубликован был данный полином Жозефом-Луи Лагранжем в своей работе в 1795 году. Решение системы можно представить в форме интерполяционного многочлена Лагранжа

$$P_n(x)=L_n(x)=\sum_{j=k}^{k+n} y_j \prod_{\substack{i=k \\ i\neq j}}^{k+n} \frac{x-x_i}{x_j-x_i} \qquad (1)$$

Но интерполяция по Лагранжу имеет один существенный недостаток, а именно: если необходимо получить $L_{n+1}(x)$, добавив к имеющимся узлам интерполяции узел x_{n+1}, все вычисления придется проводить заново. От этого недостатка избавлен интерполяционный многочлен в форме Ньютона.

Для нахождения интерполяционного многочлена в форме Ньютона введем обозначение $f_k=f(x_k)$. Выражение разделенной разности порядка n выглядит следующим образом $f(x_k, x_{k+1}, x_{k+n})=\sum_{j=k}^{k+n} f_j \left(\prod_{\substack{i=k \\ i\neq j}}^{k+n} (x_j - x_i) \right)^{-1}$. Интерполяционным многочленом Ньютона называется алгебраический многочлен

$$l_n(x) = f(x_k) + (x - x_k) f(x_k, x_{k+1}) + (x - x_k)(x - x_{k+1}) f(x_k, x_{k+1}, x_{k+2}) + \ldots$$
$$\ldots + (x - x_k)(x - x_{k+1}) \ldots (x - x_{k+n-1}) f(x_k, x_{k+1}, \ldots, x_{k+n}) \quad (2)$$

Этот многочлен тождественно равен многочлену степени n, записанному в форме Лагранжа или в какой-то другой форме в силу единственности интерполяционного многочлена.

Представим математическую модель погрешности интерполяции. Пусть имеются два набора узлов: $x_j^{(1)}$, $j=0,..,N_1$ и $x_j^{(2)}$, $j=0,..,N_2$ и два многочлена построенные на них. Тогда можно записать соответственно два выражения

$$P_n^{(1)}(x) - f(x) = c\prod_{j=k_1}^{k_1+n}\left(x - x_j^{(1)}\right) + \delta_1(x), \quad P_n^{(2)}(x) - f(x) = c\prod_{j=k_2}^{k_2+n}\left(x - x_j^{(2)}\right) + \delta_2(x). \quad (3)$$

Здесь с — величина предполагаемая независимой от положения узлов; k_1 и k_2 — номера начальных узлов, используемых интерполяционной формулой; $\delta_1(x)$ и $\delta_2(x)$ — малые величины по сравнению с первым слагаемым. Пренебрегая малыми решаем систему уравнений и находим оценку погрешности интерполяции. Обозначим $\Pi_i = \prod_{j=k_i}^{k_i+m}\left(x - x_j^{(i)}\right)$, тогда более точное значение функции $f(x) \approx \dfrac{P_n^{(1)}(x)\Pi_2 - P_n^{(2)}(x)\Pi_1}{\Pi_2 - \Pi_1}$. Рассмотрим случай, когда первый набор состоит из узлов с номерами от k до $k+n$, второй — с номерами от $k+1$ до $k+n+1$. Тогда

$$P_n^{(1)}(x) - f(x) \approx \frac{\left[P_n^{(2)}(x) - P_n^{(1)}(x)\right]\prod_{j=k}^{k+n}(x - x_j)}{\prod_{j=k+1}^{k+n+1}(x - x_j) - \prod_{j=k}^{k+n}(x - x_j)} = -\left[P_n^{(2)}(x) - P_n^{(1)}(x)\right]\frac{x - x_k}{x_{k+n+1} - x_k}. \quad (4)$$

$$f(x) \approx \frac{x_{k+n+1} - x}{x_{k+n+1} - x_k} P_n^{(1)}(x) + \frac{x - x_k}{x_{k+n+1} - x_k} P_n^{(2)}(x) = P_{n+1}(x). \quad (5)$$

Проведем численный эксперимент на конкретной задаче интерполяции.

Таблица 1

Интерполяция многочленом Лагранжа

n	$P_n(x)$	Δ_n	Δ_n^{exact}	k_Δ
1	0,997	1,56E-03	0,00157	-0,00554
2	0,986	1,48E-05	1,11E-05	0,247765
3	0,961	6,02E-06	6,07E-06	-0,008
4	0,924	1,34E-07	1,21E-07	0,096955
5	0,875	3,85E-08	3,88E-08	-0,00892
6	0,816	1,38E-09	1,31E-09	0,050273
7	0,746	2,95E-10	2,98E-10	-0,00953

n	$P_n(x)$	Δ_n	Δ_n^{exact}	k_Δ
8	0,666	1,48E-11	1,44E-11	0,666
9	0,579	2,47E-12	2,49E-12	0,579
10	0,484	1,64E-13	1,61E-13	0,484
11	0,383	2,09E-14	2,15E-14	0,383
12	0,277	1,89E-15	9,99E-16	0,277
13	0,168	4,50E-15	4,50E-15	0,168
14	0,056		-1,05E-14	0,056

Пусть $f(x)=\cos x$, $x_j=\frac{j}{m}\frac{\pi}{2}$, $y_j=f(x_j)$, $j=0,\ldots,m$, m=14. Величина $\Delta_n=|P_n(x)-P_{n+1}(x)|$ представляет собой погрешность интерполяции; Δ_n^{exact} — разность между интерполированным и точным значением; $k_\Delta=1-\Delta_n^{exact}/\Delta_n$ — имеет смысл коэффициента уточнения интерполированного значения. Для построения подобной таблицы с использованием формулы (4) возьмем два набора точек $x_j^{(1)}$ от 1 до n+1 и $x_j^{(2)}$ от 0 до n. Из таблиц 1 и 2 видно, что значения, полученные при помощи интерполяционного многочлена в форме Лагранжа и Ньютона, существенно не отличаются.

Таблица 2

Интерполяция многочленом Ньютона

n	$P_n(x)$	Δ_n	Δ_n^{exact}	k_Δ
1	0,997	1,56E-03	0,00157	-0,00554
2	0,986	1,48E-05	1,11E-05	0,247765
3	0,961	6,02E-06	6,07E-06	-0,008
4	0,924	1,34E-07	1,21E-07	0,096955
5	0,875	3,85E-08	3,88E-08	-0,00892
6	0,816	1,38E-09	1,31E-09	0,050273
7	0,746	2,95E-10	2,98E-10	-0,00953

n	$P_n(x)$	Δ_n	Δ_n^{exact}	k_Δ
8	0,666	1,48E-11	1,44E-11	0,666
9	0,579	2,47E-12	2,49E-12	0,579
10	0,484	1,64E-13	1,61E-13	0,484
11	0,383	2,13E-14	2,17E-14	0,383
12	0,277	1,33E-15	1,22E-15	0,277
13	0,168	0	6,38E-16	0,168
14	0,056		1,80E-14	0,056

Таблица 3

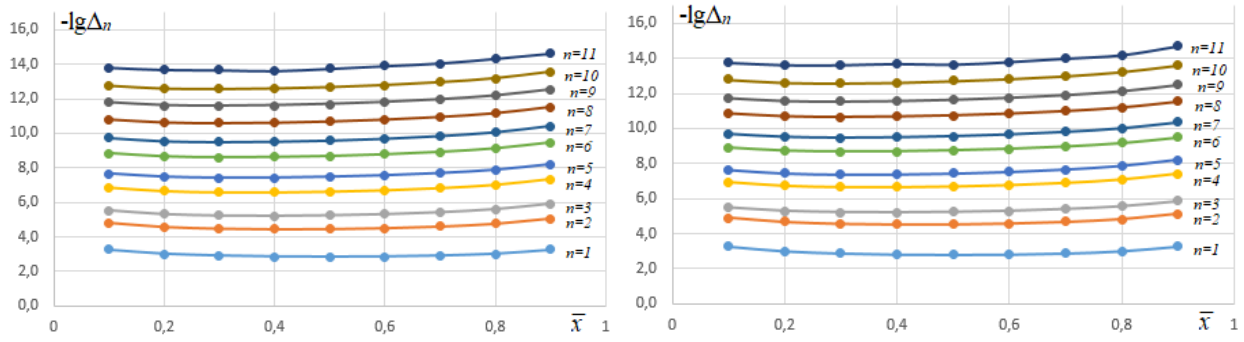
Интерполяция многочленом Лагранжа с двумя наборами точек

n	$P_n(x)$	Δ_n	Δ_n^{exact}	k_Δ
1	0,998	1,48E-05	8,65E-06	0,414343
2	0,986	3,61E-06	3,66E-06	-0,01229
3	0,961	5,75E-08	4,82E-08	0,162379
4	0,924	1,28E-08	1,30E-08	-0,01431
5	0,875	3,75E-10	3,43E-10	0,084261
6	0,816	6,81E-11	6,91E-11	-0,01554
7	0,746	2,96E-12	2,81E-12	0,050146

n	$P_n(x)$	Δ_n	Δ_n^{exact}	k_Δ
8	0,666	4,36E-13	4,43E-13	-0,017
9	0,579	2,59E-14	2,50E-14	0,034
10	0,484	2,94E-15	2,61E-15	0,113
11	0,383	3,33E-16	4,44E-16	-0,333
12	0,277	4,44E-16	3,89E-16	0,125
13	0,168		1,94E-15	
13	0,056		8,20E-15	

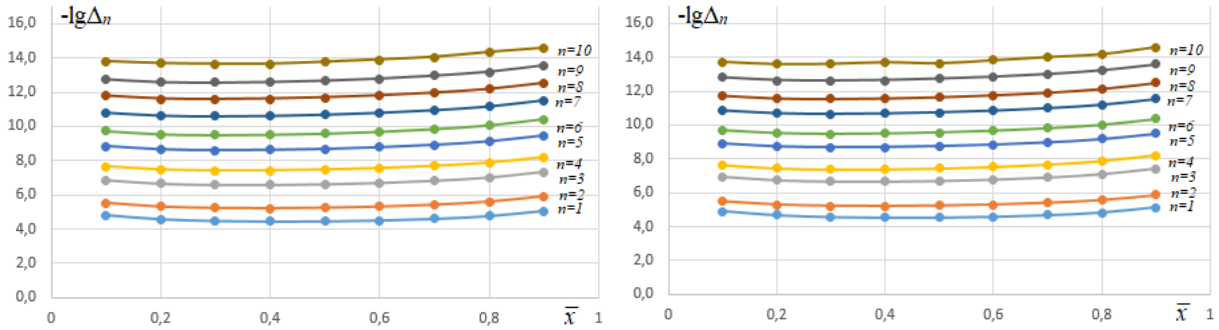
Из таблицы 3 видно, что интерполяция при помощи интерполяционного многочлена Лагранжа с двумя наборами точек ускорило уточнение значения.

Результаты интерполяции и оценки погрешности удобно представлять на графике в виде зависимости $-\lg\Delta_n$ от $\bar{x}=(x-x_j)/(x_{j+1}-x_j)$, $x\in(x_j, x_{j+1})$. На рис.1-2 разные кривые соответствуют различным n (при j=2). Попарное сближение кривых объясняется тем, что функция *cos x* — четная, и в ее разложении по степеням x присутствуют только четные члены. На рис. 1,б и 2,б изображены кривые, аналогичные проведенным на рис. 1,а и рис. 2,а соответственно, только для оценки погрешности использованы точные значения функции *cos x*. Также видно, что кривые на рис. 2 соответствуют кривым на рис.1 при n+1.



а *б*

Рис. 1. Результаты интерполяции при помощи интерполяционного многочлена в форме Лагранжа:
а – $\Delta_n=|P_n(x)-P_{n+1}(x)|$; *б* – $\Delta_n=|P_n(x)-f(x)|$



а *б*

Рис. 2. Результаты интерполяции при помощи интерполяционного многочлена в форме Ньютона с двумя наборами точек: *а* – $\Delta_n=|P_{n+1}(x)-P_{n+2}(x)|$; *б* – $\Delta_n=|P_{n+1}(x)-f(x)|$

Таким образом, после проведения численного эксперимента можно сказать, что результаты интерполяции с помощью интерполяционных многочленов в форме Лагранжа и Ньютона не имеют существенных различий по точности. А при формировании двух наборов из n точек из одного набора данных можно получить интерполяционный многочлен n+1 степени, который используется для оценки погрешности многочлена степени n. Незначительное отличие графиков рис.1, а, б и рис.2, а, б говорит о высокой точности оценки погрешности интерполяции.

СПИСОК ЛИТЕРАТУРЫ

1. Житников В. П., Шерыхалина Н. М., Поречный С. С., Зарипов А. А. Исследование свойств численных методов с помощью вычислительного эксперимента: учеб. пособие // Уфимск. гос. авиац. техн. ун-т. – Уфа : РИК УГАТУ, 2019. – 287 с.

УДК 336.767+004.428.4

Э. Ф. БАДРЕТДИНОВА
badretdinova.elnara@mail.ru
Науч. руководв. – канд. физ.-мат. наук, доц. Е. И. ПРОКУДИНА

Уфимский государственный авиационный технический университет

МАТЕМАТИЧЕСКОЕ И ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ЗАДАЧИ ВЫБОРА ПАЕВОГО ИНВЕСТИЦИОННОГО ФОНДА

***Аннотация*.** Разработан алгоритм расчета мер риска и мер доходности, с помощью которого можно выбирать наиболее подходящий по стратегии для инвестора объект для инвестирования среди паевых инвестиционных фондов, а также программное обеспечение, решающее задачу выбора паевого инвестиционного фонда с учетом оценок риска и доходности.
***Ключевые слова*:** задача выбора паевого инвестиционного фонда; мера риска; мера доходности; эмпирический закон распределения; инвестирование.

Актуальность темы, рассматриваемой в статье, обусловлена тем, что паевые инвестиционные фонды - доступный и эффективный инструмент для инвестирования, не требующий большого стартового капитала. Также такой объект инвестирования является удобным для начинающих инвесторов, которые еще не совсем понимают, в какие секторы предпочтительней направлять инвестиции и как собрать диверсифицированный портфель активов. Стоит отметить, что инвестиции всегда влекут за собой определенные риски, которые несомненно стоит учитывать, чтобы снизить и исключить вероятность потери денежных средств, которые были вложены в эти инвестиции.

Конечно же, каждый инвестор, вкладывая деньги в паевые инвестиционные фонды, желает получить доход, поэтому при выборе объекта для инвестирования важно учитывать и доходность.

Целью работы является разработка ПО, упрощающего задачу выбора объекта для инвестирования среди паевых инвестиционных фондов.

Пусть задано множество из N ПИФов и временные ряды ежедневных доходностей паев ПИФов. Необходимо построить рейтинг данных ПИФов, выбрать наилучший из них в качестве объекта для инвестирования.

Для решения задачи был разработан следующий алгоритм:

Дано: Временные ряды ежедневных доходностей паев ПИФов.

1. Построить эмпирический закон распределения случайной величины X_i – ежедневной доходности пая i-го ПИФа $i=\overline{1,N}$.

2. Оценить риск вложения средств в пай i-го ПИФа на основе меры риска $V_r(X_i)$. [3]

3. Оценить доходность вложения средств в пай i-го ПИФа на основе меры доходности $V_d(X_i)$.

4. Построить рейтинг ПИФов в соответствии с:

– мерой риска

– мерой доходности

– критерием $V(X_i)= \alpha V_r(X_i)-(1-\alpha)V_d(X_i)$, $0 \le \alpha \le 1$

Необходимо построить эмпирический закон распределения:

Пусть задан временной ряд доходностей паев ПИФов.

Найдем числа x_{min} и x_{max}. Возьмем общий интервал $[x_{min}, x_{max}]$.

Интервал делим на k равных частичных интервалов. Длина каждого частичного интервала:

$$h = \frac{x_{min} - x_{max}}{k}$$

Приблизительно число интервалов k можно оценить по формуле Стерже-са:

$$k = 1 + 3{,}322 \cdot \lg n$$

Для вычисления относительных частот подсчитаем n_i количество чисел заданного массива, попавших в i-ый интервал.

Относительная частота w_i:

$$w_i = \frac{n_i}{n}$$

Каждый интервал будет представлять значение его середины x_i'.

Таким образом, полагаем, что случайная величина X принимает значения x_1', …, x_i', с соответствующими вероятностями w_1, …, w_i.

После нахождения эмпирического закона распределения можно приступить к нахождению значений мер риска и критерия доходности.

Необходимо вычислить следующие меры риска, которые для решения задачи выбора паевого инвестиционного фонда будет нужно минимизировать, так как чем ниже риски, тем выгоднее инвестиции: [1]

– Дисперсия:

$$DX = E((X - EX)^2)$$

– Среднеквадратическое отклонение:

$$\sigma = \sqrt{DX}$$

– Левосторонний момент второго порядка:

$$M = E((max\{EX - X, 0\})^2)$$

– Стандартный левосторонний момент:

$$M = \sqrt{E((max\{EX - X, 0\})^2)}$$

– VaR (ValueatRisk):

$$VaR_\alpha X = min\{x | P(X \leq x) \geq \alpha\}, \alpha \to 1 \quad [2]$$

– CVaR (ConditionalValueatRisk):

$$CVaR_\alpha X = E(x | X > VaR_\alpha x), \alpha \to 1 \text{ [4]}$$

Необходимо вычислить следующие критерии доходности, которые для решения задачи выбора паевого инвестиционного фонда нужно будет максимизировать, так как чем выше доходность, тем выгоднее инвестиции:

– Математическое ожидание:

$$EX = \sum_{i=1}^{N} p_i \cdot x_i$$

– Ожидаемая полезность:

$$V(X_i) = E(u(X_i)),$$

$$u(x) = \begin{cases} x^\alpha, x \geq 0 \\ -\lambda \cdot |x|^\alpha, x < 0 \end{cases}, \alpha > 0, 0 < \alpha < 1$$

– Взвешенная полезность:

$$V(X_i) = \frac{Ew(X_i)}{Ev(X_i)},$$

где *w(x)* и *v(x)* - некоторые функции, для которых выполняются условия: w'>0, w"<0, v'<0, w">0.

– Ранговая полезность:

$$V(X_i) = \sum_{j=1}^{m} u(x_{ij}) \left(g\left(\sum_{k=1}^{j} p_{ik} \right) - g\left(\sum_{k=1}^{j-1} p_{ik} \right) \right)$$

$$g(x) = 1 - \frac{(1-x)^{\gamma}}{\sqrt[\gamma]{x^{\gamma} + (1-x)^{\gamma}}}, \text{ где } 0.56 < \gamma < 0.75$$

$$u(x) = \begin{cases} x^{\alpha}, x \geq 0 \\ -\lambda \cdot |x|^{\alpha}, x < 0 \end{cases}$$

Для решения задачи выбора паевого инвестиционного фонда было разработано ПО с интерфейсом, представленным на рисунках 1-3. Исходными данными для примера являются ПИФы акций Сбербанка, Райффайзен, Газпромбанка, ВТБ, Арсагера (1.05.2021-31.05.2021)

Процесс вычисления закончен!
Можно ознакомиться с результатами

Загрузите файлы: Выберите файл Файл не выбран
Загруженные файлы:

Номер: 1 Имя файла: сбербанк – фонд акций добрыня никитич.csv Удалить	**Номер: 2** Имя файла: райффайзен - акции.csv Удалить	**Номер: 3** Имя файла: опиф акций «газпромбанк - акции».csv Удалить	**Номер: 4** Имя файла: втб — фонд акций.csv Удалить	**Номер: 5** Имя файла: арсагера - фонд акций.csv Удалить

Расчёт

Таблица полученных данных;
Нажмите на интересующий параметр для сортировки:

	Дисперсия	Среднеквадратическое отклонение	Стандартный левосторонний момент второго порядка	Value at risk (α = 0.8)	Conditional value at risk	Математическое ожидание	Ожидаемая полезность	Взвешенная полезность	Ранговая полезность	Риск - Доходность
сбербанк – фонд акций добрыня никитич.csv	0.334	0.578	0.429	0.050	1.362	0.261	0.070	0.003	-0.305	0.551
райффайзен - акции.csv	0.642	0.801	0.478	0.094	0.958	0.230	-0.178	0.002	-0.422	0.364
опиф акций «газпромбанк - акции».csv	0.481	0.693	0.520	0.498	1.126	0.262	0.160	0.003	-0.331	0.432
втб — фонд акций.csv	0.186	0.431	0.361	0.035	0.807	0.249	0.244	0.002	-0.203	0.279
арсагера - фонд акций.csv	0.361	0.601	0.446	0.115	0.880	0.176	-0.101	0.002	-0.489	0.352

Рис. 1. Интерфейс ПО

	Дисперсия	Среднеквадратическое отклонение	Стандартный левосторонний момент второго порядка	Value at risk (α = 0.8)	Conditional value at risk	Математическое ожидание	Ожидаемая полезность	Взвешенная полезность	Ранговая полезность	Риск - Доходность
втб — фонд акций.csv	0.186	0.431	0.361	0.035	0.807	0.249	0.244	0.002	-0.203	0.279
сбербанк – фонд акций добрыня никитич.csv	0.334	0.578	0.429	0.050	1.362	0.261	0.070	0.003	-0.305	0.551
арсагера - фонд акций.csv	0.361	0.601	0.446	0.115	0.880	0.176	-0.101	0.002	-0.489	0.352
опиф акций «газпромбанк - акции».csv	0.481	0.693	0.520	0.498	1.126	0.262	0.160	0.003	-0.331	0.432
райффайзен - акции.csv	0.642	0.801	0.478	0.094	0.958	0.230	-0.178	0.002	-0.422	0.364

Рис. 2. Пример построения рейтинга по дисперсии

Для проведения вычислительного эксперимента были взяты данные о ПИФах банка ВТБ за период времени с 11 мая по 11 июня 2021 года.

	Дисперсия	Среднеквадратическое отклонение	Стандартный левосторонний момент второго порядка	Value at risk (α = 0.8)	Conditional value at risk	Математическое ожидание	Ожидаемая полезность	Взвешенная полезность	Ранговая полезность	Риск - Доходность
11.05-11.06. втб — фонд акций.csv	0.222	0.471	0.346	0.037	0.615	0.171	0.039	0.002	-0.325	0.222
11.05-11.06. втб – фонд еврооблигаций.csv	0.083	0.288	0.213	0.264	0.562	-0.095	-0.456	-0.001	-0.639	0.329
11.05-11.06. втб — фонд металлургии.csv	0.445	0.667	0.477	0.248	0.963	0.089	-0.220	0.001	-0.584	0.437
11.05-11.06. втб — фонд перспективных инвестиций.csv	0.284	0.533	0.387	0.238	0.833	0.026	-0.251	0.000	-0.577	0.404
11.05-11.06. втб — фонд потребительского сектора.csv	0.910	0.954	0.747	0.819	2.122	0.085	-0.085	0.001	-0.699	1.018
11.05-11.06. втб — фонд предприятий с государственным участием.csv	0.209	0.457	0.327	0.199	0.752	0.185	0.092	0.002	-0.299	0.284
11.05-11.06. втб — фонд электроэнергетики .csv	0.172	0.414	0.289	0.079	0.660	0.080	-0.179	0.001	-0.431	0.290

Рис. 3. Данные о ПИФах ВТБ с 11 мая по 11 июня 2021 года

Также были взяты исходные данные о тех же ПИФах, но уже за период времени с 18 мая по 18 июня 2021 года.

	Дисперсия	Среднеквадратическое отклонение	Стандартный левосторонний момент второго порядка	Value at risk (α = 0.8)	Conditional value at risk	Математическое ожидание	Ожидаемая полезность	Взвешенная полезность	Ранговая полезность	Риск - Доходность
18.05-18.06. втб — фонд акций.csv	0.276	0.526	0.373	0.422	0.807	0.080	-0.171	0.001	-0.475	0.364
18.05-18.06. втб – фонд еврооблигаций.csv	0.282	0.531	0.375	0.635	1.032	0.020	-0.287	0.000	-0.583	0.506
18.05-18.06. втб — фонд металлургии.csv	0.675	0.821	0.592	0.662	1.406	-0.119	-0.596	-0.001	-0.928	0.763
18.05-18.06. втб — фонд перспективных инвестиций.csv	0.515	0.718	0.558	0.615	1.242	0.059	-0.228	0.001	-0.693	0.591
18.05-18.06. втб — фонд потребительского сектора.csv	0.111	0.333	0.254	0.189	0.592	-0.026	-0.208	0.000	-0.499	0.309
18.05-18.06. втб — фонд предприятий с государственным участием.csv	0.260	0.509	0.384	0.199	0.813	0.169	0.090	0.002	-0.341	0.322
18.05-18.06. втб — фонд электроэнергетики.csv	0.213	0.462	0.318	0.427	0.776	0.012	-0.341	0.000	-0.558	0.382

Рис. 4. Данные о ПИФах ВТБ с 18 мая по 18 июня 2021 года

ПИФ	Дисперсия		Среднеквадратическое отклонение		Стандартный левосторонний момент 2-го порядка		Value at Risk		Conditional Value at Risk		Математическое ожидание		Ожидаемая полезность		Взвешенная полезность		Ранговая полезность		Риск - Доходность	
	11.05-11.06	18.05-18.06	11.05-11.06	18.05-18.06	11.05-11.06	18.05-18.06	11.05-11.06	18.05-18.06	11.05-11.06	18.05-18.06	11.05-11.06	18.05-18.06	11.05-11.06	18.05-18.06	11.05-11.06	18.05-18.06	11.05-11.06	18.05-18.06	11.05-11.06	18.05-18.06
втб — фонд акций	4	4	4	4	4	3	1	3	2	3	2	2	2	2	1	2	2	2	1	3
втб – фонд еврооблигаций	1	1	1	1	1	1	6	1	1	1	7	6	7	3	4	3	6	3	4	1
втб — фонд металлургии	6	7	6	7	6	7	5	7	6	7	5	7	5	7	2	4	5	7	6	7
втб — фонд перспективных инвестиций	5	5	5	5	5	4	4	6	5	5	6	4	6	5	3	3	4	5	5	5
втб — фонд потребительского сектора	7	6	7	6	7	6	7	5	7	6	3	3	3	4	2	2	7	6	7	6
втб — фонд предприятий с государственным участием	3	3	3	3	3	5	3	2	4	4	1	1	1	1	1	1	1	1	2	2
втб — фонд электроэнергетики	2	2	2	2	2	2	2	4	3	2	4	5	4	6	2	3	3	4	3	4

Рис. 5. Сравнение полученных рейтингов ПИФов
за рассматриваемые периоды времени

Сравнивая два полученных рейтинга, можно отметить, что даже за такой небольшой промежуток времени в рейтинге произошли изменения. Это доказывает то, что инвестору важно оценивать риск и доходность для верного распределения инвестиций.

Можно сделать вывод, что паевые инвестиционные фонды действительно удобный инструмент для инвестирования, но при покупке паев ПИФов необходимо отталкиваться от значений мер риска и мер доходности, это поможет не только сохранить капитал инвестора, но и преумножить его.

СПИСОК ЛИТЕРАТУРЫ

1.Шоломицкий А. Г. Теория риска //Выбор при неопределенности и моделирование риска. М.: Издательский дом ГУ ВШЭ. – 2005.
2.Киселева И. А. VaR-модели оценки инвестиционных рисков //Иннов: электронный научный журнал. – 2017. – №. 1 (30).
3.Лосик А. Г. Оценка инвестиционных рисков на рынке ценных бумаг. – 2019.
4.Бозняков А. В. Управление рисками инвестиций с использованием методогии CVaR. – 2017.

УДК 004.021

А. И. БАСЫРОВ
bruder.ocn@gmail.com
Науч. руководитель – канд. физ.-мат. наук, доц. Р. П. АБДРАХМАНОВА

Уфимский государственный авиационный технический университет

МАТЕМАТИЧЕСКОЕ И ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ РАЗРАБОТКИ ПРОЦЕДУРНОЙ ГЕНЕРАЦИИ КОНТЕНТА

Аннотация. В статье рассматривается задача процедурной генерации контента. Предложены математические методы решения поставленной задачи. Разработан алгоритм на основе предложенных методов. Описано разработанное ПО.
***Ключевые слова*:** BSP-деревья; автоматизация контента; сбалансированное дерево; процедурная генерация; двоичное разбиение пространства.

Под процедурной генерацией контента (ПГК) понимают автоматизацию и полуавтоматизацию создания и динамические изменения различных составляющих видеоигр, таких как: изменение игровых правил, объектов, уровней и окружения, двумерной или трехмерной графики, персонажей, звуков, музыки и др.

Основной проблемой алгоритмов ПГК является генерация игровых правил. Процедурная генерация игровых правил позволит существенно разнообразить видеоигры за счет динамического изменения правил в процессе игры (адаптируясь под желания игрока), а также создать абсолютно новые игровые механики и жанры. Разработка языка описания игр является теоретически значимой, т. к. результатом будет строго научно-теоретический аппарат, который позволит формализировать и описать возможные пространства игровых правил. Помимо этого, алгоритмы генерации могут быть полезны дизайнерам игрового контента для быстрого создания и тестирования различных игровых прототипов.

Из вышеизложенного следует актуальность данной темы. Данная работа анализирует математический подход к созданию программного обеспечения разработки процедурной генерации виртуальных пространств, а в частности игровых уровней.

Целью данной работы является повышение эффективности разработки видеоигр путем создания математического и программного обеспечения разработки процедурной генерации контента (ПГК). Это позволит автоматизировать создание видеоигр и *сэкономить средства* на их производстве, в частности снижая стоимость на разработку контента для игр, решая *проблемы однообразия* и *персонализации*, приобретающие большую значимость в связи с ростом количества потенциальных игроков.

При анализе существующих алгоритмов процедурной генерации были рассмотрены наиболее популярные алгоритмы генерации:

– *Алгоритм на основе BSP-дерева*

– *Алгоритм туннелирования*

– *Клеточные автоматы*

Рассмотрим только первые два алгоритма

1. *Алгоритм на основе BSP-дерева*

Данный алгоритм имеет *рекурсивную* структуру, но также может быть реализован в *итеративном* виде.

Метод рекурсивного разбиения пространства в выпуклые множества. В результате объекты будут представлены в виде структуры данных, называемой BSP-деревом [1].

Первоначально прямоугольный уровень заполнен стенами. Происходит разделение всей области уровня на две подобласти. Случайным образом выбирается сначала направление деления (вертикальное или горизонтальное), затем координата деления. Получается две области меньшего размера [2].

В процессе разделения областей на подобласти строится двоичное дерево, благодаря которому алгоритм носит свое название. Каждая вершина дерева хранит информацию о данной области (например, записаны координаты верхнего левого угла, ширина и высота области) и ссылки на двух потомков – если есть подобласти – или же ссылки пустые, то есть данная подобласть конечная. Корень дерева задает область всего уровня.

Таким образом наша область будет иметь вид, изображенный на рисунке 1.

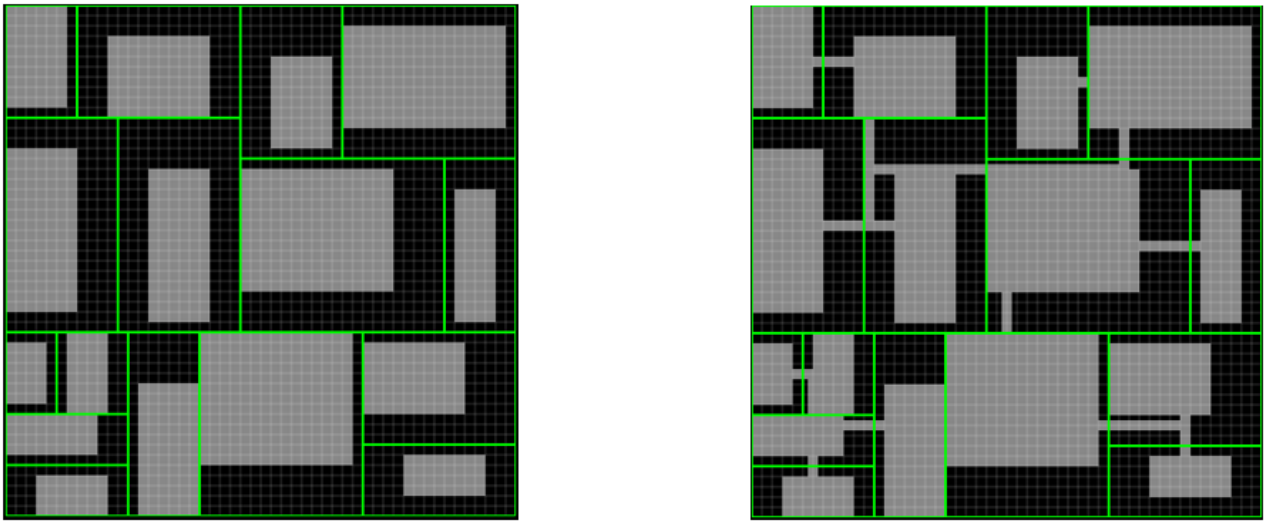


Рис. 1. Сгенерированная область и процесс соединения комнат

В зависимости от требований, выдвинутых игровому проекту, результат данного алгоритма может быть либо желаемым, либо не подходящим.

2. Алгоритм туннелирования

Данный алгоритм является чем-то вроде «игрового червя», прокапывающего в заполненной стенами области коридор и комнаты, как если бы их делал настоящий архитектор подземелий [4]. Но недостатком данного алгоритма является то, что зачастую генерируются бесполезные и излишние пути.

Особенность данного подхода заключается в том, что на каждой итерации шагов любого из червей, есть шанс создать в текущих координатах нового червя. При этом если червей стало больше одного, то у каждого из них, есть шанс удалить себя из списка цикла прохождения алгоритма. Таким образом появляются вторичные пути ведущие в тупики. Из этого следует, что в выделенной области будет один основной путь и ряд вторичных ответвлений (Рисунок 2).

Алгоритм продолжает работу, пока не будет достигнут размер задаваемой площади.

Рис. 2. Результат построенной области алгоритма туннелирования

Содержательная постановка задачи

Актуальность видеоигр растет с каждым годом, а вместе с этим изменяются интересы игроков. Компании по разработке игр заинтересованы в экономии средств путем возможной автоматизации некоторых процессов производства, и в реиграбельности разработанных проектов. Благодаря этому можно сформулировать две основные проблемы данной предметной области: автоматизация создания процедурной генерации виртуальных пространств, а в частности игровых уровней; реиграбельность создаваемых проектов.

Игры, хоть и используют процедурную генерацию для какого-либо игрового контента, но все равно имеют заранее предустановленные правила игры. Поэтому было сформировано решение разработать алгоритм процедурной генерации контента с использованием *двоичного разделения пространства* (BSP – деревом), который бы создавал игровой контент и правила, основываясь исключительно на действиях алгоритма, добавляя игре абсолютно уникальный игровой опыт и реиграбельность.

Формальная постановка задачи

Формальной постановке задачи соответствует контекстная диаграмма функциональной модели IDEF-0 (Рисунок 3).

Рис. 3. Нотация IDEF0

В соответствии с вышеприведенной схемой опишем входные данные:

А) Размеры игровой локации и комнат: параметры ширины и высоты комнат и общей локации, где будут создаваться комнаты.

Б) Игровые объекты: Любой игровой контент: персонажи, объекты, предметы и т. д.

В) Тип генерации: заранее подготовленный тип генерации (комнаты будут иметь геометрическую примитиву, либо комнаты будут создаваться абсолютно случайной формой), содержащий в себе количество итераций для прохождения робота-агента, а также длина пути, которую он должен пройти.

На рисунке 4 изображена декомпозиция диаграммы IDEF0

Рис. 4. Декомпозиция диаграммы

Исходя из вышеизложенного, сформулируем *математическую постановку задачи:*

Дано:

Размер области **W** x **H**, где W – ширина заданной области, а **H** – высота. Максимальный размер каждой комнаты – (**W**-2) x (**H**-2). Количество итераций прохода робота агента – **It.**

Необходимо:

– Найти количество подобластей множества **D** = <d_1, d_2, … , d_i, … , d_n > разделенной области W x H.

– Построить комнаты при числе итераций прохождения агента равном **It.**

– Найти центры комнат **Room(C)** в подобластях

– Соединить комнаты коридорами.

Определение количества подобластей множества и нахождение центров комнат

Пусть верхний левый угол области начинается с X_0 и Y_0, а ее размеры W x H клеток. Получены размеры комнат A x B, при этом 1 ⩽ A ⩽(W-2), 1 ⩽B ⩽(H-2). Тогда координаты X_1, Y_1 верхнего угла будут заданы случайным образом в

диапазоне от X_0 + 1 до X_0 + W – A – 1, а Y_1 – в диапазоне от Y_0 + 1 до Y_0 + H – B – 1.

Возьмем высоту комнаты Hi и ширину комнаты Wi из множества комнат Room = < r_1, r_2, … , r_i, … r_n >. Рассчитаем H_i /2 и W_i/2 - центры каждой комнаты. Обозначим координаты центра комнаты C_i , тогда Room(C_i)- множество центров комнат.

Алгоритм соединения комнат

1. Начать работу с промежуточным множеством Room(C_i)

2. Обозначить текущий центр комнаты currentC. Тогда для каждого currentC из Room(C_i):

1) Обозначить текущее минимальное расстояние minDist = бесконечности (условно большое значение).

2) Обозначить текущую ближайшую комнату как ClosestRoom.

3. Для каждого центра комнат C из Room(C_i)

1) Обозначить currentDist как расстояние от текущей комнаты до ближайшего центра комнаты.

2) Найдем расстояние currentDist между currentC и C с помощью формулы расстояния между двумя точками: currentDist = $\sqrt{(X_1 - X_2)^2 + (Y_1 - Y_2)^2}$, где X_1, X_2 и Y_1, Y_2 координаты центров комнат.

3) Если текущее расстояние currentDist меньше минимального minDist, то:

– Минимальное расстояние приравниваем текущему.

– Текущий центр комнаты будет равен ближайшей комнате ClosestRoom = C

4. Провести коридор между CurrentC и ClosestRoom

Таким образом, алгоритм процедурно генерирует игровое пространство с подобластями для игровых комнат, соединяя каждую комнату, созданную в игровой области коридорами, выходящими из центров каждой ближайшей комнаты.

Математическая постановка задачи двоичного разбиения пространства

Рассмотрим алгоритм двоичного разбиения пространства на основе «BSP-дерева»

1) Ввести параметры

2) Если заданное множество полигонов пустое, то закончить алгоритм

3) Для заданного множества полигонов S выбрать разбивающую плоскость L.

4) Рассечь все полигоны, пересекающиеся с L.

5) Отнести все полигоны, находящиеся с фронтальной стороны L, к фронтальному поддереву F, а все полигоны, находящиеся с обратной стороны L, к оборотному поддереву B

6) Выполнить алгоритм рекурсивно для множества полигонов фронтального поддерева F

7) Выполнить алгоритм рекурсивно для множества полигонов оборотного поддерева B.

– Разбивающая плоскость выбирается таким образом, чтобы сбалансировать дерево, то есть чтобы число полигонов во фронтальном и оборотном поддереве было приблизительно одинаково:

– $\min(|N(F_i) — N(B_i)|)$

– где $N(F_i)$ — число полигонов с фронтальной стороны некоторой разбивающей плоскости i, $N(B_i)$ — число полигонов с оборотной стороны разбивающей плоскости i.

Алгоритм, описывающий использование BSP-дерева представлен на рис. 5.

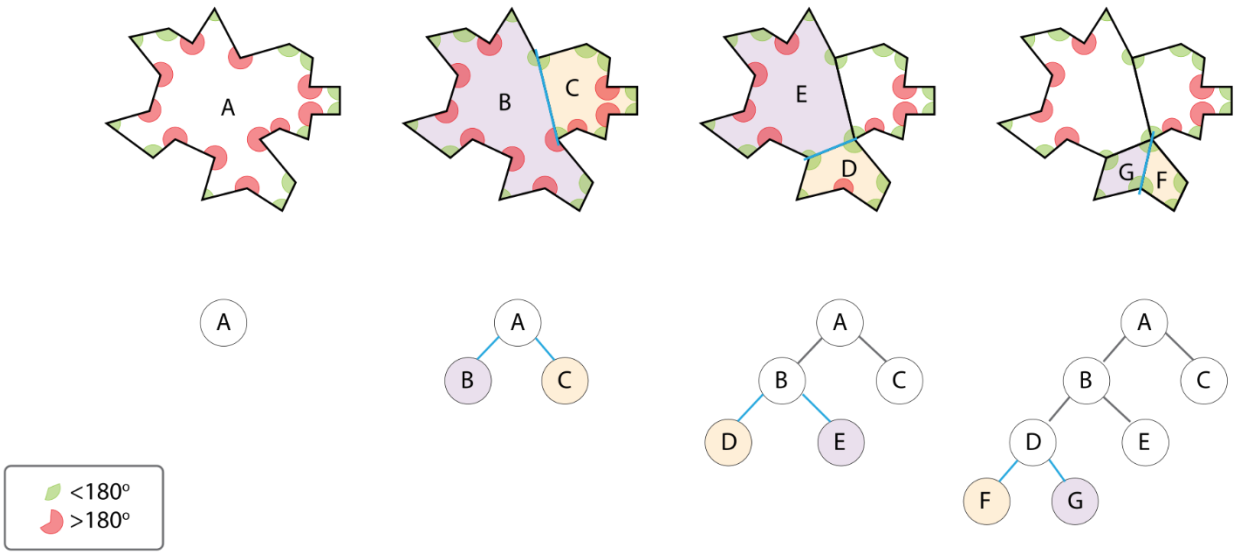


Рис. 5. Пример построения BSP-дерева

Размер BSP-дерева равен суммарному размеру множеств во всех узлах. Другими словами, размер BSP-дерева — число фрагментов, на которые были разбиты объекты. Так как BSP-дерево не содержит бесполезные прямые (прямые, которые разбивают пустую грань), то количество узлов пропорционально размеру дерева.

В результате проведенной работы было разработано ПО на языке C#, выполняющее следующие функции:

1) Генерация комнат с помощью алгоритмов ПГК

2) Изменение размеры комнаты и всего этажа

3) Настройка поля зрения камеры

4) Изменение типа генерации контента (на абсолютно случайные вариации сгенерированной комнаты)

5) Задание отступа между комнатами

6) Переход к процессу игры

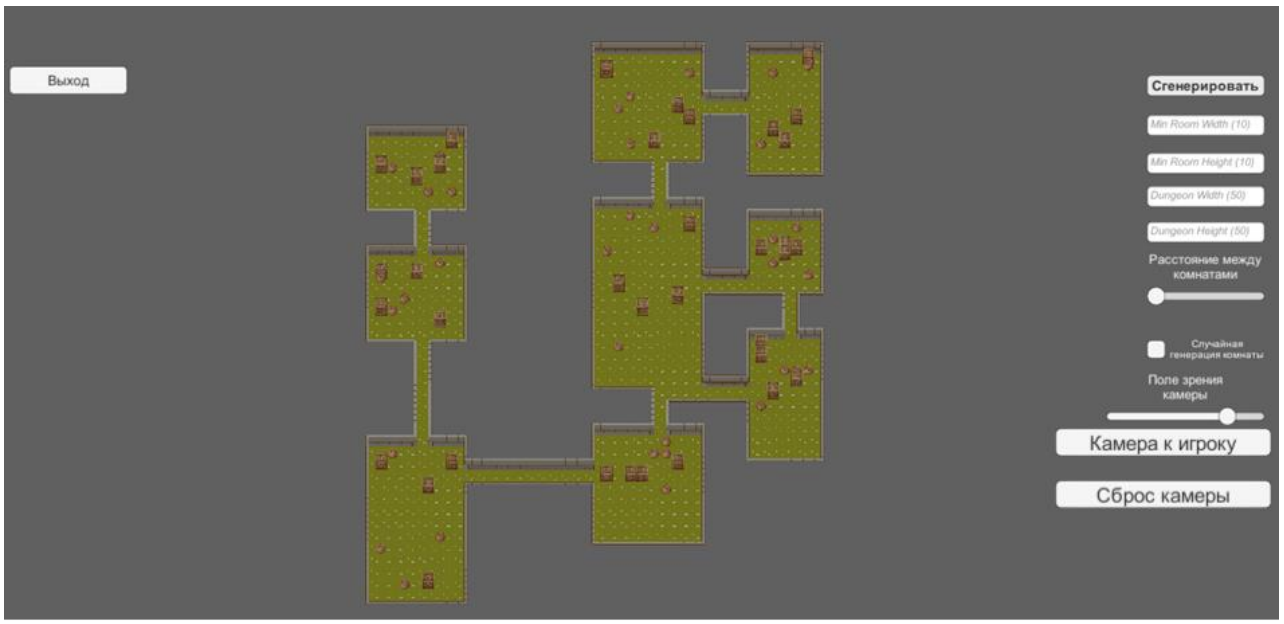


Рис. 6. Интерфейс программы

СПИСОК ЛИТЕРАТУРЫ

1. Описание алгоритма BSP-дерева [Электронный ресурс] URL: http://www.roguebasin.com/index.php?title=Basic_BSP_Dungeon_generation
2. How to use BSP trees to generate game maps Интернет-ресурс: URL: https://gamedevelopment.tutsplus.com/tutorials/how-to-use-bsp-trees-to-generate-game-maps—gamedev-12268
3. Описание алгоритма туннелирования [Электронный ресурс] URL: http://dungeonmaker.sourceforge.net/DM2_Manual/manual1.html
4. Generate random cave levels using cellular automata [Electronic resource]/Интернет-ресурс. URL: https://gamedevelopment.tutsplus.com/tutorials/generate-random-cave-levels-using-cellular-automata—gamedev-9664.

УДК 004.023

В. А. БЕСПОЯСОВА, А. И. КОНОНЕНКО
v.markutsaa@mail.ru, kononenko.arkady.mo10@yandex.ru
Науч. руководв. – канд. техн. наук, доц. Е. Ю. САЗОНОВА

Уфимский государственный авиационный технический университет

МАТЕМАТИЧЕСКОЕ И ПРОГРАММНОЕ ОБЕСПЕЧЕНИЯ ДЛЯ ЗАДАЧИ МАРШРУТИЗАЦИИ ТРАНСПОРТА С УЧЕТОМ ВРЕМЕННЫХ ОКОН И ДОРОЖНЫХ СИТУАЦИЙ

Аннотация. В статье рассматривается задача маршрутизации транспорта с учетом временных окон и дорожных ситуаций. Авторами статьи представлено математическое обеспечение задачи в виде математической модели и модифицированного метода ближайшего соседа с учетом дорожных ситуаций. Для реализации программного обеспечения был использован следующий стек технологий: Python 3.6; Web framework Django; JavaScript + jQuery; PostgreSQL + PostGIS; Leaflet + Leaflet Routing Machine.
***Ключевые слова*:** транспортная логистика; задача маршрутизации транспорта; Vehicle Routing Problem; задача маршрутизации транспорта с учетом временных окон и дорожных ситуаций.

Введение

В условиях постоянно развивающейся торговли и образования новых предприятий, торговых точек, складов, нуждающихся в продуманном цикле грузоперевозок, менеджеры по логистике сталкиваются с проблемой перемещения материальных ресурсов. Перед работниками возникает целый ряд вопросов: как наиболее выгодно и быстро доставить продукцию; сколько транспортных средств необходимо выделить; какой грузоподъемности транспортный средства использовать; как уложиться в график посещения необходимых пунктов обслуживания. Также необходимо упомянуть, что в современном мире в условиях растущей конкуренции каждая организация стремится минимизировать свои расходы, значительная часть которых может приходиться на доставку товаров при отсутствии грамотной логистики. Для оптимизации этих расходов необходимо использовать для доставки рациональные маршруты, чтобы в конечном счете снизить затраты организации на услуги доставки. Так как стоимость каждого маршрута формируется из количества потраченного в дороге топлива, а расход топлива напрямую зависит от длины маршрута и времени

проезда по нему, то конечной целью является минимизация длины и времени маршрутов.

Все вышесказанное обуславливает актуальность разработки математического и программного обеспечения для задачи построения рациональных маршрутов. Данная задача может быть сведена к классу задач маршрутизации транспорта (Vehicle Routing Problems, VPR), которые лежат на пересечении двух хорошо изученных задач: задача коммивояжера (Travel Salesman Problem, TSP) и задача об упаковке рюкзака (Bin packing problem). В статье рассматривается задача маршрутизации транспорта с учетом временных окон и дорожных ситуаций.

Постановка задачи маршрутизации транспорта с учетом временных окон и дорожных ситуаций

Рассмотрим постановку задачи нахождения рациональных маршрутов транспорта. Даны координаты точек, нуждающихся в товаре, их запросы, то есть количество продукции, которое им необходимо, а также временные окна, в пределах которых можно осуществить доставку в пункт потребления, информация о транспортных средствах, находящихся в депо, их грузоподъемность. Требуется найти такое решение, при котором потребности каждой точки будут удовлетворены, при этом товары должны быть доставлены в пределах указанного промежутка времени или же с минимальным опозданием, а количество транспортных средств, участвующих в развозе, минимально. Также при решении задачи необходимо учитывать меняющееся в течение дня время поездок между точками. Полученное решение должно быть отражено в графическом виде на карте какого-либо картографического сервиса. Описанная задача относится к задачам маршрутизации транспорта с «жесткими» или «мягкими» временными окнами (рис. 1).

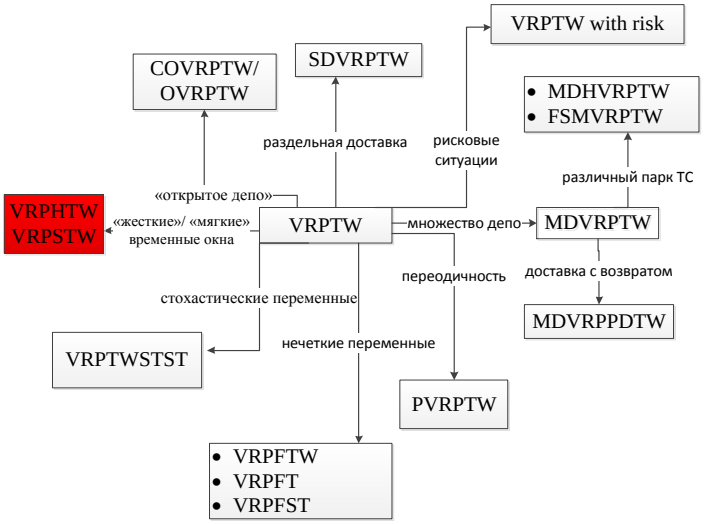


Рис. 1. Классификация задач маршрутизации транспорта

Математическое обеспечение задачи маршрутизации транспорта с учетом временных окон и дорожных ситуаций

Рассмотрим математическую модели задачи маршрутизации транспорта с учетом временных окон и дорожной ситуации.

Пусть $G(V', E)$ ориентированный граф, где $V' = \{0, 1, \dots, N\}$ – множество вершин, E – множество ребер (участков дорог). Вершина 0 представляет собой депо, а множество вершин $V = V'\{0\}$ представляет собой n клиентов. Каждый клиент имеет временное окно $[a_i, b_i]$. Каждому ребру $\{i, j\} \in E$ сопоставлена число $d_{ij} -$ расстояние и t_{ij} – время. q_i единиц товара поставляется из депо ($q_0 = 0$). Набор из m автомобилей грузоподъемности Q базируются в депо и должны быть использованы для доставки товара клиентам. Требуется найти набор замкнутых маршрутов. Целевая функция выражена стоимостью пройденного пути, и она должна стремиться к минимуму: $min \sum_{i=0}^{n} \sum_{j=0}^{n} \sum_{v=1}^{m} c_{ij} x_{ijv.}$ Каждый маршрут должен удовлетворять следующим ограничениям: каждый клиент должен быть посещен строго один раз: $\sum_{i=1}^{n} \sum_{v=1}^{m} x_{ijv} 0 = 1 \quad j = 1, \dots, n$; спрос каждого клиента удовлетворен: $\sum_{v=1}^{m} y_{iv} = q_i \quad i = 1, \dots, n$; спрос, удовлетворенный каждым ТС, не превышает грузоподъемности ТС: $\sum_{i=1}^{n} y_{iv} \leq Q_v \quad v = 1, \dots, m$; временные окна должны

быть учтены:

$a_i \le w_{iv} \le b_i \;\; i = 1 \dots n \;\; v = 1 \dots m;\; \sum_{j=1}^{n} x_{ijv} w_{jv} \ge \sum_{i=1}^{n} x_{jiv}\left(w_{iv} + s_i + c_{ij}\right).$

В качестве метода решения задачи маршрутизации транспорта в соответствии с заданными ограничениями был выбран метод ближайшего соседа. Основным достоинством данного метода является его простота, однако к недостаткам можно отнести то, что он может выдать не оптимальное решение. Тем не менее, проверив работу метода в заданных условиях был сделан вывод целесообразности его использования.

Работу метода можно описать так: на каждой итерации ищем ближайшего клиента, в чье временное окно транспортное средство может попасть, при отсутствии такого клиента ищется тот, опоздание к которому или же время ожидания будет минимально. В качестве исходных данных принимается матрица времен поездок между клиентами. По условию задачи необходимо учитывать ситуацию на дорогах, так как в разное время суток время поездки из одной точки в другую может меняться. Таким образом, на каждой итерации проверяется время суток и выбирается соответствующая матрица времен. Матрица времен генерируется путем деления каждого значения матрицы расстояний на среднюю скорость передвижения по городу в определенное время суток.

Авторы статьи апробировали предложенный метод на дорогах Уфы. Подробнее рассмотрим вычисление матрицы времен. Для вычисления средней скорости передвижения транспортных средств по Уфе был использован модуль «Пробки» сервиса Яндекс.Карты. По данным сервиса уровень пробок в Уфе в течение дня варьируется от нуля баллов до двух. Максимальная загруженность дорог приходится на периоды с семи до десяти часов утра и с семнадцати до девятнадцати часов вечера. Таким образом, для симуляции меняющейся ситуации на дорогах было принято решение сгенерировать четыре матрицы времен, полагаясь на результаты наблюдения. Для симуляции различного состояния дорог в разные дни недели было решено также во время генерации матриц добавлять случайное значение из определенного диапазона к скорости, на которую

делится расстояние между двумя точками. Несмотря на одинаковые начальные параметры, решения будут отличаться друг от друга, так как имитируется изменчивость ситуации на дорогах не только в разное время суток, но и в разные дни, компенсируя невозможность бесплатного получения актуальной информации о пробках и дорожных ситуациях в городе. Таким образом, расчет матриц времен будет проходить согласно данным таблицы 1.

Расчет скорости передвижения между каждым клиентом: $v = v' + rand(-v'', +v'')$, где v' – средняя скорость в определенное время суток; v'' – отклонение скорости.

Таблица 1

Средняя скорость передвижения по городу в разное время суток

Время суток	Средняя скорость	Отклонение скорости
7^{00} - 10^{00}	25 км/ч	5 км/ч
10^{00} - 17^{00}	35 км/ч	8 км/ч
17^{00} -19^{00}	23 км/ч	3 км/ч
19^{00} - 00^{00}	38 км/ч	10 км/ч

Рассмотрим алгоритмическое обеспечение задачи маршрутизации транспорта. Входными данными являются массив с расстояниями от одного клиента до другого; массив с запросами клиентов; массив с грузоподъемностью автомобилей. Выходными данными является массив массивов с порядком посещения клиентов для каждого транспортного средства, включенного в решение. Общая схема алгоритма решения задачи маршрутизации транспорта в условиях временных окон выглядит следующим образом:

Шаг. 1. Из полученного массива расстояний от каждого клиента до каждого генерируется матрицы времен поездок от клиента к клиенту. Процесс генерации матриц описан в предыдущем разделе.

Шаг. 2. До тех пор, пока не удовлетворен спрос каждого клиента в цикле повторяется:

Шаг 1.1. Выбирается первое транспортное средство из списка

Шаг 1.2. Находится ближайший клиент, который не был посещен транспортным средство

Шаг 1.3. Пока грузоподъемность ТС превышает спрос следующего клиента шаги 1.3.1-1.3.3 повторяются в цикле:

Шаг 1.3.1. Ближайший клиент, который не был посещен, добавляется в маршрут автомобиля.

Шаг 1.3.2. От грузоподъемности ТС отнимается запрос клиента.

Шаг 1.3.3. Находится следующий ближайший клиент.

Шаг 3. Выводится результат в виде массива массивов с порядком посещения клиентов для каждого ТС, задействованного в решении.

Так как решается задача маршрутизации транспорта с временными окнами, процесс поиска следующего клиента для посещения усложняется. Оптимальным решением задачи будет такое, при котором каждый клиент посещен вовремя. Однако иногда в сложившихся условиях невозможно посещение всех клиентов в срок. Так как в решаемой задачи временные окна приняты «мягкими», допустимо опоздание транспортного средства к клиенту. В таком случае, если нет «идеального» клиента, идет поиск того, к которому опоздание будет минимально или же, если водитель к каждому доступному клиенту приезжает заранее, осуществляется поиск клиента, время ожидание которого будет минимально.

Программное обеспечение задачи маршрутизации транспорта с учетом временных окон и дорожных ситуаций

Для реализации программного обеспечения был использован следующий стек технологий: Python 3.6; Web framework Django; JavaScript + jQuery; PostgreSQL + PostGIS; Leaflet + Leaflet Routing Machine. На рисунке 2 представлена структурная схема программного решения.

Рис. 2. Структурная схема программного решения

Логически программу можно разделить на три части. Первая часть – это модуль ввода данных, где пользователь добавляет в базу информацию о клиентах (местоположение, запросы, временное окно) и транспортных средствах (вместимость); полученные данные поступают в модуль решения задачи. Вторая часть – модуль решения задачи, где на основании входных данных решается задача маршрутизации транспорта в условиях транспортных ситуаций и полученный результат анализируется и выводится пользователю на экран. Третья часть – модуль показа результатов, в данном модуле полученное решение задачи выводится пользователю на экран.

Интерфейс программного решения представлен на рисунке 3.

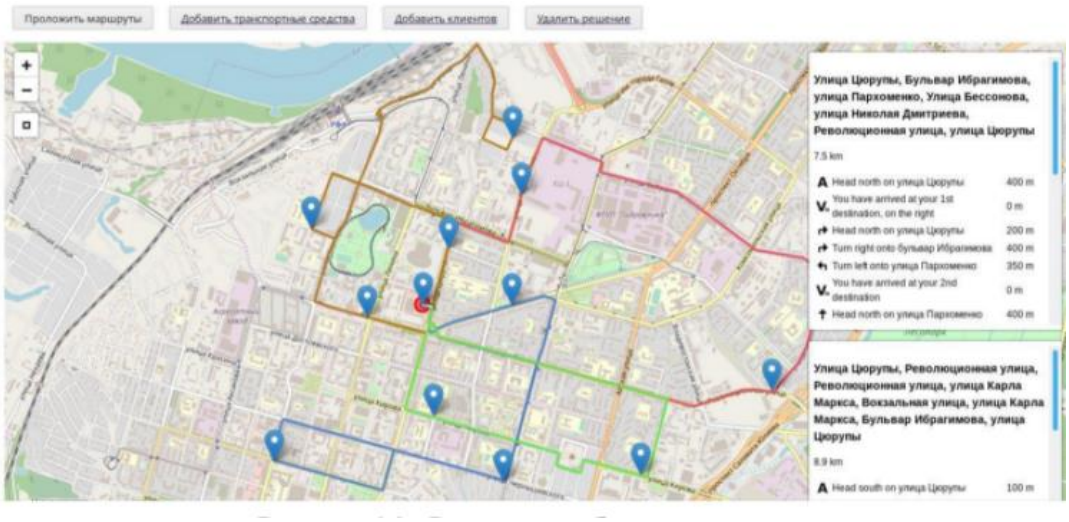


Рис. 3. Интерфейс сервиса

Авторами статьи был проведен численный эксперимент, который показал, что программа работает удовлетворительно при надежном и качественном интернет-соединении, и время ожидания ответа при максимально допустимом

количестве клиентов (70) не превышает 45 секунд, при условии, что будет отправлено 4900 запросов к сервису маршрутизации. Также было проведено тестирование программного решения в нормальных, экстремальных и исключительных условиях, которое показало, что программа корректно выполняет заявленные функции В экстремальных и исключительных ситуациях программа выдает сообщение об ошибке и продолжает работу в штатном режиме.

Заключение

Авторами статьи приведена содержательная постановка задачи маршрутизации транспорта с учетом грузоподъемности и временных окон в условиях дорожных ситуаций. Для решения задачи, на основе аналитического обзора методов решения был выбран метод поиска ближайшего соседа. Разработано математическое обеспечение задачи маршрутизации транспорта с учетом различных ограничений в условиях дорожных ситуаций в виде математической модели и модификация алгоритма поиска ближайшего соседа, подходящая для решения задачи при заданных условиях. Разработано программное обеспечение, позволяющее решить задачу маршрутизации транспорта с учетом грузоподъемности и временных окон в условиях дорожных ситуаций. Проведено тестирование программного обеспечения в нормальных, экстремальных и исключительных условиях, которое показало, что программное обеспечение корректно выполняет функции. Применение программного решения позволит снизить транспортные расходы на доставку грузов на 3-5%.

Результаты исследования, приведенные в статье, получены в рамках выполнения грантов РФФИ 19-07-00709 и государственного задания No FEUE-2020-0007.

СПИСОК ЛИТЕРАТУРЫ

1. Бронштейн, Е. М. Детерминированные оптимизационные задачи транспортной логистики/ Е.М. Бронштейн, Т.А. Заико // Автоматика и телемеханика. – 2010. – выпуск 10. – С. 133–147.
2. Ерзин А.И. Задачи маршрутизации: учеб. пособие / А.И. Ерзин, Ю.А. Кочетов. – Новосиб. гос ун-т. – Новосибирск: РИЦ НГУ, 2014. – 95 с.
3. Рассадникова Е. Ю. Система поддержки принятия решений при планировании транспортного процесса с учетом специальных ограничений (на примере нефтехимического предприя-

тия): дис. … канд. техн. наук: 05.13.01: защищена 17.06.15: утв. 12.11.15. — Уфа, 2015. — 215 с.
4. Рассадникова Е. Ю. Методы и алгоритмы определения рациональных маршрутов для задачи маршрутизации транспортных средств с учетом временных окон и других условий / George Kovács, Nafissa Yusupova, Olga Smetanina, Rassadnikova E. Yu. Methods and Algorithms of Rational Routes Determination for Vehicle Routing Problem with Time Windows and Other // Pollack Periodica. – 2018. – V. 13. – №. 1. – pp. 65-76
5. Bräysy, O. Vehicle Routing Problem with Time Windows Part I: Route construction and local search algorithms / O. Bräysy, M. Gendreau // Transportation Science. – 2005. – Vol. 39. – № 1. – pp. 104 – 108.
6. Hansen, P. Chapter 8. Variable Neighborhood Search/ P. Hansen, N. Mladenovic. – 28 p.
7. Hansen, P. Variable Neighborhood Search: Principles and application/ P. Hansen, N. Mladenovic /Operations Research. – 2001. – Vol. 130. – pp. 449 – 467.

УДК 004

Р. Э. ВАЛИАХМЕТОВА
valiahmetovaregina@mail.ru
Науч. руководитель – д.т.н., профессор А. Ф. ВАЛЕЕВА

Уфимский государственный авиационный технический университет

МАТЕМАТИЧЕСКОЕ И ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ДЛЯ РЕШЕНИЯ ЗАДАЧИ УПРАВЛЕНИЯ ЗАПАСАМИ

Аннотация. Объектом исследования является оптово-розничная компания, функционирующая на современном российском рынке на территории Республики Башкортостан и за ее пределами. Предметом исследования является процесс управления запасами фирмы в условиях существенной случайной компоненты параметров спроса и времени выполнения заказа. Исследовательская работа посвящена разработке математического и программного обеспечения, решающего задачу управления запасами и разработка системы управления запасами витаминизированной продукции, профессиональных дезинфицирующих средств и уборочного инвентаря торгующей компании ООО «Аквавит». В работе приводятся результаты проведенного анализа предметной области, обзора существующих программных продуктов, анализ методов и моделей системы управления запасами. В работе представлены все существующие модели и методы, модифицированные алгоритмы для детерминированной и вероятностной модели, разработанная имитационная модель системы управления запасами, математическая модель и программная реализация. В рамках исследования был разработан алгоритм расчета параметров моделей для конкретной бизнес-ситуации и выполнена программная реализация системы управления запасами в соответствии с техническим заданием, а также проведен выбор эффективной стратегии управления запасами, позволяющей минимизировать затраты на содержание и выполнение заказа с учетом издержек, связанных с расходами на логистику.
***Ключевые слова*:** система управления запасами; модели и методы управления запасами.

Одним из основных условий успешной деятельности любой торгующей организации является разработка эффективной системы управления запасами для стабильного непрерывного рабочего процесса и беспромедлительного удовлетворения потребностей клиентов, которая оказывает серьезное воздействие на деятельность организации в целом.

Управление товарными запасами решает огромное множество организационно экономических вопросов формирования и поддержания ассортимента товаров на определенном уровне. Необходимость грамотного управления запасами связано с изменением спроса на конкретные товары.

Целью данной работы является исследование моделей, методов для решения задачи управления запасами и разработка системы управления запасами

витаминизированной продукции, профессиональных дезинфицирующих средств и уборочного инвентаря торгующей компании ООО «Аквавит».

Перечень задач, которые поставлены в соответствии с целью исследовательной работы:

проанализировать методы и модели управления запасами;

разработать имитационную модель системы управления запасами витаминизированной продукции, профессиональных дезинфицирующих средств и уборочного инвентаря;

разработать имитационный алгоритм расчета параметров моделей для конкретной бизнес-ситуации;

разработать программное обеспечение системы управления запасами компания;

произвести оценку качества программного обеспечения на базе вычислительного эксперимента.

Объектом исследования является оптово-розничная компания, функционирующая на современном российском рынке на территории Республики Башкортостан и за ее пределами.

Предметом исследования является процесс управления запасами фирмы в условиях существенной случайной компоненты параметров спроса.

Содержательная постановка задачи

Торговая оптово-розничная компания ООО «Аквавит» производит продажу и поставку витаминизированной продукции, профессиональных дезинфицирующих средств и уборочного инвентаря, запасы которых хранятся на складе. Менеджеры компании подают заявку логисту на определенный месяц (по спросу) на определенный продукт. Кроме того, компания принимает участие на аукционах, на которых отдел закупок медучреждения публикует заявку на приобретение необходимой продукции на электронных торгах, которые проходят на основании Федерального закона "О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных

нужд" от 05.04.2013 N 44-ФЗ. По результатам аукционов формируется спрос на год на определенный вид продукции, а именно: в каждом месяце закладывается уровень спроса на каждый вид продукции. В начале каждого месяца компания пересматривает уровень запасов, и решает, какое количество продукции заказать у поставщика. Для хранения запасов используется склад, находящийся на территории компании и являющийся собственностью компании. Склад несет расходы на хранение запасов: ежемесячную оплату газа, электроэнергии для поддержания условий хранения товара, а также затраты на хранение учитывают заработную плату работника, который обслуживает складское помещение, заработную плату охранника, и выплату налога в количестве 39% от заработной платы наемных работников. Затраты системы управления запасами включают в себя: затраты на пополнение запаса, потери от дефицита/переизбытка продукции, списания товара в следствие его порчи или дефекта. Затраты на логистику маршрутизации складываются из следующих параметров: затраты на заработную плату водителя, выплата налога в 39% от заработной платы водителя, амортизация машины, расход на доставку до клиента, оплачиваемые компанией ООО «Аквавит». Имеется информация о поступающих заявках на продажу продукции определенного вида, о доставке продукции по определенному адресу до склада и о количестве продукции, находящейся на складе в текущий момент учета. Данная информация передается в отдел по маршрутизации и доставке товара. При этом этот отдел располагает сведениями о различных клиентах в следующих городах: Белебей, Белорецк, Стерлитамак, Уфа, Салават, Сибай, Октябрьский, размещенных на территории Республики Башкортостан; о депо с парком автомобильных транспортных средств (ТС) одинаковой грузоподъемностью, являющимися собственностью компании.

Требуется:

Выбрать эффективную стратегию управления запасами, позволяющую минимизировать затраты на содержание и выполнение заказа с учетом издержек, связанных с расходами на логистику.

Модели управления запасами

Любая модель системы управления запасами включает в себя следующие основные параметры и возникающие процессы: начальные условия, спрос, принятие решений о пополнении запаса, имеющийся запас и некоторый расход запаса. Общая схема существующих моделей управления запасами представлена на рисунке 1.

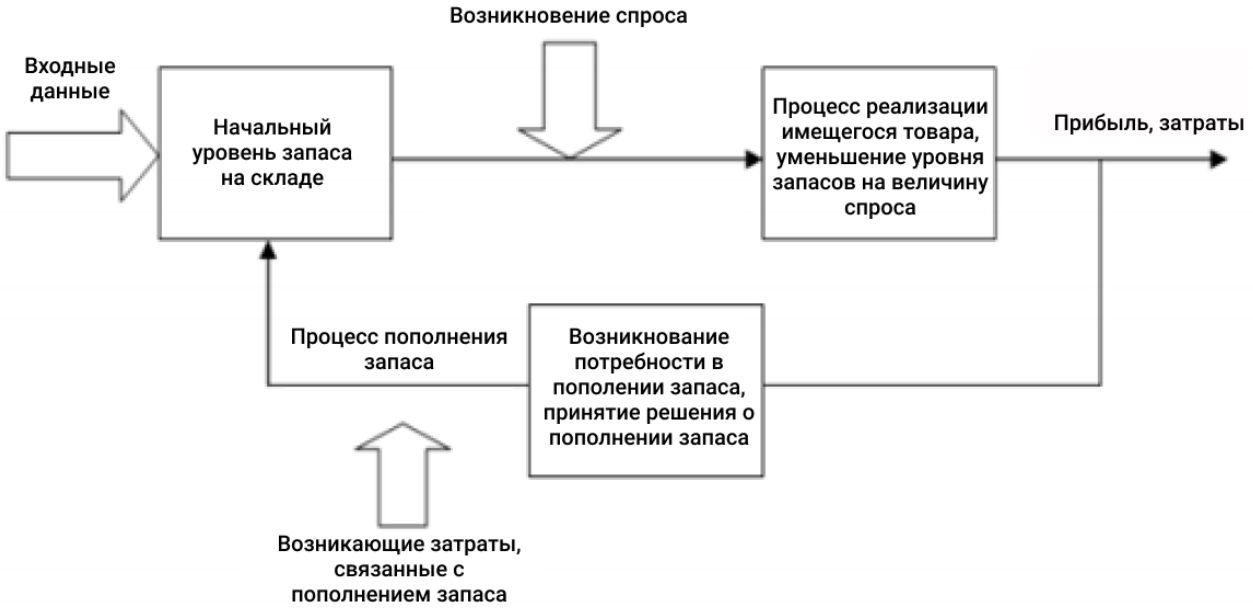


Рис. 1. Процессы происходящие внутри модели управления запасами

Особенности анализа моделей управления запасами в целом обуславливаются следующими факторами:

– спрос носит случайный характер;

– длительность процедур пополнения запасов является случайной величиной;

– стоит задача определения объема увеличения запасов;

– необходимость выбора моментов подачи заказов на такое увеличение, включая моменты поступления заказов.

Различают детерминированные и вероятностные модели управления запасами в зависимости от действий случайных факторов на параметры системы управления (объемы спроса, промежутки между возникновением спроса, время

выполнения заказа). Если хотя бы один параметр является случайной величиной, модель будет вероятностной, в противном случае – детерминированной.

Общая схема решения для поиска стратегий управления запасами и поиска маршрутов

Шаг 1. Процедура ЗАПАСЫ (вход: n, T, I0, i, K, h, w,(s1,S1),…,(sn, Sn), D, TD; выход: Q* , (s*,S*) – стратегия с меньшими средними общими затратами в месяц)

Шаг 2. Процедура ЗАЯВКА (вход: prod, n1, client, address; выход: prod, n1, client, address)

Шаг 3. Процедура ТРАНСПОРТИРОВКА (вход: n, cij, eij, α, β, τij, qit, M, si, ai, bi, l, penalty_timei, mck, lpalj, wpalj, hpalj, mpalj, qpj, hpalj, Lv, Wv, Hv, Qv, pkont, qkont, vkont;, M1; выход: матрица, состоящая из R рациональных маршрутов, карта размещения заказа в ТС v, значение fpackv).

Математическая модель системы управления запасами

Перейдем к рассмотрению моделирования системы управления запасами для компании ООО «Аквавит» при рассмотрении различных стратегий осуществления запасов. Введем следующие обозначения.

Описание изменения количества товара по времени:

В каждом периоде контроля запасов *T* компания пересматривает уровень запасов и решает, сколько товара заказать.

При возникновении спроса на товар он немедленно удовлетворяется, если уровень запасов равен спросу на товар.

Если спрос превышает уровень запасов, поставка той части товара, которая превышает спрос над предложением, откладывается и выполняется при будущих поставках.

При поступлении заказа товар в первую очередь используется для максимально возможного выполнения отложенных поставок (если таковые имеются).

Остаток заказа (если таковой имеется) добавляется в запасы.

Количество товара, находящегося в запасах в течение n месяцев вычисляют по формуле:

$$\bar{I}^{+} = \frac{\int_{0}^{n} I^{+}(t)dt}{n} \tag{1.1}$$

Затраты на хранение в месяц составляют:

$$h=(k+0,39*(zp1+zp2)+zp1+zp2)/kol \tag{1.2}$$

где k – затраты на коммунальные услуги: содержание, газ, электроэнергия; zp1 – заработная плата работника, который обслуживает складское помещение; zp2 – заработная плата охранника; kol – общее количество хранимого товара на складе; nalog – налог 39% от заработной платы наемных работников.

Общие затраты на хранение в месяц составляют:

$$C_x=\Sigma h_i \tag{1.3}$$

Количество товара в отложенных поставках:

$$\bar{I}^{-} = \frac{\int_{0}^{n} I^{-}(t)dt}{n} \tag{1.4}$$

Издержки, образовавшиеся в связи с отложенными поставками, в месяц составляют:

$$C_Д = w\bar{I}^{-}(t). \tag{1.5}$$

Объем заказа Q равен:

$$Q = \begin{cases} S - I, \text{если } I < s \\ 0, \quad \text{если } I \geq s \end{cases} \tag{1.6}$$

Если запас пополняется на Q единиц, то затраты компании $C_П$ вычисляются по формуле:

$$C_п = K + iQ \tag{1.7}$$

где K – затраты на заказ, i – затраты на заказ единицы продукции.

Если Q=0, то затрат нет.

Общие расходы составляют:

$$Соб=С_П+С_Х+С_Д. \quad (1.8)$$

Требуется определить выгодную стратегию управления запасами с меньшими общими издержками $С_{об}$.

Заключение

Исследовательская работа посвящена разработке математического и программного обеспечения для решения задачи выбора эффективной стратегии управления запасами компании, а также передача поступающих заявок в систему логистики маршрутизации по доставке товара клиенту.

Основные результаты работы:

1) Проведен аналитический обзор существующих программных продуктов.

2) Описана математическая модель задачи выбора эффективной стратегии управления запасами.

3) Исследованы существующие модели и методы для решения задачи для решения задачи выбора эффективной стратегии управления запасами компании.

4) Модифицированы алгоритмы для детерминированной и вероятностной моделей управления запасами.

5) Разработан алгоритм для имитационной модели управления запасами.

6) Реализованы разработанные и модифицированные алгоритмы в виде программного обеспечения.

7) Проведены вычислительные эксперименты, направленный на определение эффективности разработанного алгоритма и проанализированы полученные результаты эксперимента.

СПИСОК ЛИТЕРАТУРЫ

1. Лукинский В.В. Актуальные проблемы формирования теории управления запасами: монография / В.В. Лукинский – Спб. : СПбГИЭУ, 2008.-213 с.
2. Алесинская Т.В. Основы логистики.Функциональные области логистического управления. – Таганрог: Изд-во ТТИ ЮФУ, 2009. 79 с.

3. Аникин Б. А., Тяпухин А. П. Коммерческая логистика: учеб. – М.: ТК Велби, Изд-во Проспект, 2006. – 432 с. ISBN 5-98-032-810-6
4. Алесинская Т.В. Основы логистики.Функциональные области логистического управления. – Таганрог: Изд-во ТТИ ЮФУ, 2009. 79 с.
5. Бродецкий Г.Л. «Управление запасами» «Эксмо» 2007 г.
6. Букан, Дж. Научное управление запасами / Дж. Букан, Э. Кенингсберг. – М.: Издательство Наука, 1967. – 383 с.
7. Волков, И.К. Исследование операций / И.К. Волков, Е.А. Загоруйко. – М.: Издательство МГТУ, 2002 – 435 с.
8. Гмурман В.Е. Теория вероятностей и математическая статистика: Учеб. пособие для вузов/В.Е. Гмурман. – 9-е изд., стер. – М.: Высш. шк., 2003. – 479 с.
9. Гордон М.П., Логистика товародвижения. - М.: Центр экономики и маркетинга. 2002. - 168с.
10. Грузинов В.П., Экономика предприятия:Учебник для вузов/ Под ред. Проф. В.П.Грузинова.-М.:банки и биржи, ЮНИТИ, 1999.-535с.

УДК 519

К. Р. ГАЛЛЯМУТДИНОВА
s@kamill.ru
Науч. руководов. – д-р. техн. наук, проф. Н. М. ШЕРЫХАЛИНА

Уфимский государственный авиационный технический университет

ИНТЕРПОЛЯЦИЯ ФУНКЦИЙ С ПОМОЩЬЮ КУБИЧЕСКОГО СПЛАЙНА

Аннотация. В данной статье будет рассмотрена задача интерполяции функций с помощью сплайна, в которой использован метод прогонки для решения систем линейных алгебраических уравнений, а также проведен численный эксперимент.
***Ключевые слова*:** интерполяция; численный метод; сплайн; метод прогонки.

Интерполяция – это метод нахождения неизвестных промежуточных значений функций, по имеющемуся дискретному набору известных значений. Термин «интерполяция» впервые употребил Джон Валлис в своем трактате «Арифметика бесконечных» (1656).

До появления ЭВМ большая часть практических вычислений строилась на применении таблиц элементарных функций, таких как синусы, логарифмы и т.п. Далее решалась задача интерполяции. В наиболее простом случае соседние точки графика этой функции соединялись отрезком прямой (линейная интерполяция).

С появлением ЭВМ возникла потребность использовать численные методы решения задач интерполяции. Многим из тех, кто занимается научными и инженерными расчетами, часто приходится оперировать наборами значений, полученных опытным путем или методом случайной выборки.

На практике чаще всего применяют интерполяцию многочленами. Это, как правило, связано с тем, что многочлены легко вычислять, легко аналитически находить их производные и множество многочленов плотно в пространстве непрерывных функций.

В данной работе мы будем применять метод кубического сплайна и проведем численный эксперимент с оценкой погрешности.

Пусть отрезок $[a, b]$ разбит на n частичных отрезков $[x_i, x_{i+1}]$, где $x_i < x_{i+1}$, i=0,1, …, n-1, x_0=a, x_n =b. Обозначим = $h_i = x_i - x_{i-1}$. В случае равномерного разбиения h=(b-a)/n, x_i=. $a + ih$

Функция $f(x)$ задана своими значениями в узловых точках x.

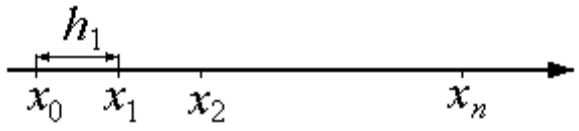


Рис. 1. Разбиение интервала при интерполяции

Сплайном называется функция, которая вместе с несколькими производными непрерывна на всем заданном отрезке $[a, b]$, а на каждом частичном отрезке $[x_i, x_{i+1}]$ в отдельности является некоторым алгебраическим многочленом.

$$y(x) = \begin{cases} f_1(x), & x \in [x_0, x_1], \\ f_2(x), & x \in [x_1, x_2], \\ \cdots & \cdots \\ f_n(x), & x \in [x_{n-1}, x_n]. \end{cases}$$

Для данной научной работы был выбран сплайн третьей степени, имеющий на отрезке $[a, b]$ непрерывную, по крайней мере, первую производную. Обозначим его через $S_3(x)$. На каждом отрезке кубический сплайн имеет следующий вид:

$$S_3(x) = a_{i0} + a_{i1}(x - x_i) + a_{i2}(x - x_i)^2 + a_{i3}(x - x_i)^3,\ x \in [x_i, x_{i+1}],$$

и удовлетворяет следующим условиям:

$$S_3(x_i) = f(x_i),\ i = 0,\ldots,n.$$

Исходя из того, что сплайн на каждом отрезке определяется четырьмя коэффициентами для его построения на всем отрезке требуется определить 4n коэффициентов. Для их однозначного определения нам необходимо задать 4n уравнений. Помимо этого, условие дает 2n уравнений, так как данный многочлен должен проходить через две заданные точки: начало и конец отрезка. При

этом функция $S_3(x_i)$, удовлетворяющая этим условиям, будет непрерывна во всех внутренних узлах.

Условие непрерывности производных сплайна $S_3'(x)$, $S_3''(x)$, во всех внутренних узлах x_i, i=1,...,n-1 сетки дает 2(n-1) равенств.

Итого получаем 4n-2 уравнений.

Два дополнительных (краевых) условия обычно зададим в виде ограничений на значение производных сплайна на концах промежутка [a,b].

Для того, чтобы построить интерполяционный кубический сплайн воспользуемся следующим алгоритмом.

Пусть каждому значению аргумента x_i, i=0,...,n соответствуют значения функции $f(x_i)=y_i$ и требуется найти функциональную зависимость в виде сплайна, удовлетворяющего следующим требованиям:

1) функция $S_3(x)$ непрерывна на отрезке [a,b] вместе со своими производными до второго порядка включительно;

2) $S_3(x_i)=y_i$, i=0,1,...,n;

3) функция $S_3(x)$ удовлетворяет одному из вариантов краевых условий а-в (условия а,б,в могут задаваться смешанно, т.е. на одном конце первая производная, на другом - вторая).

Сформулированная задача имеет единственное решение.

Вторая производная $S''_3(x)$, которая выражается непрерывной линейной функцией представим в виде многочлена Лагранжа 1-ой степени.

$$S_3''(x)=\frac{x_i-x}{h_i}m_{i-1}+\frac{x-x_{i-1}}{h_i}m_i \qquad (1)$$

где $h_i = x_i$-x_{i-1}, $m_i= S''_3(x_i)$.

Проинтегрировав дважды обе части выражения и использовав условия непрерывности функции и первой производной получим следующую систему уравнений:

$$\frac{h_i}{6}m_{i-1}+\frac{h_i+h_{i+1}}{3}m_i+\frac{h_{i+1}}{6}m_{i+1}=\frac{y_{i+1}-y_i}{h_{i+1}}-\frac{y_i-y_{i-1}}{h_i},\ i=1,\dots,n-1 \qquad (2)$$

В конечном итоге решая систему уравнений относительно параметров m_i получим:

$$S_3(x) = \frac{(x_i - x)^3 - h_i^2(x_i - x)}{6h_i} m_{i-1} + \frac{(x - x_{i-1})^3 - h_i^2(x - x_{i-1})}{6h_i} m_i + \qquad (3)$$

$$+ \frac{x_i - x}{h_i} y_{i-1} + \frac{x - x_{i-1}}{h_i} y_i$$

По этой формуле вычисляются значения функции $S_3(x)$. Важно отметить, что решение системы уравнений происходит методом прогонки.

Проведем численный эксперимент на конкретном примере и представим результаты в таблице.

Таблица 1

n	Δ_{max}	$\Delta_{оц}$	K_Δ
5	1,02E-03	-	-
10	6,29E-05	6,39E-05	16,25636
20	3,91E-06	3,93E-06	16,0827
40	2,44E-07	2,45E-07	16,02083
80	1,53E-08	1,53E-08	16,00522
160	9,54E-10	9,54E-10	16,00131
320	5,96E-11	5,96E-11	16,00031
640	3,73E-12	3,73E-12	16,00015
1280	2,33E-13	2,33E-13	16,00286
2560	1,45E-14	1,46E-14	16,00763
5120	1,11E-15	9,09E-16	13,1
10240	2,22E-16	2,78E-16	5

Пусть $f(x) = \cos x$, интерполировать функцию мы будем на отрезке [0,π] при равномерном разбиении с удвоением числа отрезков n. Краевые условия – равенство 1 второй производной на левом конце отрезка и -1 на правом конце. Колонка Δ_{max} – представлена максимальная погрешность $|S_3(x)-f(x)|$, вычисленная в точках, находящихся между узлами сетки, K_Δ - отношение погрешности предыдущей строки к данной (коэффициент уменьшения погрешности при удвоении n). Видно, что K_Δ сохраняет значение, соответствующее четвертому

порядку точности ($K_\Delta \approx 2^4$) до значений n=1000-3000, выше которых в общей погрешности результата преобладает погрешность округления.

Однако, необходимо отметить, что для практического применения оценки погрешности необходимо знать верхнюю оценку k-й производной функции $f(x)$. Но это не всегда возможно. Для оценки погрешности можно применить правило, использующее закономерность зависимости погрешности от h или n. При этом наблюдается, что при увеличении числа узлов погрешность интерполяции в какой-нибудь конкретной точке x может изменяться нерегулярно, поскольку положение этой точки относительно соседних узлов (отношение $(x-x_{j-1})/(x_j-x_{j-1})$) может различаться для разных n. На примере данного численного эксперимента видно, что максимальная погрешность на отрезке уменьшается $[0,\pi]$ в $K_\Delta \approx 2^k$ раз при удвоении n. Используя свойство сохранения значения K_Δ для максимума погрешности $\Delta_{\max}(n)$ можно получить оценку в виде

$$\Delta_{\text{оц}}(2n) = \frac{\Delta_{\max}(n)}{2^k}. \qquad (4)$$

Для этого необходимо иметь способ оценки величины $\Delta_{\max}(n)$, если даже точное значение интерполируемой функции $f(x)$ неизвестно. Можно использовать следующий способ, заключающийся в сравнении значений $S_3(x)$, вычисленных при разных числах отрезков, на которые разбивается отрезок $[a,b]$ - n и $2n$. При удвоении n при равномерном или неравномерном разбиении возникает n новых узловых точек $x_{j-1/2}$, лежащих между общими узлами x_{j-1} и x_j (рис. 2.5.1). Тогда в качестве оценки $\Delta_{\max}(n)$ выберем

$$\Delta_{\max}(n) \approx \max_{1 \le j \le n} \left| S_3^{2n}\left(x_{j-1/2}\right) - S_3^{n}\left(x_{j-1/2}\right) \right|. \qquad (5)$$

Для таблицы 1 были выбраны корректные краевые условия. Однако, при выборе других краевых условий наблюдается сравнительно большая погрешность интерполяции. Для наглядности результат представлен в виде таблицы.

Таблица 2

n	Δ_{max}	$\Delta_{оц}$	K_Δ
5	1,90E-02	-	-
10	4,58E-03	4,74E-03	4,14E+00
20	1,13E-03	1,14E-03	4,04E+00
40	2,82E-04	2,83E-04	4,01E+00
80	7,06E-05	7,06E-05	4,00E+00
160	1,76E-05	1,76E-05	4,00E+00
320	4,41E-06	4,41E-06	4,00E+00
640	1,10E-06	1,10E-06	4,00E+00
1280	2,76E-07	2,76E-07	4,00E+00
2560	6,89E-08	6,89E-08	4,00E+00
5120	1,72E-08	1,72E-08	4,00E+00
10240	4,31E-09	4,31E-09	4,00E+00

После проведения численного эксперимента следует отметить плюсы и минусы такого подхода.

К плюсам мы относим то, что график построенной функции будет проходит через каждую точку из набора, при этом заданным массивом точек построенная функция будет определяться однозначно. Степень многочленов никак не зависит от числа узлов сетки, а значит не изменится при его увеличении. В отличие от интерполяционных многочленов Лагранжа, последовательность интерполяционных кубических сплайнов на равномерной сетке всегда сходится к интерполируемой непрерывной функции. Минусом является выбор краевых условий, с помощью которых в конструкцию сплайна включаются параметры, при выборе которых мы управляем его поведением. При выборе некорректных краевых условий (иногда предлагается принимать $S''_3(a)=S''_3(b)=0$) точность интерполяции функции и ее первой производной, как правило уменьшается.

СПИСОК ЛИТЕРАТУРЫ

1. Житников В. П., Шерыхалина Н. М., Поречный С. С., Зарипов А. А. Исследование свойств численных методов с помощью вычислительного эксперимента: учеб. пособие // Уфимск. гос. авиац. техн. ун-т. – Уфа : РИК УГАТУ, 2019. – 287 с.

УДК 004.42

Ш. Т. ГАРЕЕВ, Р. Р. ГАЛИМОВ
shamil.gareev27@gmail.com
Науч. руководитель – д-р техн. наук, проф. В. Е. ГВОЗДЕВ

Уфимский государственный авиационный технический университет

РАЗРАБОТКА ИНТЕЛЛЕКТУАЛЬНОГО КОМПЛЕКСА ДЛЯ КОНТРОЛЯ И УДАЛЕННОГО ЛОГИРОВАНИЯ ОБОРУДОВАНИЯ ГАЗОВОЙ И НЕФТЯНОЙ ПРОМЫШЛЕННОСТИ

Аннотация. Контроль работы оборудования является ключевой задачей обеспечения безотказного функционирования объектов нефтегазового комплекса. Статья посвящена разработке интеллектуального комплекса, который позволяет автоматизировать процесс контроля состояния оборудования.
***Ключевые слова*:** датчик; оборудование; интеллектуальная система; аппаратно-программный комплекс; регистратор; сервер; программное обеспечение.

Контроль показаний датчиков, расположенных на объектах нефтедобычи и объектах газовой отрасли, является одной из важнейших задач автоматизации нефтегазового комплекса, объединяющего объекты добычи, переработки, транспортировки и хранения. На всех перечисленных объектах применяются различные датчики контроля температуры, давления, влажности и т. д., отвечающие за корректную работу оборудования [1]. Однако контроль или мониторинг данных устройств бывает сильно затруднен, поскольку многие объекты располагаются на удалении от диспетчерского (контрольного) пункта.

Для получения актуальной информации с указанных датчиков, а также параметризации техническому персоналу зачастую необходимо лично присутствовать на объекте и с помощью ручного инструмента производить мониторинг или параметризацию, что представляет неудобства, особенно в тех случаях, когда объект находится за десятки километров от основного места работы сотрудников предприятия.

Оборудование нефтяных, газовых и других промышленных объектов требует своевременного контроля состояния. Система контроля может обеспечиваться различными способами, такими как: традиционные, которые учитывают человеческий фактор, автоматические системы контроля, а также контроль

оборудования с помощью интеллектуальных систем нового поколения [2]. Наиболее эффективным способом контроля является использование автоматизированных систем с применением интеллектуальных технологий [3, 4].

Цель работы состоит в том, чтобы разработать интеллектуальную систему контроля нового поколения применительно к объектам газовой и нефтяной промышленности, которая будет способна получать информацию о состоянии системы удаленно.

Для реализации поставленной задачи был разработан аппаратно-программный комплекс, состоящий из регистратора (рис. 1), который размещается на объектах контроля, и сервера, обеспечивающего хранение и визуализацию информации, полученную с регистратора.

Рис. 1. Регистратор АПК

Регистратор осуществляет сбор данных по геолокации, имеет 7 аналоговых и 7 дискретных входов, по которым передается информация с контролируемого оборудования, а также сохраняет данные во внутренней памяти и передает их на сервер по каналам GPRS. Аналоговые входы имеют интерфейс «токовая петля 4-20 mA». Максимальное входное напряжение составляет +24 В. Дискретные входы имеют интерфейс «сухой контакт». Максимальное входное напряжение составляет +24 В. Каждый регистратор оснащается Wi-Fi точкой доступа, на котором имеется интерфейс конфигурации логируемых данных для возможности изменения названия датчиков и подключаемых устройств. В кон-

фигураторе имеется интерфейс для скачивания накопленных данных (FTP-сервер). Данные в регистраторе защищены от модификации. Интерфейс конфигуратора регистратора представлен на рис. 2.

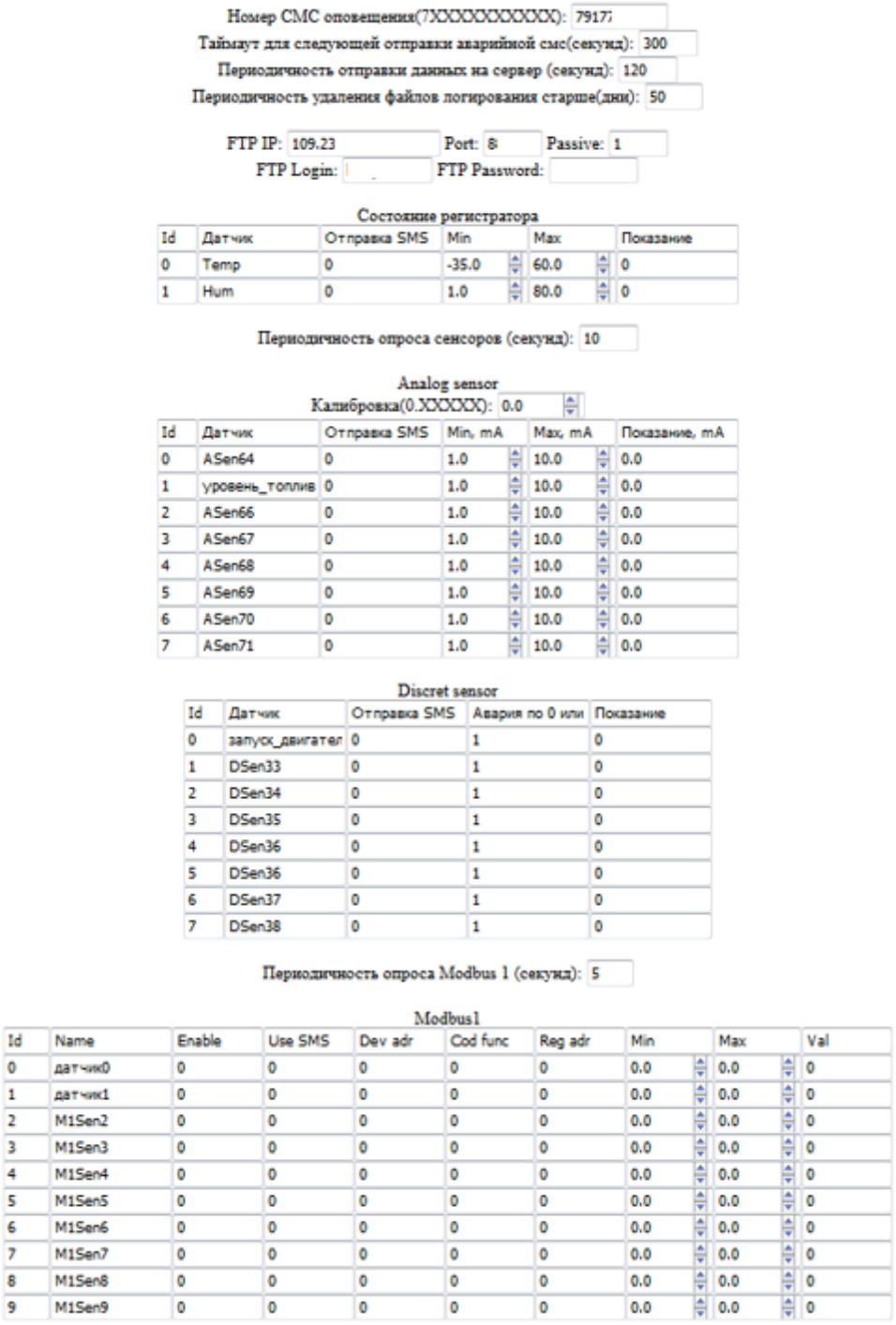


Рис. 2. Конфигуратор регистратора

Для визуализации и последующего анализа данных, собранных регистратором, было разработано программное обеспечение, позволяющее осуществ-

лять связь регистратора с сервером с последующим выводом информации на экран пользователя.

Программное обеспечение, написанное на языке Python, выполняет следующие функции:

– получение данных от неограниченного количества регистраторов и сохранение в БД SQL;

– визуализация сохраненных данных в виде графиков и показаний с возможностью навигации по времени и устройствам в WEB интерфейсе.

Данные собираются с регистраторов, установленных на контролируемом оборудовании.

Скомпилированное приложение позволяет осуществлять мониторинг состояний объектов газовой и нефтяной отрасли. Данные, полученные с регистраторов, сохраняются в БД SQL. Приложение визуализирует сохраненные данные в виде графиков и показаний с возможностью навигации по времени и устройствам в WEB интерфейсе. Таким образов, АПК предоставляет возможность автоматизировать процесс контроля состояния промышленных объектов и тем самым повысить безопасность работы объектов промышленного комплекса.

СПИСОК ЛИТЕРАТУРЫ

1. Гладышева И. В. Роль автоматизации операционных процессов в развитии производственной системы предприятий нефтегазового комплекса //Цифровая экономика и" Индустрия 4.0": проблемы и перспективы. – 2017. – С. 279-287.
2. Филиппов С. Новая технологическая революция и требования к энергетике //Форсайт. – 2018. – Т. 12. – №. 4.
3. Скобелев П. О. Интеллектуальные системы управления ресурсами в реальном времени: принципы разработки, опыт промышленных внедрений и перспективы развития //Приложение к теоретическому и прикладному научно-техническому журналу «Информационные технологии. – 2013. – №. 1. – С. 1-32.
4. Ярославцева Д. А. Пример внедрения интеллектуальных информационно-измерительных систем //Измерение. Мониторинг. Управление. Контроль. – 2018. – №. 1 (23).

УДК 004.023

Ш. З. КАШАЕВ
kashaev.schamil@yandex.ru
Науч. руководитель – д-р техн. наук, проф. А. Ф. ВАЛЕЕВА

Уфимский государственный авиационный технический университет

РЕШЕНИЕ ЗАДАЧИ МАРШРУТИЗАЦИИ ТРАНСПОРТНЫХ СРЕДСТВ С МНОЖЕСТВОМ ДЕПО ДЛЯ ДОСТАВКИ РАЗЛИЧНЫХ ГРУЗОВ

Аннотация. Объектом исследования является задача маршрутизации транспортных средств. В работе приводятся результаты проведенного анализа предметной области, обзора задачи маршрутизации транспортных средств с множеством депо, анализ методов решения задач маршрутизации.
***Ключевые слова*:** маршрутизации транспортных средств; множество депо; транспортная логистика, эвристические методы, генетический алгоритм.

Введение

Существует несколько уровней транспортных перевозок: внутрицеховые, перевозки в предприятии, перевозки между городами, регионами, странами, перевозки межконтинентального уровня. Целью оптимизации транспортной логистики является минимизация затрат необходимых для перевозок. В качестве затрат выступают разные ресурсы, такие как: стоимость обслуживания ТС, время, человеческий труд и т.д..

Задача транспортной логистики – оптимизация транспортных грузоперевозок. Это обусловлено тем, что затраты на транспортные операции, по разным оценкам составляют от 30-50% от общих логистических затрат [1]. Денежные траты на обслуживание транспортных средств являются большей частью всех транспортных издержек. Также стоит заметить, что цены на обслуживание поднимаются каждый год.

При перевозках из одного пункта в другие возникает проблема выбора рационального маршрута. Для составления маршрутов перевозок, с минимальными издержками, существуют транспортно-логистические услуги. На сегодняшний день для составления маршрутов практически все компании исполь-

зуют автоматизированные системы. Такой подход позволит снизить затраты от 15% до 35% [2].

Обзор задачи маршрутизации

Задача маршрутизации ТС (VRP – Vehicle Routing Problem) была представлена в 1959 году [3]. Имеется множество транспортных средств и множество клиентов, которых необходимо посетить. Также задаются ограничения: транспортное средство начинает и заканчивает свой путь в депо и клиент может быть обслужен только одним ТС. Необходимо составить маршрут для транспортных средств, при прохождении которого затраты были бы минимальны. Данная задача является NP-трудной, это означает, что сложность экспоненциально зависит от входных данных.

Существует несколько известных вариаций задачи маршрутизации, такие как: CVRP с ограниченной грузоподъемностью ТС, MDVRP с множеством депо, VRPTW с временными окнами, VRPSD с раздельной доставкой и т.д..

Задача маршрутизации ТС с несколькими депо (MDVRP – Multi Depot Vehicle Routing Problem) является расширением CVRP. Заключается в нахождении плана маршрутов для парка ТС с одинаковыми ограничениями на грузоподъемность, расположенных в разных депо и обслуживающих множество клиентов, так чтобы затраты были минимальны. Пример решения такой задачи представлен на рисунке 1.

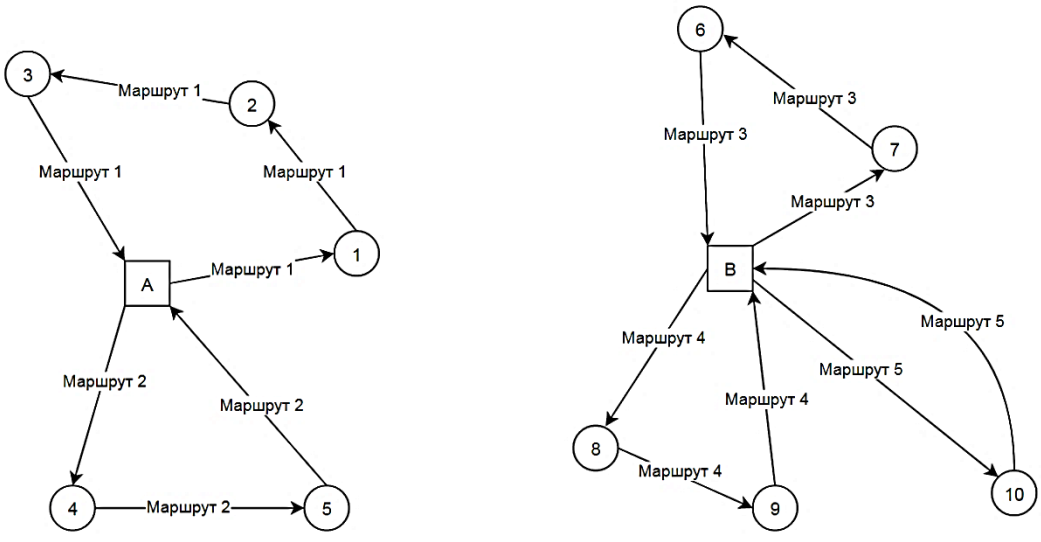


Рис. 1. Пример решения задачи маршрутизации ТС с несколькими депо

Входные данные задачи: 2 депо и 12 клиентов. Решениями являются 2 маршрута для депо А и 3 маршрута для депо В:

– Депо А – Маршрут 1 (А-1-2-3-А) и Маршрут 2 (А-4-5-А)

– Депо В – Маршрут 3 (В-7-6-В), Маршрут 4 (В-8-9-В) и Маршрут 5 (В-10-В)

Методы решения и оценка эффективности

Существует несколько походов к решению задач маршрутизации:

1. Точные методы (*Exact Approaches*).

Точные методы, перебирают все возможные варианты решения, пока не будет достигнуто оптимальное. Такой подход не выгоден при решении таких типов задач, так как, при увеличении размеров входных данных, время решения экспоненциально растет. Примерами методов данного класса являются: метод ветвей и границ, метод ветвей и отсечений.

2. Эвристические методы (*Heuristics*).

Эвристические алгоритмы, при больших размерах входных данных, позволяют находить рациональные решения за приемлемое время. Эвристика не гарантирует получение оптимального решения. Эвристические методы делятся на 2 класса: простые эвристики и метаэвристики. Эвристические алгоритмы часто применяются для решения задач класса NP-трудных.

3. Метаэвристические методы (*Meta-Heuristics*).

Являются подклассом эвристических методов. Примерами метаэвристик являются: имитация отжига, поиск с запретами генетический алгоритм, муравьиный алгоритм.

4. Простые эвристики (*Simple Heuristics*). Примеры простых эвристик: сохранение, заметание, двухфазный алгоритм.

Так как задача маршрутизации ТС с несколькими депо является NP-трудной, то для нахождения решения было бы эффективней применение эвристических алгоритмов.

Далее представлена общая схема решения задачи маршрутизации ТС с несколькими депо. Решение будет состоять из 3-х частей:

1. Распределение клиентов по депо.
2. Построение начальных маршрутов для каждого депо.
3. Построение рациональных маршрутов для каждого депо.

Для решения была выбрана метаэвристика генетический алгоритм. Этот метод основан на работе с популяцией решений и генетических операторах. Для сравнения были взяты 2 модификаций алгоритма: генетического алгоритма с мутацией и генетического алгоритма со скрещиванием, мутацией и с использованием стратегии элитизма.

Эксперимент 1. Эксперимент 1 проводился на наборе данных из 2 депо и 22 клиентов. В депо разные парки ТС. Для тестового набора известны названия населенных пунктов, в которых находятся депо и клиенты, спрос каждого клиента, парки ТС с грузоподъемностью и расходом. Количество итераций для генетических алгоритмов было взято 15 и 30. Размеры популяции были взяты 15 и 30. Количество элитных особей для генетического алгоритма со скрещиванием, мутацией и с использованием стратегии элитизма было взято 5 и 10.

Результаты работы алгоритмов с первым тестовым набором представлены в таблице 1. В ячейках указаны цены конечных маршрутов доставки в рублях. В скобках указаны количество итераций и размер популяций, а также для генетического алгоритма со скрещиванием, мутацией и с использованием стратегии элитизма указано количество элитных особей. ГАм – генетический алгоритм с мутацией, ГАсмэ - генетический алгоритм со скрещиванием, мутацией и с использованием стратегии элитизма.

Таблица 1

Сравнение результатов работы алгоритмов для задачи маршрутизации ТС с множеством депо на первом наборе данных

№	ГАм(15,15)	ГАсмэ(15,15,5)	ГАм(30,30)	ГАсмэ(30,30,10)
1	124214,08	124232,8	124214,08	**122066,6**
2	**123978,69**	122841,42	124214,08	122841,42
3	124214,08	124177,69	**122738,5**	122841,42
4	124214,08	122841,42	122841,42	**122066,6**
5	125923,11	**122066,6**	123964,27	**122066,6**

Эксперимент 2. Эксперимент 2 проводился на наборе данных из 2 депо и 22 клиентов. В депо разные парки ТС. Для тестового набора известны названия населенных пунктов, в которых находятся депо и клиенты, спрос каждого клиента, парки ТС с грузоподъемностью и расходом. Количество итераций для генетических алгоритмов было взято 15 и 30. Размеры популяции были взяты 15 и 30. Количество элитных особей для генетического алгоритма со скрещиванием, мутацией и с использованием стратегии элитизма было взято 5 и 10.

Результаты работы алгоритмов со вторым тестовым набором представлены в таблице 2.

Таблица 2

Сравнение результатов работы алгоритмов для задачи маршрутизации ТС с множеством депо на втором наборе данных

№	ГАм(15,15)	ГАсмэ(15,15,5)	ГАм(30,30)	ГАсмэ(30,30,10)
1	102922,55	94366,98	97105,08	85281,02
2	103559,67	93993,37	97138,92	84199,96
3	107144,30	95738,54	**94138,53**	**83867,50**
4	**101497,52**	**89880,82**	98801,16	84046,45
5	104869,84	90168,64	97279,69	85765,40

Вывод: по результатам из таблиц 1 и 2 можно сделать вывод о том, что генетический алгоритм со скрещиванием, мутацией и стратегией элитизма дает лучшие решения по сравнению с генетическим алгоритмом только с мутацией.

СПИСОК ЛИТЕРАТУРЫ

1. Алесинская Т.В. Основы логистики. Общие вопросы логистического управления: Учебное пособие. – Таганрог: Изд-во ТРТУ, 2005. – 121 с.
2. Моргунов В.И., Джабраилов А.Э. Маркетинг. Логистика. Транспортно-складские логистические комплексы – М.: Издательско-торговая корп. «Дашков и К», 2010. – 388 с.
3. B. Dantzig, J. H. Ramser. The Truck Dispatching Problem: Management Science. – 1959. – vol. 6, no. 1 – pp. 80 – 91.

УДК 004

Ю.Д. САЛИМОНЕНКО
iyulya99@gmail.ru
Науч. руководитель – канд. техн. наук, проф. А. Ф. ВАЛЕЕВА

Уфимский государственный авиационный технический университет

РЕШЕНИЕ ЗАДАЧИ МАРШРУТИЗАЦИИ ДЛЯ ДОСТАВКИ ТОВАРА С УЧЕТОМ ВРЕМЕННЫХ ОГРАНИЧЕНИЙ

Аннотация. Объектом исследования является процесс построения рационального маршрута. Предметом исследования являются модели и методы построения рационального маршрута. В работе приводятся результаты проведенного анализа предметной области, аналитического обзора программных решений для решения задачи построения рациональных маршрутов, результаты анализа методов решения задач маршрутизации транспорта, который позволил выбрать методы и разработать алгоритмы для решения задачи маршрутизации транспорта с временными окнами. С помощью разработанного программного продукта был проведен вычислительный эксперимент, позволивший сделать выводы о том, что наилучшей моделью для построения оптимального маршрута для доставки товаров клиентам в рассматриваемых условиях является разработка эволюционного алгоритма с временными ограничениями.
Ключевые слова: построение оптимального маршрута; задача маршрутизации транспорта с временными окнами; эволюционный алгоритм; эвристические алгоритмы

Обзор классов задач маршрутизации транспортных средств

Задача маршрутизации транспортных средств является одним из классов задач логистики, имея своей целью минимизацию транспортных расходов, пройденного расстояния или времени доставки груза.

Впервые проблема маршрутизации была предложена Г. Дангицом и Дж. Рамсером в 1959 году. Задача заключалась в поиске оптимального маршрута для доставки конкретно заданного количества одних товаров, используя транспортные средства одинаковой грузоподъемности. Авторы поставили математическую формулировку и решили задачу о поставке бензина на заправочные станции. Данная задача является одной из самых известных в области комбинаторной оптимизации даже на сегодняшний день.

В условиях реального времени оптимизация доставки грузов является актуальной проблемой для большого количества предприятий. С увеличением объемов производства нарастает сложность распределения ресурсов, ТС могут использоваться по выделенным ресурсам неэффективно, происходит рост кон-

куренции и, как следствие, может снижаться качество оказываемых услуг. В связи с чем фирмам со временем требуется автоматизация распределения ресурсов, спрос на траспортно-логистические услуги повышается каждый год. Особенно актуально решение задач маршрутизации при внутренних перевозках по городу, т.к. в настоящее время 75% от структуры грузоперевозок составляют перевозки мелкопартийных товаров.

Благодаря цифровизации транспортная логистика имеет возможность стать более экономной для компаний. Речь идет о снижении трудозатрат на обработку заказов от клиентов, упрощении взаимодействия с заказчиками, замене бумажной документации электронной, увеличения продуктивности, технологичности и скорости работы. За 2020 год спрос на автоматизацию рынка логистических услуг увеличился почти на 20% в связи со стремлением организаций уменьшить транспортные расходы. При этом следует учесть и исследования экспертов [], которые говорят о возможной экономии от 3 до 30% на транспортных расходах в зависимости от степени автоматизации и загруженности компании.

Общий вид задачи транспортной маршрутизации VRP выглядит следующим образом: имеется парк ТС, которые изначально находятся в депо, являющимся началом и концом каждого машрута, и определенное количество покупателей, которым необходимо доставить товар (Рисунок 1.1). Задана матрица неотрицательных стоимостей или расстояний между клиентами. Целью задачи VRP является нахождение маршрута для каждого ТС, такого, чтобы все покупатели были обслужены ровно одним ТС и чтобы общая стоимость маршрутов была минимальной.

Но большинство VRP задач при практическом применении оказываются сложнее, чем классическая модель. Например, существует следующая классификация моделей задач VRP, которая была предложена в работе P. Toth и D. Vigo [1]:

1. Задача маршрутизации ТС с учетом грузоподъемности (Capacitated Vehicle Routing Problem, CVRP): каждое ТС имеет ограниченную грузоподъемность. Разновидностями задачи CVRP являются задачи 2L-CVRP и 3L-CVRP, в которых помимо грузоподъемности ТС учитывается размещение груза внутри ТС. В задаче 2L-CVRP – двумерное размещение, в задаче 3L-CVRP – трехмерное размещение.

2. Задача маршрутизации ТС с временными окнами (Vehicle Routing Problem with Time Windows, VRPTW): у каждого клиента есть временное ограничение, во время которого он должен быть обслужен. Как правило, клиент имеет возможность сделать заказ в течение рабочего дня. При этом обслуживание клиента вне рамок временного окна не допускается. Это одна из наиболее сложных классификаций данной задачи. Решение этой задачи позволяет сделать вывод, можно ли обслужить всех клиентов. Если ответ отрицательный, то ставится задача обслужить максимально возможное число клиентов.

Благодаря решению задачи VRPTW [9] можно заранее смоделировать перевозки и оценить приблизительно время доставки каждого груза. Клиенты, которых не смогут обслужить, оповещаются заранее. В некоторых разновидностях задачи VRPTW обслуживание клиента в определенном заранее временном окне не является критически важным условием, но его нарушение добавляет некий штраф к значению целевой функции. Кроме того, решение задачи VRPTW позволяет подобрать время выезда и, тем самым, исключить простои автотранспорта.

3. Задача маршрутизации ТС с множеством депо (Multiple Depot Vehicle Routing Problem, MDVRP): используется несколько депо для обслуживания клиентов.

4. Задача маршрутизации ТС с раздельной доставкой (Split Delivery Vehicle Routing Problem, SDVRP): каждый клиент может быть обслужен одновременно несколькими ТС.

5. Периодическая задача маршрутизации ТС (Periodic Vehicle Routing Problem, PVRP): задан период планирования в размере нескольких дней (временной горизонт), когда клиенты посещаются с разной частотой, заданной для каждого клиента.

6. Задача маршрутизации ТС с немедленным возвратом товаров (Vehicle Routing Problem with Pick-up and Delivery, VRPPD): клиенты могут возвращать некоторые товары в депо.

7. Задача маршрутизации ТС с возвратом товаров (Vehicle Routing Problem with Backhauls, VRPB): клиенты могут возвращать некоторые товары в депо, но только после того, как весь товар будет доставлен клиентам.

8. Задача маршрутизации ТС с возможностью дозагрузки (Vehicle Routing Problem with Satellite Facilities, VRPSF): ТС могут дополнительно загрузиться на маршруте в промежуточных пунктах-складах.

9. Задача маршрутизации ТС со случайными данными (Stochastic Vehicle Routing Problem, SVRP): некоторые компоненты задачи (количество и спрос клиентов, расстояния между городами и клиентами) могут иметь случайное поведение.

В результате анализа методов сделан следующий вывод:

Наилучшими алгоритмами для решения задач VRP являются метаэвристики, которые дают возможность преодолевать локальный оптимум в процессе поиска решений и позволяют находить решение NP-трудных задач.

Алгоритм для решения задачи маршрутизации с временными окнами

В статье определен эволюционный алгоритм для поиска рациональных маршрутов доставки груза клиентам, общая схема которого предложена в работах [1,2,3]

Алгоритм $(\mu+\lambda)$ – EA, где $\mu = 1$, $\lambda=1,2$, реализация для задачи маршрутизации с временными окнами.

Выходные данные: рациональный маршрут xoptimal ij.

Evolution(): поиск решения, цикл по количеству итераций от 1 до n

Заполнение

GenerateInitialPopulation(): генерация начальной популяции размером mu

GetRandomSolution(): генерация случайного решения

Мутация lamda-раз (генерация новых решений на основе старых случайных решений, цикл от 1 до lamda)

Mutation(): Выбирается случайная особь, генерируется новое решение путем перестановки двух городов

Отбор наилучших решений:

FilterBestSolutions(): фильтрация наилучших решений

CalculateObjectiveFunction(): вычисление целевой функции

(Если временное окно нарушено, то cost = cost + penalty_time)

Предложена математическая модель задачи доставки груза различным клиентам с временными окнами. В качестве набора тестовых данных использовались реальные данные поступающих заявок на доставку витаминов, проф. средств/инвентаря по уборке, запасы которых хранятся на складе компании. Для проведения сравнительного анализа с результатами были были использованы разработанные алгоритмы (1+1)-EA и (1+2)-EA.

Проводилось тестирование разработанного эволюционного алгоритма (1+1)-EA и (1+2)-EA для решения задачи маршрутизации транспортных средств с временными окнами (VRPTW). Так как эвристические алгоритмы не могут гарантировать нахождение лучшего решения, в экспериментах тестовый набор прогонялся 8 раз для нахождения лучшего решения.

Эксперимент. Эксперимент проводился на тестовом наборе из 17 клиентов и временных окон для 8 клиентов. Для тестового набора известны:

Координаты депо = Стерлитамак;

Грузоподъемность ТС = 1500 кг;

Координаты и спрос клиентов;

Временные окна для некоторых клиентов;

Количество итераций для эволюционных алгоритмов было взято 200 и 300.

Результаты выполнения алгоритмов представлены в таблице 3.5. В ячейках таблицы указаны расстояния конечного маршрута. В первом столбце (1,…,8) указан номер прогона тестового набора. 200I, 300I - количество итераций.

Таблица 1

Сравнение результатов работы алгоритмов для задачи маршрутизации ТС с временными ограничениями

Номер теста	(1+1)-EA (200I) (руб.)	(1+2)-EA (200I) (руб.)	(1+1)-EA (300I) (руб.)	(1+2)-EA (300I) (руб.)
1	4860	5440	4737	5403
2	5617	4748	5829	4923
3	5120	5278	5261	4878
4	4981	4883	6088	4820
5	5669	5551	5171	4414
6	5693	4736	5636	5072
7	4913	4461	4926	50342
8	5473	5415	5073	4601

Выводы: из полученных результатов в таблице 1 был сделан вывод о том, что для задачи маршрутизации транспортных средств с временными окнами с помощью эволюционного алгоритма (1+2)-EA (300 итераций) были получены лучшие решения.

После анализа результатов, полученные с помощью алгоритмов (1+1)-EA и (1+2)-EA, можно сделать вывод, что решения, полученные алгоритмом (1+2)-EA получаются лучше чем решения, полученные алгоритмом (1+1)-EA. Это можно объяснить тем, что в алгоритме (1+2)-EA при каждой итерации вместо двух, как в (1+1)-EA, происходит сравнение трех маршрутов. Отсюда можно сделать вывод, что при решении прикладных задач с большим количеством клиентов лучше использовать эволюционный алгоритм (1+2)-EA вместо (1+1)-EA.

СПИСОК ЛИТЕРАТУРЫ

1. Toth P., Vigo D. The Vehicle Routing Problem. – Philadelphia: Society for Industrial and Applied Mathematics. – 2002. – 386 p.
2. Land A.H., Doig A.G. An automatic method of solving discrete programming problems // Econometrica. – 1960. – V. 28. – P. 497-520.
3. Гладков Л.А., Гладкова Н.В. Особенности и новые подходы к решению динамических транспортных задач с ограничением по времени // Известия ЮФУ. Технические науки. – 2013. – № 7 (144). – С. 178-185.
4. Гладков Л.А., Курейчик В.В., Курейчик В.М. Генетические алгоритмы: Учебное пособие. Под ред. В.М. Курейчика. – Ростов-на-Дону: ООО «Ростиздат», 2004. – 400 с.
5. Кощеев И.С. Оптимизация доставки груза потребителям с учетом его размещений внутри транспортных средств на основе эвристических методов: Дис. на соиск. учен. степ. канд. техн. наук (05.13.01) / УГАТУ. – Уфа, 2015. – 133 с.

УДК 004

Ю. А. СНЕЖКО, В. М. ОГИЛЬКО
julia.sneg@mail.ru, nochnoymonstr@gmail.com
Науч. руководитель – канд. техн. наук, ст. науч. сотр. Г. Р. ВОРОБЬЕВА

Уфимский государственный авиационный технический университет

ВЕБ-ГИС ДЛЯ ОТОБРАЖЕНИЯ ГЕОМАГНИТНЫХ СТАНЦИЙ

Аннотация. В настоящей работе обсуждаются результаты разработки информационной системы на основе геоинформационных технологий, предназначенной для исследования и аналитической обработки геомагнитных данных. Ожидается, предложенный программный способ визуализации позволит пользователю удобно управлять данными на карте.
Ключевые слова: ГИС; геоинформационная система; геомагнитные данные; актуальность.

Введение. На данный момент существует множество задач, которые требуют для своего решения неравномерно распределенных данных. В случае географии, одной из таких областей являются задачи, связанные с геомагнитным полем Земли.

Составление достоверной карты геомагнитного поля является задачей, требующей точного следования расположению точек в системе координат. Чтобы начать составлять карту требуется получить огромное количество данных, источником которых являются геомагнитные станции, расположенные по всему миру. В настоящее время данные о геомагнитном поле Земли регистрируются такими станциями непрерывно. Это облегчает этап получения данных за определенный промежуток времени. Но даже с таким огромным количеством данных, при размещении их на карте остаются места, где параметры магнитного поля известны не будут. Возможных причин отсутствия данных немало. Одной из них является неспокойная геомагнитная обстановка, из-за которой часть станций может не зафиксировать данные.

Актуальность. Практическую значимость получения достоверных пространственных данных сложно переоценить, поэтому решению проблемы уделяется большое внимание. Наше приложение позволит пользователю удобно управлять данными на карте и при необходимости скачивать их.

Целью данной статьи является разработка Веб-ГИС для отображения геомагнитных станций.

Исходные данные. В качестве исходных данных используются геомагнитные данные, имеющиеся в открытом доступе на портале SuperMAG в геомагнитной системе координат N, E, Z.

Обработка, визуализация и интерпретация геомагнитных данных.

Так как точек слишком много для ручной обработки, мы получаем координаты при помощи парсинга файлов с данными о станциях. Затем каждой точке присваиваются координаты и она отрисовывается с помощью маркера.

Архитектура веб-ориентированной информационной системы.

Предлагаемая система визуализации основана на архитектуре клиент-сервер, типичной для веб-приложений. Взаимодействие клиент-сервер осуществляется следующим образом (рис 1).

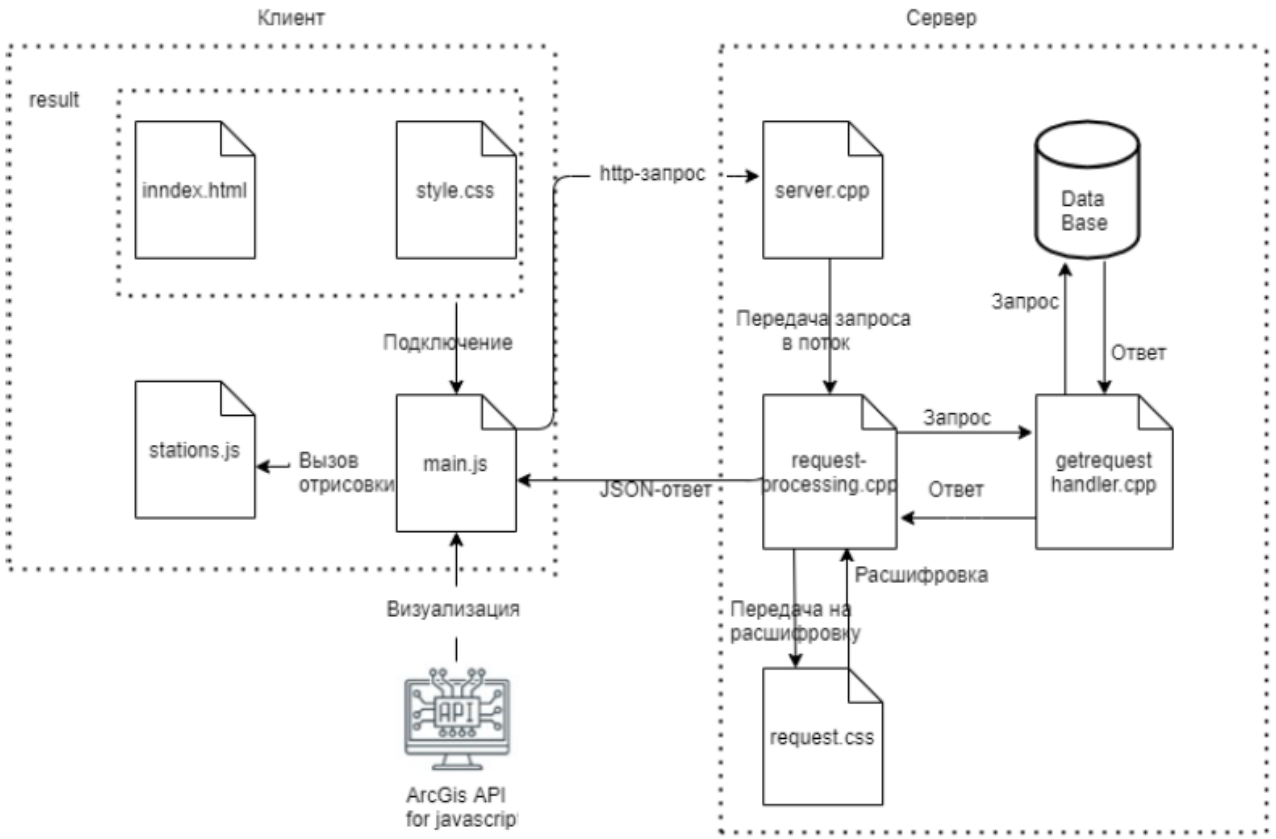


Рис. 1. Архитектура информационной системы

Обсуждение результатов. В ходе проделанной работы была разработана веб-ориентированная информационная система, которая представляет из себя одностраничный сайт. Сайт можно разбить на 3 основных составляющих:

Блок - меню

Блок – карта

Блок – фильтры

Блок-информация

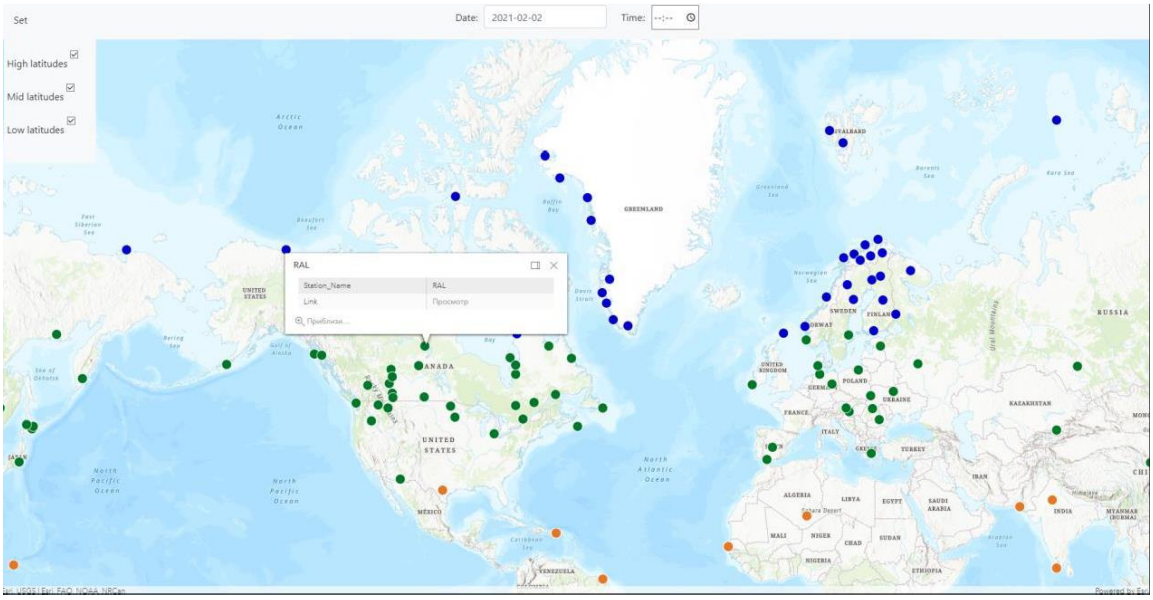


Рис. 2. Экранная форма разработанной Веб-ГИС

Блок – меню состоит из трех компонентов:

– Панель выбора даты – позволяет выбрать дату для просмотра на выбранную дату.

– Панель выбора даты – позволяет выбрать время для просмотра на выбранное время.

– Выпадающая панель “Set” – позволяет выбрать станции для отображения в зависимости от их расположения.

Блок – карта отвечает за:

– Отображение станций на карте с доступными для скачивания данными на выбранную пользователем дату

– Возможность просмотра информации о выбранной станции путем нажатия левой кнопкой мыши на нужную точку

Блок – фильтры позволяет с помощью чек-боксов выбрать станции для отображения на карте: расположенные в высоких широтах, в средних широтах и экваториальных.

Блок-информация содержит в себе информацию о выбранной станции, такую как код станции и ссылку на данные с нее.

Таким образом была разработана удобная информационная система для визуализации геомагнитных станций на карте.

Научная новизна. ГИС с подобными функциями в свободном доступе найти не удалось. Разработанная Веб-ГИС как раз предоставляет пользователю необходимый функционал.

Заключение

В ходе работы было создано приложение для отображения геомагнитных станций.

Работа поддержана грантом РФФИ № 20-07-00011-а.

СПИСОК ЛИТЕРАТУРЫ

1. Демьянов В. В., Савельева Е. А. Геостатистика теория и практика / Ин-т проблем безопасного развития атомной энергетики РАН. [под редакцией Р. В. Арутюняна] Москва: Наука, 2010. - 327 с.
2. Документация Python 3.7.11 // [Электронный ресурс] : сайт. — URL: https://docs.python.org/3.7/ (дата обращения 20.07.21)
3. Документация JavaScript // [Электронный ресурс] : сайт. — URL: https://devdocs.io/javascript/ (дата обращения 25.07.21)
4. Документация ArcGIS API for JavaScript // [Электронный ресурс] : сайт. — URL: https://developers.arcgis.com/documentation// (дата обращения 27.07.21)

УДК 004.051 + 004.623 + 004.922

Н. С. ТАРАТОРИН
www.klaem-assassin@mail.ru
Науч. руководв. – канд. физ.-мат. наук, доц. Е. И. ПРОКУДИНА

Уфимский государственный авиационный технический университет

МАТЕМАТИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ПОСТРОЕНИЯ ИНФОРМАТИВНОЙ СЦЕНЫ В ЗАДАЧЕ ВИЗУАЛИЗАЦИИ ДАННЫХ ПРОФИЛЕМЕТРИИ

Аннотация. Рассмотрена математическая база особенностей построения сцены визуализации данных профилеметрии, позволяющих добиться информативной картинки, на основе которой пользователь разработанной программы смог бы сформулировать качественное заключение по проведенному исследованию.
***Ключевые слова*:** трехмерная графика; профилеметрия; построение сцены.

В данной работе рассматривается задача разработки математического обеспечения, позволяющего построить трехмерную версию скважины по результатам произведенной профилеметрии и некоторых режимов их визуализации. В статье [1] описано геофизическое исследование профилеметрии и рассмотрен процесс восстановления аппроксимированной трехмерной цилиндрической формы исследуемого объекта – скважины. Цель текущей работы – рассмотреть дополнительные аспекты организации визуализации, позволяющие пользователю получить информативную сцену для своих нужд, а именно:

– отсечение цилиндрической формы представления данных плоскостью;

– построение развертки скважины;

– построение поверхностной сетки;

– построение осей для двух видов представления данных.

Ниже приведено описание данных профилеметрии. Более подробно процесс геофизического исследования профилеметрии и вид прибора профилемера описан в работе [1].

N – количество рычагов;

M – количество глубин замеров;

$\lambda = 2 \cdot \pi/N$ – угол между соседними рычагами;

$V = \begin{pmatrix} v_{1,1} & \cdots & v_{1,M} \\ \vdots & \ddots & \vdots \\ v_{N,1} & \cdots & v_{N,M} \end{pmatrix}$ – матрица расстояний от точки соприкосновения рычага со стенкой скважины до центра прибора;

$D = (d_1 \quad \ldots \quad d_M)$ – вектор глубин, на которых были произведены замеры.

Считаем, что изначально все, что доступно пользователю, это цилиндрическое представление данных. В данном типе визуализации у пользователя нет удобной возможности оценить внутреннее состояние стенок скважины (только если не поместить точку обзора внутрь ствола скважины, что считается неудобным), поскольку при расположении точки обзора вне ствола скважины будет видна лишь внешняя сторона ствола. Решено предоставлять пользователю возможность отобразить данные в цилиндрической форме отсеченной плоскостью, совпадающей с центральной осью прибора. Пусть $\overline{vn} = (A \quad 0 \quad C)^T$ – вектор нормали плоскости отсечения. Определена следующая функция фильтрации, позволяющая произвести описанную операцию:

$$filter\left(\overline{vn}, P = \begin{pmatrix} x \\ y \\ z \end{pmatrix}\right) = \left\{ p = \begin{pmatrix} xp \\ yp \\ zp \end{pmatrix} \in P \,\middle|\, A \cdot xp + C \cdot zp \geq 0 \right\}$$

У данной операции есть один недостаток – часть данных не отображается для пользователя, однако то, что было отражено, визуализируется без всяческих искажений.

Под разверткой в данной работе будем понимать результат некоторой трансформации, которую можно представить как разворот рулона бумаги. Поскольку исходные данные являются описанием точек объекта, только лишь в идеальных условиях который должен быть приближен к цилиндру, необходимо скорректировать данное преобразование вводом параметра радиуса r^{flat}, вокруг которого будет производиться разворот. От этого параметра будет зависеть, каким деформациям подвергнется конечная фигура (деформация заключа-

ется в изменении расстояний между вершинами: если $v_{i,j}$ меньше r^{flat}, то соответствующая точка будет ближе к соседним точкам развертки, нежели цилиндрической формы представления; если больше – то дальше от соседних). Как пример, можно взять этот параметр равный минимальному или среднему значению из зафиксированных расстояний. Математически данное преобразование представим следующим образом:

$$P_{i,j}^{flat} = \begin{pmatrix} x_{i,j} \\ y_{i,j} \\ z_{i,j} \end{pmatrix} = \begin{cases} x_{i,j} = \pi \cdot r^{flat} \cdot \left(\left(\frac{2 \cdot (i-1)}{N} \right) - 1 \right) \\ y_{i,j} = d_j \\ z_{i,j} = v_{i,j} \end{cases}$$

В отличие от отсечения плоскостью данное преобразование позволяет представить данные таким образом, чтобы внешняя и внутренняя поверхности всей скважины, а не части, были полностью просматриваемы пользователем, однако стоит помнить, что данные были подвержены хоть и незначительной, но все же деформации.

Описываемый процесс построения поверхностной сетки годится как для цилиндрической формы представления данных, так и для развертки. Построение поверхностной сетки разделено на два этапа: построение вертикальных и горизонтальных линий. Вертикальные линии принято строить вдоль точек полученных данных:

$$Ver = \left(ver_i \middle| ver_i = \left(ver_{i,j} \middle| ver_{i,j} = p_{i,j} \in P \right), j = \overline{1, M} \right), i = \overline{1, N}$$

Горизонтальные же линии необходимо строить с некоторым постоянным шагом по глубине $step$. Стоит заметить, что горизонтальные линии необязательно будут проходить через точки, полученные в результате преобразования исходных данных. Пусть необходимо отобразить сегмент скважины от кровли $roof$ до подошвы $sole$. Определим два индекса, обозначающие первый (ri) и последний (si) номера глубины исходных данных, входящих в интервал визуализации.

$$ri: d_{ri} > roof, \nexists d_j \in D: d_{ri} > d_j > roof$$

$$si: d_{si} < sole, \nexists d_j \in D: d_{si} < d_j < sole$$

Введем две функции, позволяющие найти индексы двух ближайших глубин ld и ud из исходного набора данных к некоторой заданной.

$$ld(d) = \begin{cases} i: d_i < d, ri \le i \le si, \nexists j, ri \le j \le si: d_i < d_j \le d \\ 0, otherwise \end{cases}$$

$$ud(d) = \begin{cases} i: d_i > d, ri \le i \le si, \nexists j, ri \le j \le si: d_i > d_j \ge d \\ 0, otherwise \end{cases}$$

Предположим, что горизонтальная линия должна находиться на некоторой глубине d, причем $roof \le d \le sole$, тогда она может быть отображена по следующему набору точек hor.

$$hor(d) = \left(x \middle| x = \frac{P_{i,ld(d)} \cdot \left| d - d_{ud(d)} \right| + P_{i,ud(d)} \cdot \left| d - d_{ld(d)} \right|}{\left| d_{ud(d)} - d_{ld(d)} \right|} \right), i = \overline{1, N}$$

Пусть первая горизонтальная линия будет отрисована вдоль глубины d_{ri}. Тогда количество горизонтальных линий HC можно легко посчитать, воспользовавшись следующей формулой.

$$HC = \left\lfloor \frac{sole - roof}{step} \right\rfloor$$

Теперь можно определить набор точек Hor, являющихся вершинами всех горизонтальных линий, с помощью следующей формулы.

$$Hor = \left(hor_j \middle| hor_j = hor(d_{ri} + step \cdot j) \right), j = \overline{1, HC}$$

Таким образом получен набор вершин, которому можно сопоставить множество отрезков и получить поверхностную сетку.

Решено, что в цилиндрической форме представления необходимо отобразить оси, позволяющие оценить принадлежность точки какой-либо глубине. Какую-либо дополнительную информацию отображать не стоит. Решено, что цилиндр будет информативно смотреться при визуализации с двумя отрезками длиной равной длине отображаемой скважины параллельной ее оси глубин OY. Очевидно, что такие оси можно описать двумя парами точек, по которым можно построить два отрезка, однако осталось решить, в какой конкретно плоскости они должны быть отрисованы. Решено производить поворот осей в зависи-

мости от положения камеры. Введены функции построения одного отрезка координатных осей $Axis^{cylinder}$ и $Axes^{cylinder}$, определяющая четыре вышеописанных точки, приведенная в следующей формуле ($roof$ – кровля визуализируемого интервала, $sole$ – подошва).

$$Axis^{cylinder}(\alpha) = \begin{pmatrix} \left(\max\limits_{i=\overline{1,N},j=\overline{1,M}} v_{i,j} \cdot cos\,\alpha\,, roof, \max\limits_{i=\overline{1,N},j=\overline{1,M}} v_{i,j} \cdot \sin\alpha\right)^T \\ \left(\max\limits_{i=\overline{1,N},j=\overline{1,M}} v_{i,j} \cdot cos\,\alpha\,, sole, \max\limits_{i=\overline{1,N},j=\overline{1,M}} v_{i,j} \cdot \sin\alpha\right)^T \end{pmatrix}$$

$$Axes^{cylinder}(\alpha) = \left(Axis^{cylinder}\left(\alpha + \frac{\pi}{2}\right), Axis^{cylinder}\left(\alpha - \frac{\pi}{2}\right)\right)$$

Для осевой коробки развертки введем понятие AABB (Axis Aligned Bounding Box), под которым следует понимать параллелепипед минимального размера, описывающий некоторую фигуру, причем каждое из его ребер параллельно одной из осей координат. Данная фигура интересна тем, что она очень легко строится, достаточно лишь взять минимальные и максимальные координаты вершин описываемого ею тела. AABB может быть описан восьмью точками, представленных в следующей формуле.

$$AABB\left(P^{flat}\right) = \begin{pmatrix} \left(\min\limits_{i=\overline{1,N},j=\overline{1,M}} x_{i,j}\,, \min\limits_{i=\overline{1,N},j=\overline{1,M}} y_{i,j}\,, \min\limits_{i=\overline{1,N},j=\overline{1,M}} z_{i,j}\right)^T \\ \left(\min\limits_{i=\overline{1,N},j=\overline{1,M}} x_{i,j}\,, \min\limits_{i=\overline{1,N},j=\overline{1,M}} y_{i,j}\,, \max\limits_{i=\overline{1,N},j=\overline{1,M}} z_{i,j}\right)^T \\ \left(\min\limits_{i=\overline{1,N},j=\overline{1,M}} x_{i,j}\,, \max\limits_{i=\overline{1,N},j=\overline{1,M}} y_{i,j}\,, \min\limits_{i=\overline{1,N},j=\overline{1,M}} z_{i,j}\right)^T \\ \left(\min\limits_{i=\overline{1,N},j=\overline{1,M}} x_{i,j}\,, \max\limits_{i=\overline{1,N},j=\overline{1,M}} y_{i,j}\,, \max\limits_{i=\overline{1,N},j=\overline{1,M}} z_{i,j}\right)^T \\ \left(\max\limits_{i=\overline{1,N},j=\overline{1,M}} x_{i,j}\,, \min\limits_{i=\overline{1,N},j=\overline{1,M}} y_{i,j}\,, \min\limits_{i=\overline{1,N},j=\overline{1,M}} z_{i,j}\right)^T \\ \left(\max\limits_{i=\overline{1,N},j=\overline{1,M}} x_{i,j}\,, \min\limits_{i=\overline{1,N},j=\overline{1,M}} y_{i,j}\,, \max\limits_{i=\overline{1,N},j=\overline{1,M}} z_{i,j}\right)^T \\ \left(\max\limits_{i=\overline{1,N},j=\overline{1,M}} x_{i,j}\,, \max\limits_{i=\overline{1,N},j=\overline{1,M}} y_{i,j}\,, \min\limits_{i=\overline{1,N},j=\overline{1,M}} z_{i,j}\right)^T \\ \left(\max\limits_{i=\overline{1,N},j=\overline{1,M}} x_{i,j}\,, \max\limits_{i=\overline{1,N},j=\overline{1,M}} y_{i,j}\,, \max\limits_{i=\overline{1,N},j=\overline{1,M}} z_{i,j}\right)^T \end{pmatrix}$$

Осталось разметить стороны AABB сеткой, отображая полезную информацию. Так вдоль оси OY необходимо отобразить глубины точек, вдоль оси OZ – значения, зафиксированные профилемером, а вдоль оси OX – номера каналов. Таким образом получится 6 размеченных сектора плоскостей, отображающие ту или иную информацию, причем взаимно параллельных из них несут одну и ту же информацию. Предполагается, что наблюдение за объектом, заключенного со всех сторон в размеченный AABB, будет затрудненным, поэтому необходимо позаботиться об отсечении трех граней из шести, оставляя только те, что лежат за разверткой относительно точки обзора.

Рассмотренные математические модели реализованы в программном обеспечении Prime компании ООО НПЦ “ГеоТЭК” в модуле WellProfile. Три примера построенной сцены приведены ниже:

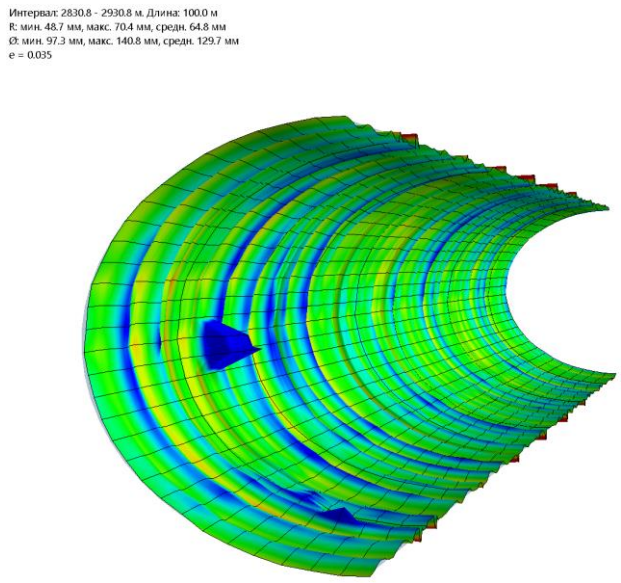


Рис. 1. Цилиднрическая форма представления данных
с отсеченнием и поверхностной сеткой

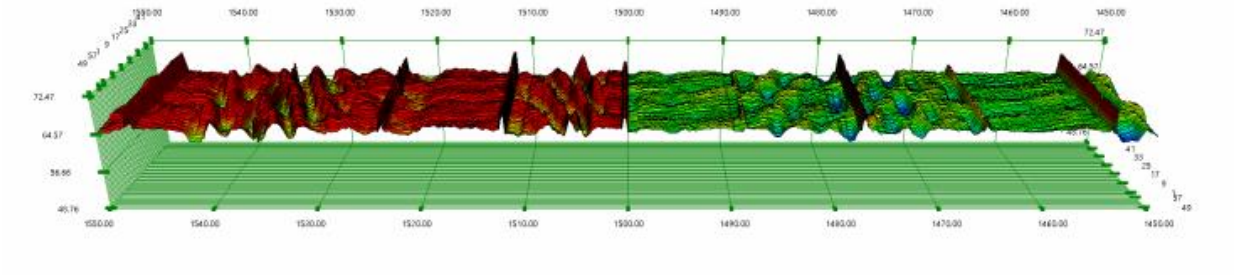


Рис. 2. Развертка с поверхностной сеткой и осевой коробкой

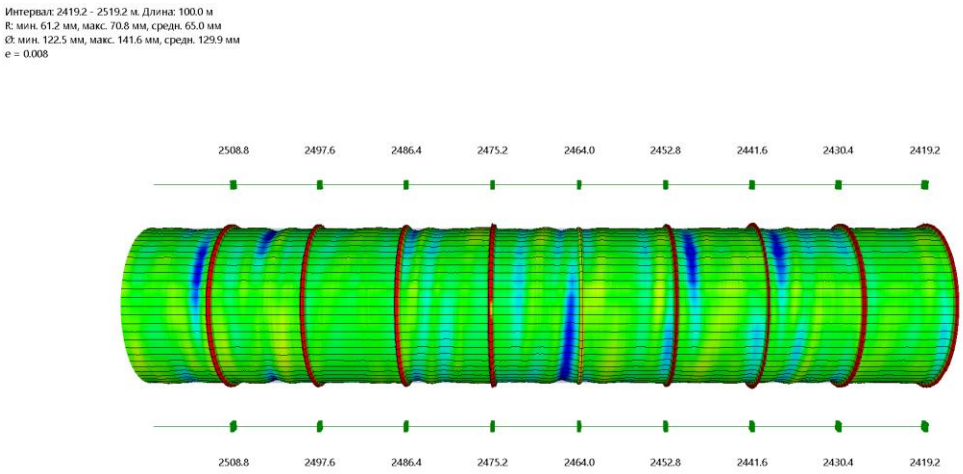


Рис. 3. Цилиднрическая форма представления с поверхностной сеткой и осями

Рассмотренные аспекты позволяют воспринимать сцену как диаграмму, которую можно вставить в любой отчет или заключение по проведенному исследованию.

СПИСОК ЛИТЕРАТУРЫ

1. Тараторин Н. Программное обеспечение визуализации результатов профилеметрии; Мавлютовские чтения: материалы XIV Всероссийской молодежной научной конференции Т. 5, Ч. 1 / Н. С. Тараторин. – Уфа: Уфимский государственный авиационный технический университет – Уфа, 2020. – стр. 182-189 (дата обращения: 10.08.2021).
2. PS Platform Multifinger Imaging Tool; URL:https://www.slb.com/-/media/files/production/product-sheet/ps-platform-multifinger-imaging-tool-ps (дата обращения: 06.09.2020).

УДК 519.688

А. Ф. ФАТТАХОВА
ilalovaais@gmail.com
Науч. руководитель – канд. техн. наук, доц. Г. А. МАКЕЕВ

Уфимский государственный авиационный технический университет

МАТЕМАТИЧЕСКОЕ И ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ЗАДАЧИ АНАЛИЗА ГИДРОДИНАМИЧЕСКИХ ТРЕНИЙ ЖИДКОСТИ В НАСОСНО-КОМПРЕССОРНЫХ ТРУБАХ

Аннотация. Статья посвящена моделированию зависимости гидравлических трений от расхода жидкости по данным закачек. Приводятся математические модели и алгоритмы решения задач расчета гидравлических трений и восстановления зависимости гидравлических трений от расхода жидкости и диаметра трубы, а также результаты вычислительных экспериментов, подтверждающих корректность результатов моделирования, полученного с помощью разработанного модуля в программном продукте ООО «РН-БашНИПИнефть» «РН-ГРИД».
Ключевые слова: гидравлические трения; математическая модель; закачка жидкости; программное обеспечение; гидроразрыв пласта.

Почти все месторождения нефти, находящиеся на настоящий момент в разработке, являются низкопроницаемыми, т. е. способность породы пласта на месторождении пропускать жидкости или газы при условии перепада давления крайне мала. Для повешения эффективности разработки месторождений с трудноизвлекаемыми запасами нефти разрабатываются новые подходы, например, такие, как технология гидравлического разрыва пласта. В наших географических условиях, когда больше 70% нефти находится в трудноизвлекаемых пластах, ГРП – это единственный способ, с которым можно разрабатывать экономически рентабельные скважины.

Для успешного завершения ГРП и максимизации выкаченного объема нефти со скважины необходимо учесть много факторов при построении плана процесса ГРП. Без предварительного планирования возможно возникновение проблем, в результате которых проведение ГРП окажется бесполезным.

Задача моделирования процесса ГРП включает в себя множество разных подзадач, решаемые с помощью анализов данных, являются важной частью подготовки к процессу ГРП на месторождении. С помощью таких анализов

можно оценить неизвестные показатели пласта, жидкостей, труб и других составляющих процесса добычи нефти.

Одним из таких подзадач является определение потерь давления на гидродинамические трения. При моделировании потерь давления на гидравлические трения при движении жидкости в трубах нужно уметь предсказывать будущие трения при разных диаметрах и расходах. Лабораторные эксперименты для нужных диаметров труб и скоростей закачки очень дороги и не всегда возможны, поэтому необходимо разработать инструмент, позволяющий определить зависимость трений от расхода жидкости на основе данных, полученных во время обычных работ на скважине.

Задача расчета гидравлический трений при движении жидкости по насосно-компрессорной трубе заключается в нахождении зависимости потерь давления на трение от времени на основе данных об операции ГРП, параметрах жидкости и конструкции скважины, в которой проводилась закачка.

Исходные данные задачи расчета гидравлических трений состоят из:

– $p_{\text{уст}}(t)$ – изменение устьевого давления во времени;

– $p_{\text{заб}}(t)$ – изменение забойного давления во времени;

– $Q(t)$ – изменение расхода закачиваемой в НКТ жидкости во времени;

– D – диаметр НКТ;

– L – длина НКТ;

– H – высота НКТ;

– ρ – плотность закачиваемой жидкости.

Предполагается, что рассматриваемая НКТ заполнена одной жидкостью, имеет один диаметр и однородна по длине.

Требуется найти изменение потерь давления на трение во времени $\Delta p_{\text{трен}}(\text{t})$ в виде функции $\Delta p_{\text{трен}}(\text{D, L, Q})$, зависящей от расхода жидкости, диаметра и длины НКТ.

Решение задачи расчета гидродинамических трений довольно простое. Удельные потери давления на трения в НКТ можно представить в виде следующей формулы:

$$L \times \Delta p_{\text{трен}}(\text{t}) = p_{\text{уст}}(t) + \rho g H - p_{\text{заб}}(t), \quad (1)$$

где $\rho g H$ – это давление столба жидкости высоты H плотностью ρ (гидродинамическое давление), а g – ускорение свободного падения на поверхности Земли.

По сути своей значения потерь давления на трения в какие-то моменты времени не дают никакой практической ценности. Для того, чтобы предсказывать гидравлические трения при конкретных значениях диаметра трубы и расхода жидкости, необходимо восстановить зависимость потерь давления на трение от расхода жидкости и диаметра трубы скважины.

Задача восстановления зависимости гидравлических трений от расхода жидкости использует найденную в предыдущем пункте зависимость удельных потерь давления на трение от времени.

В качестве исходных данных к задаче восстановления зависимости гидравлических трений от расхода жидкости и диаметра трубы даны:

– $Q(t) -$ изменение расхода закачиваемой в НКТ жидкости во времени;

– $D -$ диаметр НКТ;

– $\Delta p_{\text{трен}}(\text{t})$ – изменение удельных потерь давления на трение во времени.

Требуется найти функцию $\Delta p_{\text{трен}}(D, Q)$, наиболее полно отображающую зависимость гидравлических трений от расхода жидкости и диаметра трубы скважины.

Гидравлические потери на трение обусловлены проявлением сил вязкости в жидкости. На потери давления на трение влияет режим течения жидкости в трубах.

Различают 3 режима течения жидкости [8]:

– ламинарный режим, при котором течение является упорядоченным слоистым без перемешивания жидкости в потоке, жидкость течет по маленькой трубе и (или) с маленькой скоростью, также между слоями, которые движутся еще и относительно друг друга, возникают силы внутреннего трения (из-за вязкости жидкости);

– турбулентный режим, при котором происходит движение частиц жидкости в продольном, вертикальном и поперечном направлениях, что приводит к тому, что струйки жидкости перемешиваются, поэтому поток характеризуется беспорядочно движущимися массами жидкости, также из-за шероховатой поверхности трубы возникают вихри, так как частицы переходят во вращательное движение (при высоких скоростях движения потока);

– переходный режим, представляющий собой поток, переходящий от ламинарного к турбулентному режиму течения.

В общем случае задача восстановления зависимости гидравлических трений от расхода жидкости и диаметра трубы сложная, так как связана с задачей определения режима течения жидкости, который влияет на вид зависимости трений от расхода. Например, так как при турбулентном режиме течения расходуется энергия на преодоление вязкости при турбулентных колебаниях, потери при таком режиме будут значительно больше, чем при ламинарном [8].

В данной работе зависимость гидравлических трений от расхода жидкости будет восстановлена в виде:

– линейной зависимости для каждого диаметра трубы:

$$\Delta p_{\text{трен}}(Q) = a \times Q + b \quad (2)$$

– степенной зависимости для каждого диаметра трубы:

$$\Delta p_{\text{трен}}(Q) = a \times Q^b \quad (3)$$

Для определения параметров каждой из модели выбран метод наименьших квадратов, суть которого заключается в минимизации функции от двух переменных a и b $F(a, b)$ [3], являющейся суммой квадратов отклонений факти-

ческих значений $\Delta p_{\text{трен}}(\text{t})$ от восстановленных из найденной зависимости $\Delta p_{\text{трен}}(Q)$.

Формула функции $F(a, b)$ для линейной зависимости будет иметь следующий вид:

$$F(a,\ b) = \ \sum_{i=0}^{n}(\Delta p_{\text{трен}}(Q) - (a \times Q + b))^2 \to min \tag{4}$$

Для того, чтобы для степенной зависимости (3.3) можно было построить функцию $F(a, b)$ и найти ее параметры с помощью метода наименьших квадратов, необходимо привести ее к линейной форме [3]. Для этого прологарифмируем формулу (3.3):

$$ln\,\Delta p_{\text{трен}}(Q) = ln\,a + b \times ln\,Q \tag{5}$$

Таким образом, функцию $F(a, b)$ для степенной зависимости будет выглядеть следующим образом:

$$F(a,\ b) = \sum_{i=0}^{n}(\ln \Delta p_{\text{трен}}(Q) - (\ln a + b \times \ln Q))^2 \to min \tag{6}$$

Для нахождения коэффициентов a и b каждой модели необходимо составить решить систему из двух уравнений с двумя неизвестными для каждой из моделей соответственно [3].

Для того, чтобы составить системы уравнений, необходимо найти частные производные функций $F(a, b)$ по переменным a и b для каждой модели и прировнять их к 0 [3].

Система уравнений для линейной модели зависимости находится следующим образом:

$$\begin{cases} \dfrac{\partial F(a,b)}{\partial a} = 0 \\ \dfrac{\partial F(a,b)}{\partial b} = 0 \end{cases} \Leftrightarrow \begin{cases} -2 \times \sum \Big(\Delta p_{\text{трен}}(Q) - (a \times Q + b)\Big) \times Q = 0 \\ -2 \times \sum \Big(\Delta p_{\text{трен}}(Q) - (a \times Q + b)\Big) = 0 \end{cases}$$

$$\Leftrightarrow \begin{cases} a \times \sum Q^2 + b \times \sum Q = \sum Q \times \Delta p_{\text{трен}}(Q) \\ a \times \sum Q + b \times n = \sum \Delta p_{\text{трен}}(Q) \end{cases}, \tag{7}$$

где n – это количество выбранных пользователем характерных точек.

Аналогично находится система уравнений для степенной модели зависимости:

$$\begin{cases} \frac{\partial F(a,b)}{\partial a} = 0 \\ \frac{\partial F(a,b)}{\partial b} = 0 \end{cases} \Leftrightarrow \begin{cases} -2 \times \sum \left(ln\, \Delta p_{\text{трен}}(Q) - (ln\, a + b \times ln\, Q) \right) \times ln\, Q = 0 \\ -2 \times \sum \left(ln\, \Delta p_{\text{трен}}(Q) - (ln\, a + b \times ln\, Q) \right) = 0 \end{cases}$$

$$\Leftrightarrow \begin{cases} b \times \sum ln\, Q^2 + ln\, a \times \sum ln\, Q = \sum ln\, Q \times ln\, \Delta p_{\text{трен}}(Q) \\ b \times \sum ln\, Q + ln\, a \times n = \sum ln\, \Delta p_{\text{трен}}(Q) \end{cases}, \quad (8)$$

где n – это количество выбранных пользователем характерных точек.

Полученные системы (7) и (8) решаются методом Крамера и получаются следующие формулы для нахождения коэффициентов:

– линейной модели:

$$\begin{cases} a = \frac{n \times \sum Q \times \Delta p_{\text{трен}}(Q) - \sum Q \times \sum \Delta p_{\text{трен}}(Q)}{n \times \sum Q^2 - (\sum Q)^2} \\ b = \frac{\sum \Delta p_{\text{трен}}(Q) - a \times \sum Q}{n} \end{cases} \quad (9)$$

– степенной модели:

$$\begin{cases} b = \frac{n \times \sum \ln Q \times \ln \Delta p_{\text{трен}}(Q) - \sum \ln Q \times \sum \ln \Delta p_{\text{трен}}(Q)}{n \times \sum (\ln Q)^2 - (\sum \ln Q)^2} \\ a = e^{\frac{\sum \ln \Delta p_{\text{трен}}(Q) - b \times \sum \ln Q}{n}} \end{cases} \quad (10)$$

Для оценки качества работы разработанного программного обеспечения проведено два эксперимента: первый – на смоделированных данных для проверки корректности моделирования зависимости гидродинамических трений от расхода жидкости, второй – проверка работы ПО на реальных данных, полученных при работах на скважине.

Схема вычислительного эксперимента, проведенного для проверки корректности работы ПО, приведена на рисунке 1.

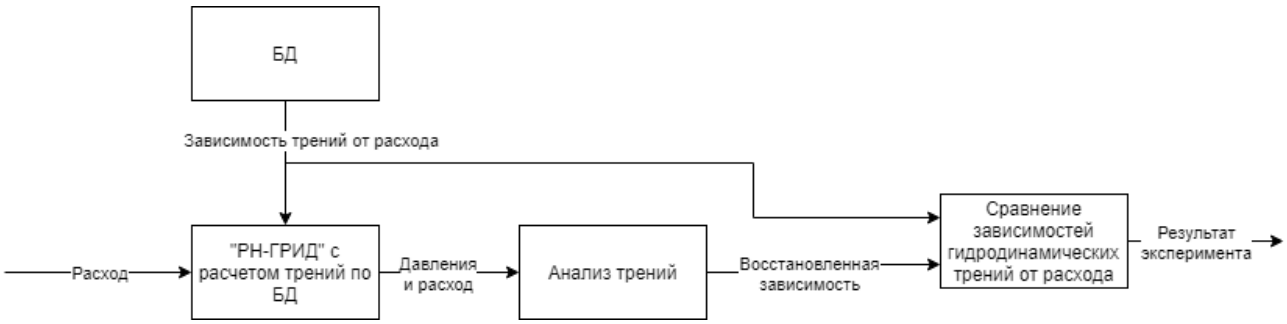


Рис. 1. Схема проведения вычислительного эксперимента для проверки корректности работы ПО

Суть данного эксперимента заключается в следующем: в базе данных жидкостей уже есть записи о зависимости гидродинамических трений от расхожа жидкости для некоторых диаметров труб. На основе этих данных был создан дизайн ГРП, в котором в пласт была закачана жидкость «W-FH» из базы данных. Во время моделирования процесса ГРП «РН-ГРИД» берет информацию о зависимости трений от расхода закачиваемой в пласт жидкости из базы данных и рассчитывает изменение давлений с учетом потерь на гидродинамические трения. На основе построенной модели ГРП были получены временные ряды изменения устьевого и забойного давлений и расхода жидкости. Для проверки корректности разработанного анализа трений необходимо восстановить зависимость трений от расхода исходя из полученных временных рядов и сравнить полученные результаты с зависимостью из базы данных. При правильности разработанного ПО восстановленная с помощью анализа трений зависимость и зависимость из базы данных жидкостей должны совпадать.

Полученные с помощью построения дизайна ГРП данные о закачке приведены на рисунке 2.

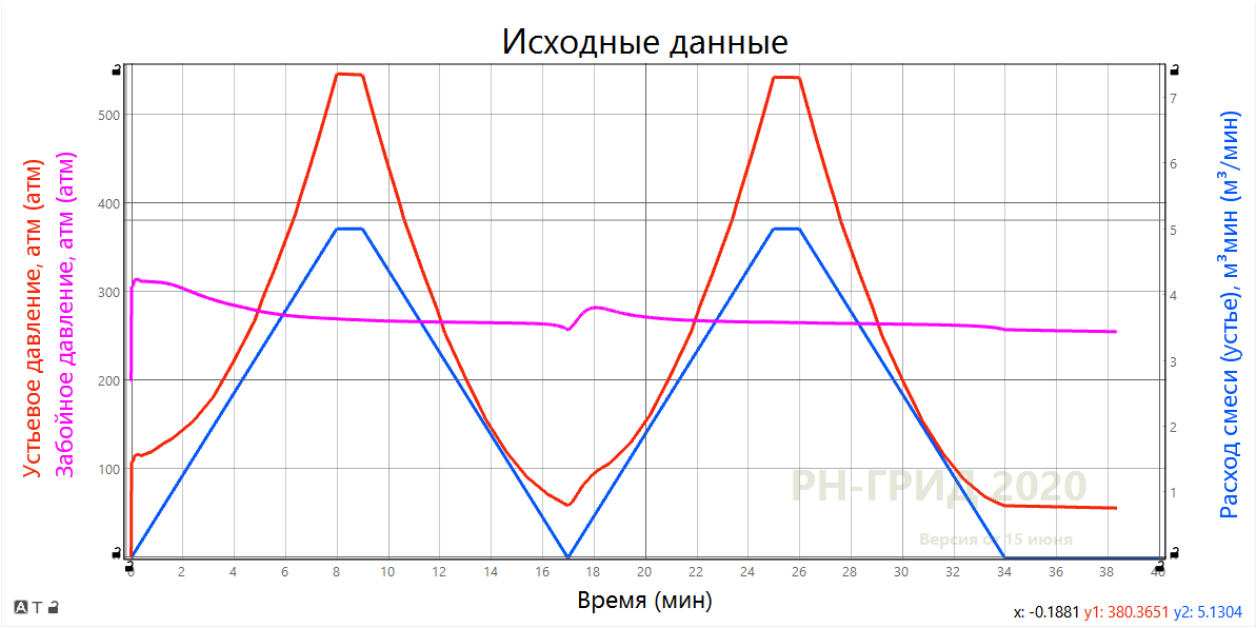


Рис. 2. Исходные данные для первого эксперимента

Далее на основе этих данных проведем анализ трений в разработанном ПО. На рисунке 3 представлены результаты моделирования в виде графиков построенных линейной и степенной моделей.

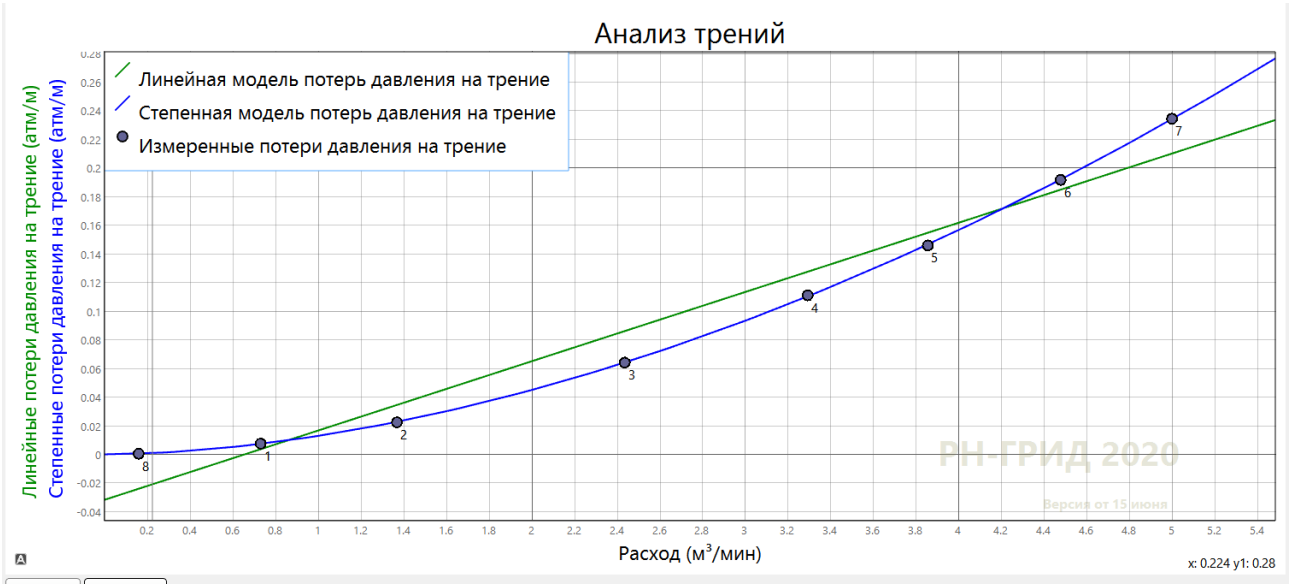


Рис. 3. Результат восстановления зависимости трений от расхода

На рисунке 4 представлены численные результаты анализа. Измеренные точки потерь давления на трение от расхода плохо ($R^2 = 0.959$) ложатся на линейную модель (ньютоновская жидкость) и отлично ($R^2 = 1$) на степенную модель (степенная жидкость).

Основные результаты интерпретации

	Параметр	Значение
1	Множитель линейной модели	0.048
2	Слагаемое линейной модели	-0.032
3	Коэффициент детерминации линейной модели	0.959
4	Показатель степенной модели	1.801
5	Множитель степенной модели	0.013
6	Коэффициент детерминации степенной модели	1

	Расход [м³/мин]	Измеренные потери давления на трение [атм/м]
1	0.16	4.701E-04
2	0.73	0.007
3	1.37	0.022
4	2.44	0.064
5	3.29	0.111
6	3.86	0.146
7	4.48	0.192
8	5.00	0.234

Рис. 4. Найденные параметры моделей зависимости трений от расхода

Далее необходимо сравнить полученные результаты с информацией, которая уже хранится в БД.

На рисунке 5 представлены данные трения жидкости «W-FH», хранящиеся в БД.

	Расход [м³/мин]	Потери давления [атм/м]
1	0.100	1.987E-04
2	0.200	6.955E-04
3	0.300	0.001
4	0.400	0.002
5	0.500	0.003
6	0.600	0.005
7	0.700	0.007
8	0.800	0.009
9	0.900	0.011
10	1.000	0.012

Рис. 5. Данные по трению жидкости «W-FH» в БД

Для того, чтобы наглядно сравнить полученные результаты и данные из БД, построим кривую для степенной модели по найденным параметрам, а также построим точки, полученные из базы данных.

Результат проведенного эксперимента представлен на рисунке 6.

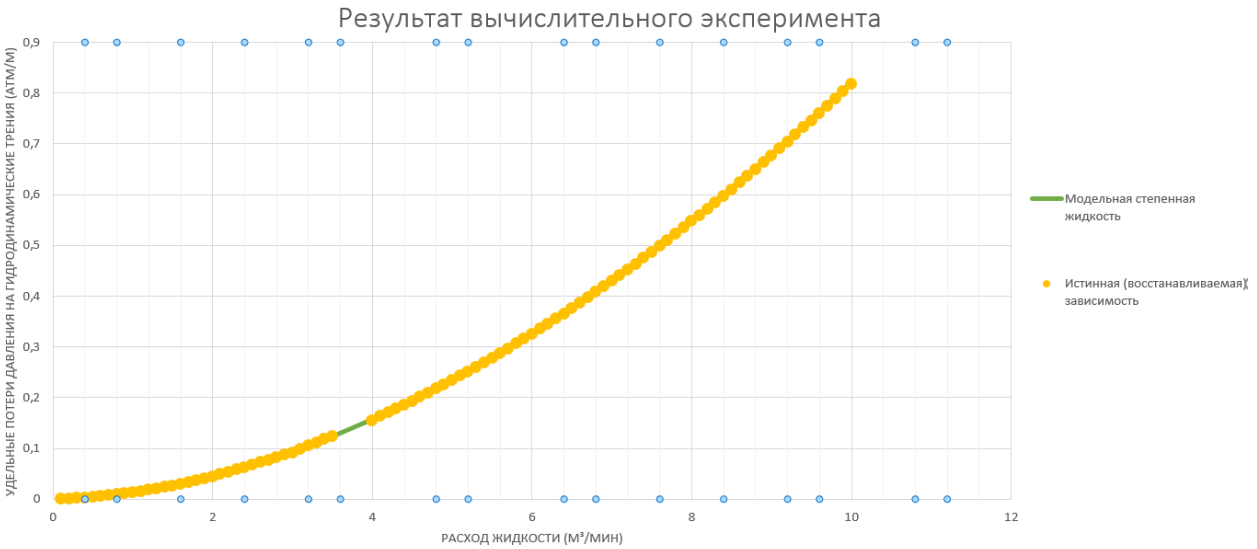


Рис. 6. Результат вычислительного эксперимента

На рисунке 6 видно, что найденная степенная модель полностью соответствует зависимости трений для жидкости из БД, по которой были рассчитаны синтетические данные, что говорит о том, что разработанное ПО для моделирования потерь давления на гидродинамические трения правильно восстанавливает зависимость гидравлических трений от расхода жидкости.

Следующим вычислительным экспериментом является проверка работы программного модуля «Анализ трений» в «РН-ГРИД» на данных, полученных на реальных закачках.

На рисунке 7 приведены данные, измеренные во время проведения операции ГРП.

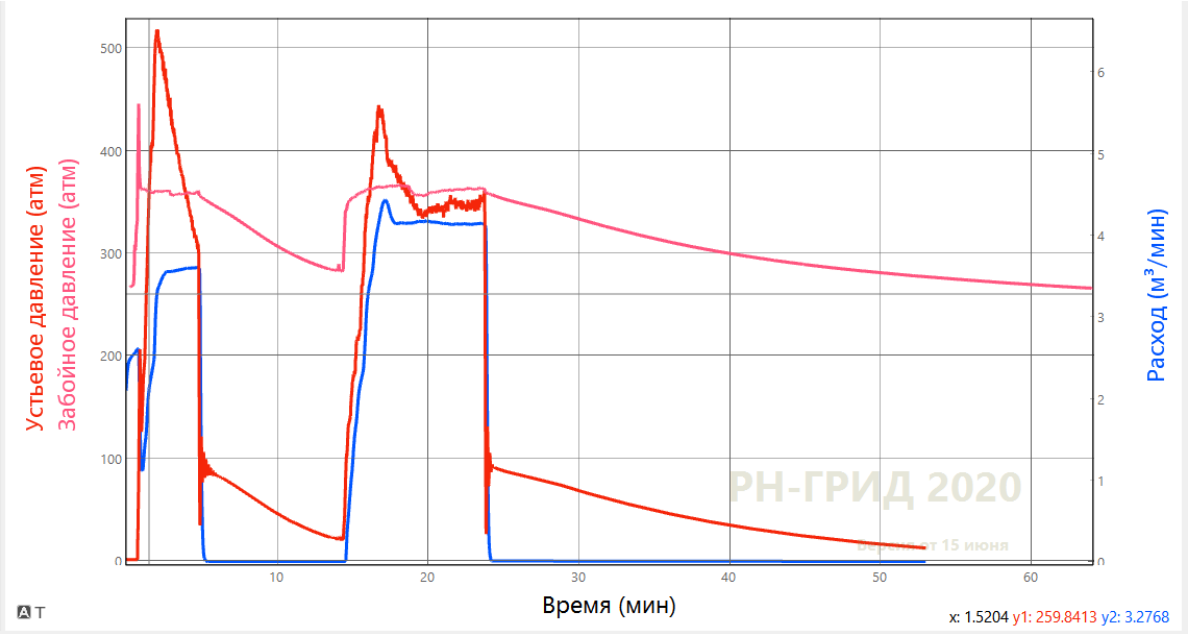


Рис. 7. Исходные данные закачек для второго вычислительного эксперимента

На рисунке 8 приведен результат моделирования в графическом виде. На рисунке видно, что линейная и степенная модели почти совпадают.

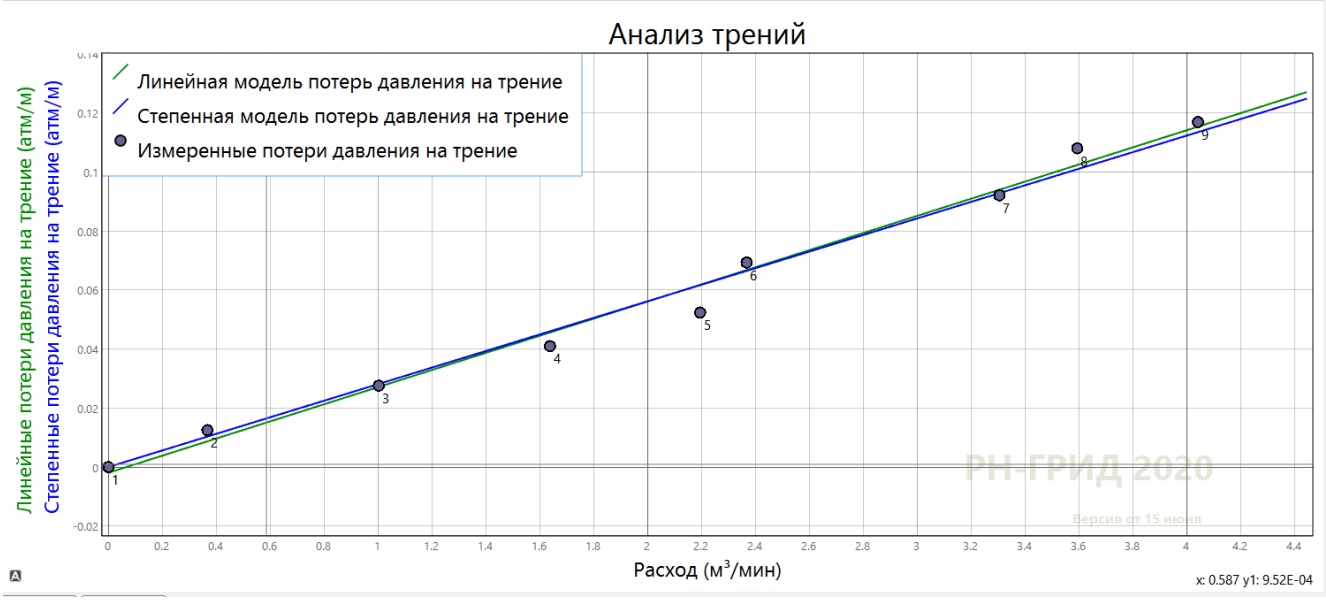


Рис. 8. Результат моделирования в графическом виде

Найденные параметры моделей и коэффициенты детерминации для каждой из них приведены на рисунке 9.

	Параметр	Значение
1	Множитель линейной модели	0.029
2	Слагаемое линейной модели	-0.002
3	Коэффициент детерминации линейной модели	0.988
4	Показатель степенной модели	1.002
5	Множитель степенной модели	0.028
6	Коэффициент детерминации степенной модели	0.998

Рис. 9. Параметры и коэффициенты детерминации найденных модельных зависимостей

По расположению точек измеренных потерь давления на трение ближе к действительности линейная зависимость, также это подтверждается показателем степенной модели, которая близка к 1, что приводит степенную зависимость в линейный вид.

Коэффициенты детерминации каждой из моделей меньше 1. Это обусловлено тем, что на измеренных при на реальных закачках данных обязательно

присутствуют шумы, которые могут быть получены по разным причинам. Например, одним из них является точность измерения манометров или других датчиков.

СПИСОК ЛИТЕРАТУРЫ

1. Гидравлический разрыв пласта [Электронный ресурс] – Электрон. текстовые дан. – Газпромнефть НТЦ – Режим доступа: https://ntc.gazprom-neft.ru/business/production/fracking/, свободный
2. Гидравлический разрыв пласта (ГРП) [Электронный ресурс] – Электрон. текстовые дан. – 2013. – Режим доступа: https://neftegaz.ru/tech-library/tekhnologii/141812-gidravlicheskiy-razryv-plasta-grp/, свободный
3. Линник Ю.В. Метод наименьших квадратов и основы теории обработки наблюдений - Гос. изд-во физ.-мат. лит., 1962 – 352с.
4. Нагнетательная скважина [Электронный ресурс] – Электрон. текстовые дан. – 2012. – Режим доступа: https://neftegaz.ru/tech-library/burovye-ustanovki-i-ikh-uzly/141461-nagnetatelnaya-vodonagnetatelnaya-skvazhina/, свободный
5. Нефтянка для инженеров, программистов, математиков и широких масс трудящихся, часть 5 [Электронный ресурс] РН-БашНИПИнефть – Электрон. текстовые дан. – 2020. Режим доступа: https://habr.com/ru/bashnipineft/, свободный
6. РН-ГРИД – симулятор гидроразрыва пласта (ГРП) нового поколения [Электронный ресурс] RN-Digital – Электрон. текстовые дан. – 2021. – Режим доступа: https://rn.digital/rngrid/, свободный
7. Симулятор гидроразрыва пласта [Электронный ресурс] Википедия. Свободная энциклопедия – Электрон. текстовые дан. –Режим доступа: https://ru.wikipedia.org/wiki/, свободный
8. Фокеева Л.Х. Гидравлика и нефтегазовая гидродинамика: учебное пособие – КФУ, 2017 – 85 с.
9. John R. Hauser. Numerical Methods for Nonlinear Engineering Models. — Springer, 2009 – 1013 с..
10. P. G. Guest. Numerical Methods of Curve Fitting. — Cambridge Academ, 2012 – 438 с.
11. Sandra Lach Arlinghaus. Practical Handbook of Curve Fitting. — CRC Press, 1994 – 249 с.

УДК 004.023

М. Ю. ФЕДОРОВ
maxim.fedorov28@yandex.ru
Науч. руководов. – математик, д-р техн. наук, проф. А. Ф. ВАЛЕЕВА

Уфимский государственный авиационный технический университет

РЕШЕНИЕ ЗАДАЧИ МАРШРУТИЗАЦИИ С РАЗДЕЛЬНОЙ ДОСТАВКОЙ

Аннотация. Рассматривается решение задачи маршрутизации транспортных средств с учетом раздельной доставки грузов для минимизации транспортных расходов с использованием метода имитации отжига.
***Ключевые слова*:** маршрутизация транспортных средств; задача раздельной доставки; метод имитации отжига.

Введение

В условиях современной стремительной жизни происходит значительное расширение производства, следовательно, и объема грузоперевозок. Транспортная логистика становится все более важной составляющей многих сфер человеческой деятельности. Оптимизация транспортной логистики дает серьезное конкурентное преимущество перед другими компаниями, позволяет удержать стабильные позиции на рынке без потери качества оказываемых услуг и снизить стоимость товара. Одним из значимых методов оптимизации транспортной логистики является внедрение систем по поиску рациональных маршрутов транспортных средств, которые позволяют снизить издержки, связанные с транспортировкой грузов.

Метод решения и оценка эффективности

Задача маршрутизации одна из наиболее сложных в области комбинаторной оптимизации. Эта задача является NP-трудной и требует разработки сложных алгоритмов для нахождения качественных решений.

В статье рассматривается VRP с раздельной доставкой (Split Delivery Vehicle Routing Problem, SDVRP): в задаче снимается общий для всех VRP запрет на многократное посещение клиента. ТС, находящиеся в депо, имеют ограни-

чение по максимальной грузоподъемности, которое требования клиента могут превышать.

Для решения задачи SDVRP был использован метаэвристический алгоритм, основанный на методе имитации отжига, реализованный в двух вариантах с разными путями изменения решения. За основу алгоритма был взят процесс кристаллизации вещества. При повышении температуры атомы покидают свои позиции и с понижением температуры пытаются перейти в состояние с наименьшей энергией, однако, с определенной вероятностью они могут перейти и в состояние с большей. Эта вероятность уменьшается вместе с температурой. Переход в состояние с большей энергией позволяет системе выбраться из локального минимума и получить близкое к оптимальному решение.

Тестирование разработанных, для решения задачи маршрутизации ТС с учетом раздельной доставки, вариантов алгоритма имитации отжига проводилось в трех экспериментах с разным количеством клиентов. В каждом эксперименте было произведено 10 прогонов алгоритма так как, эвристические алгоритмы не гарантируют нахождение лучшего решения.

Эксперимент 1. Эксперимент 1 проводился на тестовом примере S51D3. Набор содержит информацию о координатах депо и 50 клиентов, о спросе клиентов, о количестве ТС равном 15 и их грузоподъемности равной 160. В качестве минимальной температуры было выбрано значение 0.01, в качестве максимальной: 20000 и 30000. Для данного примера известно вычисленное решение, равное 972.

Результаты тестирования представлены в Таблица 1.

Таблица 1

Сравнение результатов работы алгоритмов для задачи маршрутизации ТС в эксперименте 1

Алгоритм	Вариант 1		Вариант 2	
Макс. T / Прогон	20000	30000	20000	30000
1	997.75	972.78	1002.14	1006.41
2	1001.56	**964.15**	1023.02	1035.22
2	1000.22	999.71	1011.73	1022.23

Окончание табл. 1

3	984.8	994.13	1077.12	988.09
4	988.29	977.63	1016.49	995.38
5	**961.18**	983.97	**973.84**	978.9
6	983.63	979.4	986.84	981.4
7	979.23	989	997.94	1016.91
8	1007.29	991.83	997.99	991.83
9	979.83	987.98	995.38	**967**
10	1005.69	985.32	1008.6	1017.39
Время выполнения	12 сек	19 сек	12 сек	19 сек

Эксперимент 2. Эксперимент 2 проводился на тестовом примере S76D2. Набор содержит информацию о координатах депо и 75 клиентов, о спросе клиентов, о количестве ТС равном 15 и их грузоподъемности равной 160. В качестве минимальной температуры было выбрано значение 0.01, в качестве максимальной: 30000 и 40000. Для данного примера известно вычисленное решение, равное 1147.

Результаты тестирования представлены в Таблица 2.

Таблица 2

Сравнение результатов работы алгоритмов для задачи маршрутизации ТС в эксперименте 2

Алгоритм	Вариант 1		Вариант 2	
Макс. Т / Прогон	30000	40000	30000	40000
1	1260.74	1232.14	1256.02	1283.03
2	1222.17	1238.65	1430.59	1309.57
2	1246.98	1224.12	1286.33	1362
3	1222.6	**1197.5**	1258.3	1262.69
4	1231.29	1206.83	1306.06	1293.77
5	**1215.56**	1220.74	1343.98	1267.22
6	1265.34	1211.59	1364.13	1291.43
7	1221.9	1269.96	1217.1	1291.83
8	1249.39	1203.27	1251.62	1270.36
9	1247.41	1225.03	1273.77	**1245.73**
10	1334.05	1240.94	**1214.47**	1313.11
Время выполнения	25 сек	35 сек	25 сек	34 сек

Эксперимент 3. Эксперимент 3 проводился на тестовом примере S101D2. Набор содержит информацию о координатах депо и 100 клиентов, о спросе клиентов, о количестве ТС равном 20 и их грузоподъемности равной 160. В ка-

честве минимальной температуры было выбрано значение 0.01, в качестве максимальной: 40000 и 50000. Для данного примера известно вычисленное решение, равное 1393.

Результаты тестирования представлены в Таблица 3.

Таблица *3*

Сравнение результатов работы алгоритмов для задачи маршрутизации ТС в эксперименте 3

Алгоритм	Вариант 1		Вариант 2	
Макс. Т / Прогон	40000	50000	40000	50000
1	1465.63	1456.15	1627.89	1519.61
2	1482.63	1504.93	1510.31	1614.97
2	1488.63	1509.49	1534.58	1494.65
3	1498.35	1465.59	1578.33	1558.95
4	1493.46	1532.67	1539.14	1546.64
5	1465.18	1517.49	1577.03	1523.31
6	1536.45	1476.35	**1507.79**	1567.94
7	1466.87	1471.15	1621.84	1565.12
8	**1455.47**	**1450.77**	1527.36	1545.85
9	1481.75	1508.42	1614.93	1628.36
10	1485.07	1455.25	1539	**1480.37**
Время выполнения	62 сек	80 сек	61 сек	76 сек

Вывод по экспериментам:

– В первом эксперименте лучшее значение показал первый вариант алгоритма с максимальной температурой равной 20000. Полученное решение оказалось лучше, чем известное для данного набора данных.

– Во втором эксперименте лучшее значение получил первый вариант алгоритма при максимальной температуре равной 40000;

– В третьем эксперименте лучшее значение получил первый вариант алгоритма при максимальной температуре равной 50000;

– Во втором и в третьем эксперименте полученные решения оказались хуже известных для данных наборов данных;

– На малых наборах данных оба варианта алгоритма показывают примерно одинаковый результат;

– На больших наборах данных первый вариант алгоритма показал себя лучше, чем второй.

Заключение

1. Разработан алгоритм для решения задачи раздельной доставки груза различным клиентам в двух вариантах на основе имитации отжига.

2. Проведен вычислительный эксперимент на трех наборах данных. Эксперимент показал, что на малом наборе данных оба варианта алгоритма показывают примерно одинаковые решения. Первый вариант алгоритма на больших наборах данных показал себя лучше, чем второй.

СПИСОК ЛИТЕРАТУРЫ

1. G. B. Dantzig, J. H. Ramser. The Truck Dispatching Problem // Management Science. – 1959. – vol. 6, no. 1 – pp. 80-91.
2. S. Kirkpatrick; C. D. Gelatt; M. P. Vecchi. Optimization by Simulated Annealing // Science, New Series. – 1983. – vol. 220, no. 4598. – P. 671-680.
3. The Split Delivery Vehicle Routing Problem: [Электронный ресурс]. URL: https://www.uv.es/belengue/sdvrp.html.

УДК 004.023

А. И. ХАМИТОВ
aidarin607@gmail.com
Науч. руководов. – д-р техн. наук, проф. А. Ф. ВАЛЕЕВА

Уфимский государственный авиационный технический университет

МАТЕМАТИЧЕСКОЕ И ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ДЛЯ РЕШЕНИЯ ЗАДАЧИ ТРЕХМЕРНОЙ УПАКОВКИ ГРУЗОВ, ПРЕДНАЗНАЧЕННЫХ РАЗЛИЧНЫМ КЛИЕНТАМ

***Аннотация*.** Рассматривается решение задачи трехмерной упаковки параллелепипедных грузов, предназначенных различным клиентам, в минимальное количество контейнеров транспортных средств.
***Ключевые слова*:** задача трехмерной упаковки; эволюционные стратегии.

Введение

В условиях современной рыночной конкуренции предприятиям необходимо снижать свои затраты для обеспечения максимального уровня поставки товаров потребителям и увеличения прибыли. Довольно-таки значительную часть расходов занимают затраты на транспортную логистику. Поэтому необходимо оптимизировать затраты на логистику для снижения себестоимости производимой продукции, обеспечения заказчикам лучшего обслуживания, увеличения прибыли и повышения конкурентоспособности предприятия. Одним из способов оптимизации бизнес-процессов логистики является рациональное размещение упакованных грузов в грузовом отсеке транспортных средств (ТС): максимальное использование полезного объема грузового отсека ТС (для снижения расходов на топливо для собственных ТС предприятия, для снижения расходов на аренду ТС), расположение грузов должно производиться в порядке, обратном порядку маршрутного листа ТС (для экономия времени на разгрузку).

Метод решения

Доказано, что задача одномерной упаковки в контейнер (Bin Packing Problem) относится к классу NP-трудных задач, следовательно, задачи большей

размерности, в частности задача трехмерной упаковки, так же являются NP-трудными [1].

Общий алгоритм решения задачи упаковки разделяется на две части: алгоритм, который работает непосредственно с кодировкой (перестановка номеров предметов), и алгоритм-декодер. Алгоритм, работающий с кодировкой, осуществляет составление некоего приоритетного списка, который состоит из номеров предметов. Алгоритм-декодер вычисляет целевую функцию и преобразует кодировку в промежуточное решение (в данном случае план размещения).

В данной работе предлагается использовать расширенный для трехмерной задачи декодер ABLP, применяемый в работе Hifi M. и M'Hallah R. для кругового раскроя [2]. Так как в данной работе рассматривается исключительно упаковка в контейнер параллелепипедных грузов, применением данного алгоритма для упаковки цилиндров пренебрегаем. В качестве решения представляется список координат параллелепипедных грузов, где за координаты i-го параллелепипедного груза будем подразумевать координаты левого нижнего дальнего угла.

Для нахождения рационального приоритетного списка размещения предметов в контейнеры в данной работе представлен эволюционный алгоритм $(\mu+\lambda)$-EA.

Эволюционные алгоритмы моделируют процессы естественного отбора. Агенты – это представители конкретных видов живых организмов, их поведение определяется окружающей средой. Множество агентов принято называть популяцией. Популяция эволюционирует согласно правилам отбора в соответствии с целевой функцией, задаваемой окружающей средой. Каждому агенту популяции назначается значение его пригодности в окружающей среде. Размножаются и выживают только наиболее пригодные и сильные виды. Мутация позволяет агентам приспосабливаться к условиям среды.

Так как задача упаковки является NP – сложной, она дает мотивацию для поиска и создания новых эвристик для ее решения. Так, например, в 1996 году S. Khuri исследовал использование двух эволюционных эвристик для решения задачи упаковки контейнеров [3].

Оценка эффективности

Проводилось тестирование разработанных эволюционных алгоритмов (1+1)-EA с мутацией №1 (перестановка одной пары элементов) и (1+1)-EA с мутацией №2 (перестановка двух пар элементов), а также двух вариантов алгоритма-декодера: послойная упаковка и упаковка в колонну.

Для численного эксперимента были сгенерированы три набора тестовых данных (малый – 10 клиентов по 25 предметов у каждого клиента, средний – 10 клиентов по 200 предметов у каждого клиента и большой – 10 клиентов по 400 предметов у каждого клиента).

Тестирование проходило при следующих условиях:

- Параметры ТС: длина L=900, ширина W=250, высота H= 250
- Ограничения длины грузов: нижнее l1 = 80; верхнее l2 =120;
- Ограничения ширины грузов: нижнее w1 = 70; верхнее w2 = 100;
- Ограничения высоты грузов: нижнее h1 = 60; верхнее h2 = 100;
- Для каждого набора данных было проведено по 7 прогонов;
- Каждый алгоритм тестировался на 100 и 400 итерациях.

Результат: количество ТС необходимых для упаковки.

Эксперимент №1 (на малом наборе данных):

Эксперимент проводился на малом наборе данных: имеется 10 клиентов по 25 предметов у каждого клиента.

Таблица 1

Сравнение результатов работы алгоритмов на малом наборе данных для задачи трехмерной упаковки грузов, предназначенных различным клиентам

Способ упаковки	*Послойная упаковка*				*Упаковка в колонну*			
Алгоритм	*(1+1)-EA Мутация №1*		*(1+1)-EA Мутация №2*		*(1+1)-EA Мутация №1*		*(1+1)-EA Мутация №2*	
Итерации / Прогоны	*100*	*400*	*100*	*400*	*100*	*400*	*100*	*400*
1	9	9	8	8	7	7	7	7
2	8	8	8	9	7	7	7	7
3	9	9	9	8	7	7	7	7
4	9	8	9	9	7	7	7	7
5	8	8	8	8	7	7	7	7
6	8	8	8	8	7	7	7	7
7	8	8	8	8	7	7	7	7
Среднее время работы, с	1,82	1,91	1,75	1,87	2,29	2,46	2,27	2,35

Из Таблица 1 можно сделать вывод о том, что на малом наборе данных себя лучше показал алгоритм-декодер «Упаковка в колонну», эволюционный алгоритм (1+1)-EA с мутацией №1 и эволюционный алгоритм (1+1)-EA с мутацией №2 показали одинаковые результаты.

Эксперимент №2 (на среднем наборе данных):

Эксперимент проводился на среднем наборе данных: имеется 10 клиентов по 200 предметов у каждого клиента.

Таблица 2

Сравнение результатов работы алгоритмов на среднем наборе данных для задачи трехмерной упаковки грузов, предназначенных различным клиентам

Способ упаковки	*Послойная упаковка*				*Упаковка в колонну*			
Алгоритм	*(1+1)-EA Мутация №1*		*(1+1)-EA Мутация №2*		*(1+1)-EA Мутация №1*		*(1+1)-EA Мутация №2*	
Итерации / Прогоны	*100*	*400*	*100*	*400*	*100*	*400*	*100*	*400*
1	52	53	52	51	55	54	54	54
2	52	52	53	52	54	54	54	53
3	53	52	52	51	54	54	54	54
4	52	52	51	53	54	54	54	54
5	52	53	52	51	54	55	53	53
6	54	51	52	52	54	54	54	53
7	53	52	52	52	54	53	54	54
Среднее время работы, с	26,7	27,1	24,2	24,41	15,84	18,4	18,19	19,74

Из Таблица 2 можно сделать вывод о том, что на среднем наборе данных себя лучше показал алгоритм-декодер «Послойная упаковка», эволюционный алгоритм (1+1)-EA с мутацией №2 показал результаты лучше, чем эволюцион-ный алгоритм (1+1)-EA с мутацией №1.

Эксперимент №3 (на большом наборе данных):

Эксперимент проводился на среднем наборе данных: имеется 10 клиентов по 400 предметов у каждого клиента.

Таблица 3

Сравнение результатов работы алгоритмов на большом наборе данных для задачи трехмерной упаковки грузов, предназначенных различным клиентам

Способ упаковки	*Послойная упаковка*				*Упаковка в колонну*			
Алгоритм	*(1+1)-EA Мутация №1*		*(1+1)-EA Мутация №2*		*(1+1)-EA Мутация №1*		*(1+1)-EA Мутация №2*	
Итерации / Прогоны	*100*	*400*	*100*	*400*	*100*	*400*	*100*	*400*
1	103	102	103	103	107	108	108	108
2	103	103	103	103	107	108	108	108
3	104	103	104	103	108	107	108	107
4	102	102	103	103	109	109	108	108
5	103	104	103	103	108	108	108	108
6	104	103	103	103	108	108	108	108
7	103	102	103	103	108	108	108	107
Среднее время работы, с	80,7	87,2	82,8	74,2	44,1	43,1	42,5	46,7

Из Таблица 3 можно сделать вывод о том, что на большом наборе данных себя лучше показал алгоритм-декодер «Послойная упаковка», эволюционный алгоритм (1+1)-EA с мутацией №1 показал результаты лучше, чем эволюцион-ный алгоритм (1+1)-EA с мутацией №2.

Проведя численные эксперименты, можно сделать следующие выводы:

– на малых наборах данных декодер «Упаковка в колонну» показал лучшие результаты;

– на средних и больших данных лучше себя показал декодер «Послойная упаковка»;

– на среднем наборе данных лучше использовать эволюционный алгоритм (1+1)-EA с мутацией №2;

– на малых наборах данных эволюционный алгоритм (1+1)-EA с мутацией №1 и эволюционный алгоритм (1+1)-EA с мутацией №2 показали одинаковые результаты;

– больших данных алгоритм (1+1)-EA с мутацией №1 показал лучший результат.

Заключение

1. Разработаны два декодирующих алгоритма: послойная упаковка и упаковка в колонну.

2. Разработаны эволюционные алгоритмы (1+1)-EA с различными мутациями для решения задачи трехмерной упаковки грузов, предназначенных различным клиентам.

3. Проведен вычислительный эксперимент, направленный на определение эффективности разработанного алгоритма и проанализированы полученные результаты эксперимента. Из проведенного эксперимента можно сделать вывод, что на малых наборах данных декодер «Упаковка в колонну» показал лучшие результаты, а на средних и больших данных лучше себя показал декодер «Послойная упаковка». Также эксперимент показал, что на среднем наборе данных лучше использовать эволюционный алгоритм (1+1)-EA с мутацией №2, на малых наборах данных эволюционный алгоритм (1+1)-EA с мутацией №1 и эволюционный алгоритм (1+1)-EA с мутацией №2 показали одинаковые результаты, а на больших данных алгоритм (1+1)-EA с мутацией №1 показал лучший результат.

СПИСОК ЛИТЕРАТУРЫ

1. Гэри М. Джонсон Д. Вычислительные машины и трудно решаемые задачи. — М.: Мир, 1982. — 416 с.
2. Hifi M. M'Hallah R. Approximate algorithms for constrained circular cutting problems// Computers & Operations Research. — 2004. — Volume 31. —Issue 5. — C. 675-694.
3. Khuri, S., Schu¨tz, M., & Heitko¨tter, J. (1996). Evolutionary heuristics for the bin packing problem. In D. W. Pearson et al. (Eds.), Proceedings of the second international conference on artificial neural networks and genetic algorithms (pp. 285–288). Wien: Springer.

УДК 004.023

А. И. ШАРИПОВ
aynursharipovi@gmail.com
Науч. руководитель – математик, д-р техн. наук, проф. А. Ф. ВАЛЕЕВА

Уфимский государственный авиационный технический университет

РЕШЕНИЕ ЗАДАЧИ МАРШРУТИЗАЦИИ С ОБРАТНЫМИ ПЕРЕВОЗКАМИ

Аннотация. Рассматривается решение задачи маршрутизации транспортных средств с обратными перевозками для минимизации транспортных расходов с использованием эволюционного алгоритма.
Ключевые слова: маршрутизация транспортных средств; задача маршрутизации с обратными перевозками; эволюционный алгоритм.

Введение

Решение задач маршрутизации представляет собой нахождение рациональных маршрутов доставки грузов к клиентам из одного или нескольких депо ограниченным количеством транспортных средств (ТС). Применение вычислительных машин позволяет эффективно составить график перевозок, уменьшая количество экономических затрат, а также помогает сделать компании более конкурентоспособными на рынке. В рамках статьи с использованием метода заметания и эволюционного алгоритма была исследована задача маршрутизации с обратными перевозками (VRPB). В данной задаче в отличие от классической задачи маршрутизации ТС клиенты разделены на поставщиков и потребителей.

Метод решения и оценка эффективности

Для решения поставленной задачи были рассмотрены следующие методы:

1. Точные методы

2. Эвристические методы

Точные методы представляют собой перебор всех возможных вариантов и нахождение оптимального решения. Данные методы зависят от размерности задачи. Они хорошо подходят для задач, где небольшое количество входных

данных. Если же работать с большими данными, то время нахождения оптимального решения может стремиться к бесконечности.

Эвристические методы в большинстве случаев дают решения, которые близки к оптимальному. Они используются в основном для решения NP сложных задач, поскольку могут предоставить ответ за приемлемое время, поэтому они широко применяются в реальных задачах.

Эвристические алгоритмы действительно хороши, когда необходимо решить сложные задачи, поскольку они выдают хорошее решение за небольшой промежуток времени, поэтому для решения поставленной задачи был выбран эволюционный алгоритм с двумя видами мутаций. Так же для начального распределения клиентов по транспортным средствам был использован алгоритм заметания.

Проводилось тестирование разработанных эволюционных алгоритмов (1+1)-EA с мутацией №1 и (1+1)-EA с мутацией №2 на примере задачи маршрутизации транспортных средств с обратными перевозками.

В эксперименте решением целевой функции является общая длина всех маршрутов. Тестовый набор данных содержит в себе 25 клиентов, 15 из которых являются клиентами доставки, а 10 клиентами поставщиками. Количество итераций для алгоритмов (1+1)-EA с мутацией №1 и (1+1)-EA с мутацией №2 было взято 100 и 200.

Результаты выполнения алгоритмов представлены в таблице 1 1,…,5 – количество прогонов тестового набора. 100, 200- количество итераций.

Таблица 1

Сравнение результатов работы алгоритмов для задачи маршрутизации ТС обратными перевозками

Эксперимент 1	(1+1)-EA Мутация №1 (100)	(1+1)-EA Мутация №2 (100).	(1+1)-EA Мутация №1 (200)	(1+1)-EA Мутация №2 (200)
1	6933,5796	8667,6369	**6908,2999**	8470,5782
2	**6908,2999**	8667,6369	6934,5565	8667,6369
3	**6908,2999**	**8470,5782**	**6908,2999**	8470,5782
4	**6908,2999**	8667,6369	**6908,2999**	8026,3796
5	6933,5796	**8470,5782**	6934,5565	**7829,3209**

Время работы алгоритмов представлены в таблице 2.

Таблица 2

Сравнение времени работы алгоритмов для задачи маршрутизации ТС с обратными перевозками

Эксперимент 1	(1+1)-EA Мутация №1 (100)	(1+1)-EA Мутация №2 (100).	(1+1)-EA Мутация №1 (200)	(1+1)-EA Мутация №2 (200)
1	00:00:11.11	00:00:00.06	00:00:22.32	00:00:00.06
2	00:00:10.83	00:00:00.06	00:00:23.38	00:00:00.06
3	00:00:12.47	00:00:00.07	00:00:22.30	00:00:00.06
4	**00:00: 10.82**	**00:00:00.05**	**00:00:22.23**	00:00:00.06
5	00:00: 11.91	00:00:00.07	00:00:25.28	**00:00:00.05**

Из таблицы 1 можно сделать вывод, что для решения поставленной задачи алгоритм (1+1)-EA Мутация №1 выдает лучшие решение при 100 и 200 итерация, но проанализировав таблицу 3.2 можно сказать, что время работы алгоритма (1+1)-EA Мутация №1 ухудшается с увеличение количества итераций. Алгоритм (1+1)-EA Мутация №2 работает очень быстро при любом количестве итераций, при этом он выдает результаты хуже, чем первый алгоритм. Из этого можно сделать вывод, что если пользователю нужно получить более точные результаты, то ему необходимо воспользоваться первым алгоритмом, если ему нужно получить результат очень быстро, то следует использовать второй алгоритм.

Заключение

Основные результаты:

1) Рассмотрены методы решения задач маршрутизации

2) Разработаны эволюционные алгоритмы (1+1)-EA с оператором мутации №1 и с оператором мутации №2 для решения задачи маршрутизации ТС с обратными перевозками.

3) Был проведен вычислительный эксперимент, где были проанализированы результаты работ эволюционных алгоритмов (1+1)-EA с оператором мутации №1 и с оператором мутации №2.

СПИСОК ЛИТЕРАТУРЫ

1. The Vehicle Routing Problem with Backhauls: Properties and Solution Algorithms Charlotte Jacobs-Blecha And Marc Goetschalckx School of Industrial and Systems Engineering Georgia Institute of Technology [Электронный ресурс] // Georgia Tech – URL: https://www2.isye.gatech.edu/~mgoetsch/cali/VEHICLE/VRPB/VRPB.HTM
2. Алесинская Т.В. Основы логистики. Общие вопросы логистического управления: Учебное пособие. – Таганрог: Изд-во ТРТУ, 2005. – 121 с.
3. Неруш, Ю. М. Транспортная логистика : учебник для академического бакалавриата / Ю. М. Неруш, С. В. Саркисов. — Москва : Издательство Юрайт, 2019. — 351 с.
4. Gilbert L., Stefan R., Thibaut V. Vehicle Routing // Heuristics for the Vehicle Routing Problem. – 2014. – P. 87-116.
5. Дэн Саймон Алгоритмы эволюционной оптимизации // Эволюционные стратегии. – 2013. – С. 180-209.

УДК 004.89

В. В. ЯКУПОВА, И. И. КАГИРОВ
yakupovavlada@gmail.com, il1000000002010@ya.ru
Науч. руководв. – канд. техн. наук, доц. Е. Ю. САЗОНОВА

Уфимский государственный авиационный технический университет

ПОДХОД К РЕШЕНИЮ ЗАДАЧИ РАСПОЗНАВАНИЯ ЖЕСТОВ РУК НА ОСНОВЕ ИНТЕЛЛЕКТУАЛЬНЫХ МЕТОДОВ

Аннотация. В статье рассмотрена задача автоматизации процесса распознавания жестов рук в режиме реального времени путем разработки программного обеспечения. Авторами обоснована актуальность разработки специализированного программного обеспечения. Приведены содержательная постановка задачи и структура решения задачи.
***Ключевые слова*:** распознавание жестов рук; анализ изображений и видео; цифровая обработка изображений; машинное зрение; сверточные нейронные сети.

Введение

В современном мире довольно высок процент людей, нуждающихся в специализированном программном обеспечении вследствие нарушений функций организма. По данным ВОЗ, более 5% населения мира (около 430 миллионов человек) нуждаются в реабилитации для решения проблемы «инвалидизирующей» потери слуха. «Инвалидизирующей» называется потеря слуха в слышащем лучше ухе, превышающая 40 дБ у взрослых людей и 30 дБ у детей. Прогнозируется, что к 2050 г. более 700 миллионов человек будут страдать от инвалидизирующей потери слуха. Таким образом, количество людей с нарушениями слуха стремительно увеличивается, вследствие чего возникает проблема разработки специализированного программного обеспечения.

Одним из способов улучшения условий жизни людей с нарушениями слуха является внедрение возможности использования ими жестового языка при коммуникации в обществе, что является одной из главных составляющих процесса социальной реабилитации инвалидов по слуху, их успешной интеграции и адаптации в современное общество. Жестовый язык может быть задействован во многих сферах социальной жизни: в суде, в полиции, в налоговой инспекции, в приемной врача и т.д. Однако процесс коммуникации человека,

владеющего жестовым языком, и человека, подобными знаниями не обладающего, не может быть осуществлен без сурдопереводчиков. При этом отметим, что в России число работающих сурдопереводчиков составляет всего около 900 человек, на каждого из которых приходится около 100 тысяч глухих. Очевидно, что этого количества недостаточно, чтобы люди с нарушениями слуха чувствовали себя в обществе комфортно и имели возможность пользоваться своими правами в полной мере. Поэтому одним из возможных способов решения данной проблемы является разработка программного обеспечения, выполняющего роль сурдопереводчика, то есть способного распознавать жесты рук в режиме реального времени.

Стоит упомянуть тот факт, что жесты рук при управлении компьютерными системами могут использоваться и людьми без нарушений слуха в целях достижения более удобного человеко-машинного взаимодействия.

Таким образом, требуется разработать программное обеспечение, которое будет способно распознавать жесты рук в режиме реального времени.

Постановка задачи распознавания жестов рук

Рассмотрим задачу распознавания жестов рук в режиме реального времени. Пусть имеется множество объектов S – жесты рук. Каждый элемент из множества S имеет геометрические признаки, такие как кончики пальцев, направление пальцев, контур руки, а также негеометрические признаки – цвет кожи, форма, текстура и другие.

Также имеется I – дискретное изображение сцены, поступающей с вебкамеры пользователя, в которой могут присутствовать жесты рук. При этом сама сцена находится в идеальных условиях, то есть жесты рук различимы (отсутствует взаимное перекрытие элементов руки, имеют место хорошие условия освещения и т.п.). Изображение I представлено цветовым пространством RGB.

Задача заключается в обработке изображения I таким образом, чтобы идентифицировать и распознать находящиеся на нем объекты множества S.

В качестве входных данных программы будут использоваться изображения с устройства видеофиксации (веб-камеры). Ввод входных данных программы должен быть организован посредством захвата видеопотока.

В качестве выходных данных программы будут выступать результаты распознавания жестов, выводимые на экран в виде текстовой надписи.

Структура решения задачи распознавания жестов рук

На рисунке 1 представлена формальная постановка задачи распознавания жестов рук.

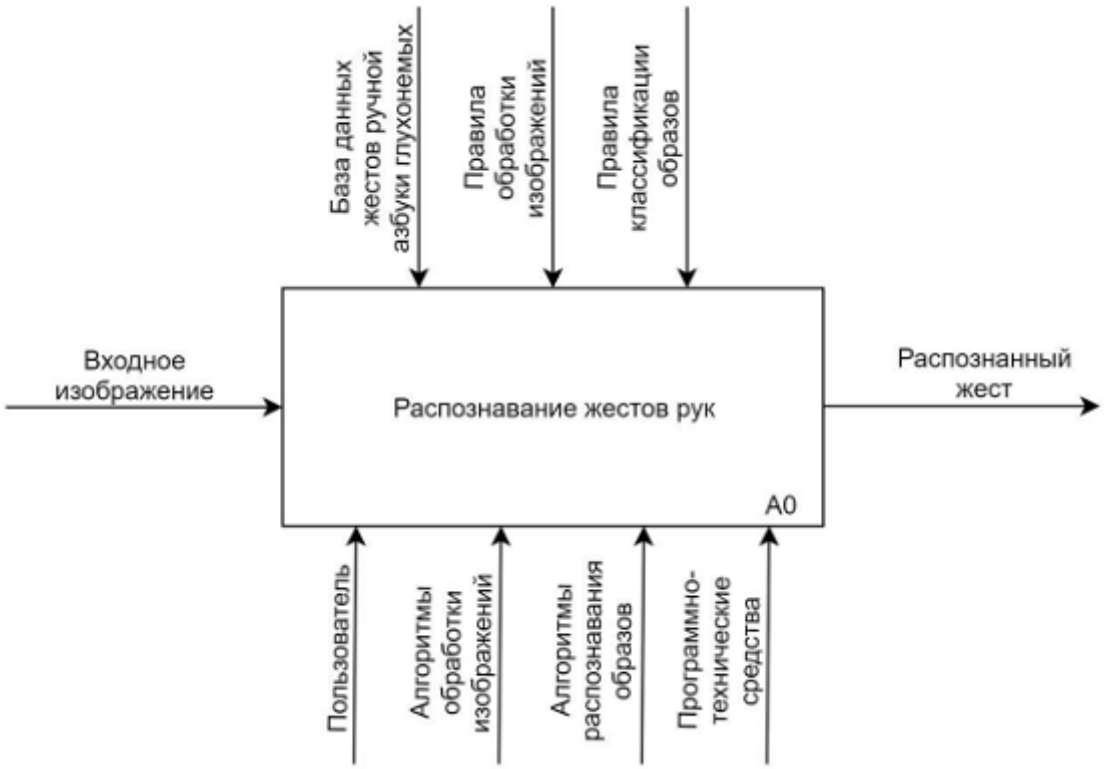


Рис. 1. Формальная постановка задачи

На вход подается изображение с веб-камеры пользователя. В качестве механизмов выступают алгоритмы обработки изображений и алгоритмы распознавания образов, участие пользователя и программно-технических средств. С учетом имеющейся базы данных жестов ручной азбуки глухонемых выдается результат распознавания жестов рук (в виде текстовой надписи), при условии, что таковые присутствуют на входном изображении.

Декомпозиция задачи распознавания жестов рук осуществляется в соответствии с рисунком 2.

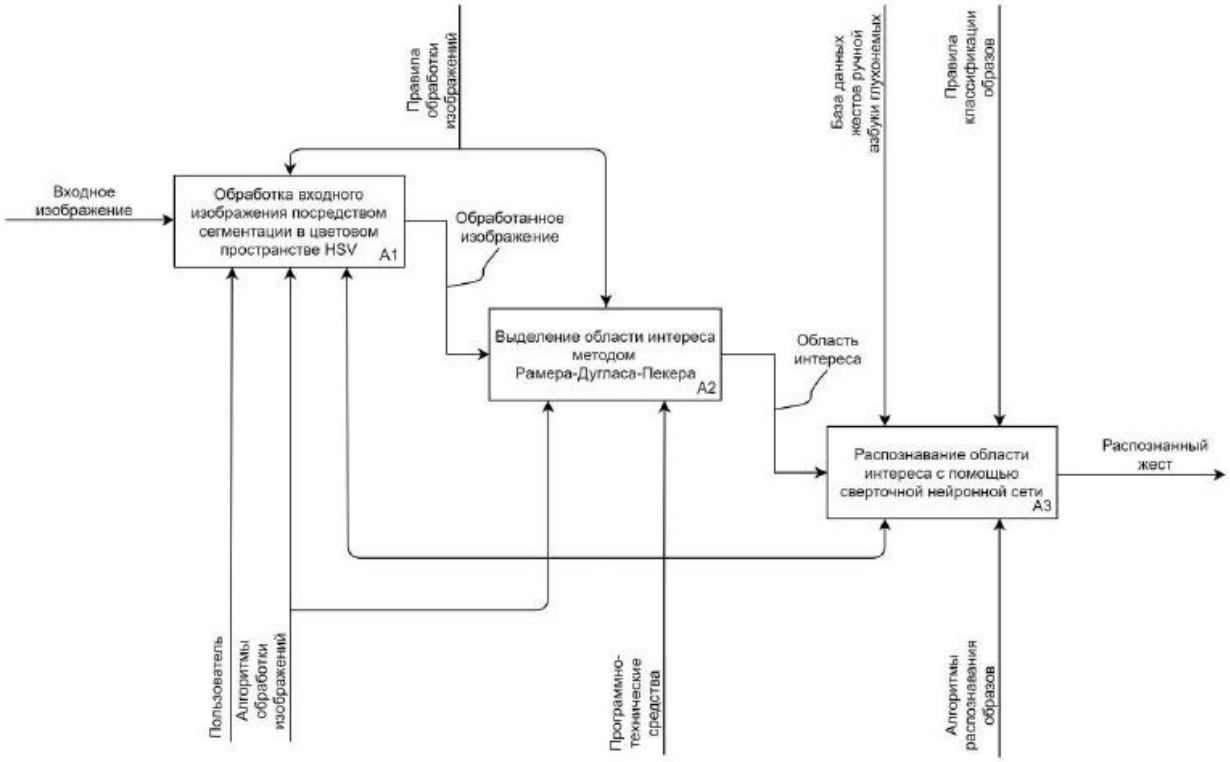


Рис. 2. Декомпозиция задачи распознава-ния жестов рук

Рассмотрим подробнее процесс распознавания жестов рук. Решение данной задачи состоит из следующих этапов: обработка входного изображения (задача обнаружения); выделение области интереса (задача отслеживания); распознавание области интереса (задача распознавания). Задача обнаружения состоит из процедур преобразования цветовых компонентов, вычисления гистограммы и обратной проекции, цифровой обработки. Задача отслеживания включает процедуры нахождения контуров и аппроксимации найденного контура. Решение задачи распознавания основано на сверточных нейронных сетях.

Авторами разработано программное обеспечение, которое позволяет автоматизировать процесс распознавания жестов рук в режиме реального времени. Программное решение было апробировано на алфавите глухонемых и может быть использовано при обучении сурдопереводчиков.

Заключение

В статье рассматривается актуальная проблема разработки специализированного программного обеспечения для людей с ограниченными возможностями, а именно задача распознавания жестов рук в реальном времени. Авторами поставлена задача распознавания жестов рук в реальном времени и предложен подход, включающий решение задач обнаружения, отслеживания и распознавания. Для решения задачи обнаружения используется процедура сегментации в цветовом пространстве; для задачи отслеживания – процедура выделения области интереса методом Рамера-Дугласа-Пекера; для задачи распознавания – классификация методом сопоставления изображения с эталоном.

Результаты исследования, приведенные в статье, получены в рамках выполнения грантов РФФИ 19-07-00709 и государственного задания No FEUE-2020-0007.

СПИСОК ЛИТЕРАТУРЫ

1. Программное обеспечение для распознавания жестов рук в режиме реального времени : выпускная квалификационная работа / Кагиров Ильяс Илдарович .— Уфа, 2019 .— 93 с. — 09.03.04 -Программная инженерия .— ВО .— Очная .— 51 с.
2. Носов А.В. Алгоритм распознавания жестов рук на основе скелетной модели кисти руки // Вестник СибГАУ. No 2(54). 2014. с. 63.
3. Абдугалимова Е.Г., Степурко К.В., Фаворская М.Н. Сегментация изображения руки на видеопоследовательности // Актуальные проблемы авиации и космонавтики. 2013. No9. С. 349.
4. Юсупова Н. И. Технологии искусственного интеллекта и машинного обучения в задачах семантического представления и анализа данных: монография // Н. И. Юсупова, О.Н. Сметанина, М. М. Гаянова и др. – М.: "Издательство "Инновационное машиностроение", 2020. – 242 с.

СЕКЦИЯ 5.3
АНАЛИЗ ДАННЫХ, ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И МАШИННОЕ ОБУЧЕНИЕ

УДК 004.057.5

Д. Ю. АНДРУШКО
andrewrush@mpo14.ru
Науч. руководв. – д-р техн. наук, проф. Д. А. РИЗВАНОВ

Уфимский государственный авиационный технический университет

КИБЕРФИЗИЧЕСКИЕ СИСТЕМЫ И ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ: ОСНОВНЫЕ ТРЕНДЫ

Аннотация. Киберфизические системы имеют сложную структуру и поведение, поэтому классически методы оценки надежности не могут быть эффективно для них применяться. Методы глубокого обучения являются возможным решением данной проблемы, поэтому проектирование архитектуры тестового стенда для оценки надежности киберфизических систем с обучением и применением нейросетевых моделей является актуальной задачей. Однако за последнее время произошло несколько событий, которые негативно повлияли на стоимость и доступность комплектующих для тестового стенда. В работе рассмотрены данные события, а также предложено решение, позволяющее увеличить количество доступных комплектующих, которые можно использовать в составе тестового стенда, т.е. частично компенсирует отрицательный эффект майнинг-бума и дефицита полупроводников.
***Ключевые слова*:** киберфизические системы; машинное обучение; графические ускорители; ARM, майнинг-бум, дефицит полупроводников.

Компоненты робототехники и сенсорика являются одной из основных областей применения для программно-аппаратных средств, предназначенных для решения задач, определяемых понятием «киберфизические системы». Киберфизическая Система (КФС) является интеграцией вычислительных, сетевых и физических процессов.

Основными требованиями к подобным системам является надежность и предсказуемость поведения. Киберфизические Системы (КФС) являются сложными как в структурном, так и поведенческом планах. Они состоят из многочисленных гетерогенных компонентов, генерирующих большие объемы данных, обменивающихся информацией и формирующих чрезвычайно сложные паттерны поведения. Это делает практически невозможным эффективную настройку и применение классических методов оценки надежности.

Популярные на сегодняшний день методы, основанные на глубоком обучении используют классификатор, нейронную сеть, обученную отличать нормальное поведение системы от ненормального. Эти методы были предложены десятилетия назад, но только недавнее бурное развитие методов искусственного интеллекта позволило создавать эффективные средства выявления ошибок на основе методов глубокого обучения.

В исследованиях [1][2] была предложена структурная модель для тестового стенда, который позволяет обучать и применять нейросетевые модели, в том числе для оценки надежности киберифизических систем. Однако с момента выхода исследования произошло несколько изменений, которые перечислены ниже.

1. Майнинг-бум привел к существенному увеличению стоимости графических процессоров и недоступности большинства новых моделей на рынке.

2. Дефицит полупроводников из-за пандемии COVID-19 и последующего снижения темпов производства также негативно отразился на конечной стоимости вычислительных устройств.

3. Как следствие из вышеперечисленного, резкое увеличение итоговой стоимости тестового стенда.

4. Кроме того были наложены санкции на нескольких производителей электроники, в частности на Huawei и ZTE, которые впоследствии частично были сняты, но все равно риски наложения санкций на покупку и производство оборудования необходимо учитывать.

5. Также корпорация Apple выпустила персональный компьютер с процессором M1 на архитектуре ARM, который успешно конкурировал с процессорами AMD и Intel в прикладных задачах [3].

В связи с новыми трендами были сформулированы следующие задачи.

1. Рассмотреть альтернативные архитектуры вычислительных устройств. Изначально в тестовом стенде использовались процессоры на архитектуре AMD64 (x86-64) и видеокарта с поддержкой технологии CUDA. Необходимо

рассмотреть другие архитектуры процессоров как возможные альтернативы в случае обострения ситуации с майнингом и дефицитом полупроводников.

2. Изучить отечественные альтернативы, которые можно будет использовать в результате наложения санкций на покупку процессоров с архитектурой AMD64.

3. Выбрать открытый программный проект, который использует машинное обучение, и внести в исходный код проекта изменения, которые позволят увеличить количество поддерживаемого оборудования и архитектур.

В отечественной микроэлектронике процессоры разрабатывают (или производят по лицензии) компании АО «МЦСТ», «Байкал Электроникс», ФГУ ФНЦ НИИСИ РАН, АО НПЦ «ЭЛВИС», Миландр, НТЦ «Модуль», ООО «КМ211», ОАО «Мультиклет», дизайн-центр «ГеоСтар Навигация», компания «ИВКС» (бренд IVA Technologies), ООО «СИНТАКОР» (Syntacore) [4]. Ниже рассмотрены основные лицензируемые или разработанные отечественными компаниями архитектуры.

Процессоры на базе архитектуры ARM изначально применялись в мобильных и энергоэффективных устройствах, но теперь все чаще используются в персональных компьютерах.

Встраиваемые системы и микроконтроллеры, в частности сетевое и телекоммуникационное оборудование, являются одной из основных сфер применения для процессоров на архитектуре MIPS, однако не ограничиваются только данной аппаратной платформой.

АО «МЦСТ» разработала отечественную реализацию SPARC-процессоров и самостоятельно создала с нуля архитектуру E2K.

RISC-V является перспективной и открытой архитектурой, которая не требует лицензионных отчислений и поэтому активно развивается энтузиастами и отдельными представителями бизнеса в сфере IT-технологий.

Наиболее простым способом переноса (портирования) программного проекта на другую архитектуру является переписывание фрагментов кода, ко-

торые содержат аппаратно-зависимые привязки. Поэтому хорошим кандидатом для исследования является любой открытый проект, который имеет отношение к машинному обучению. В рамках исследования использован исходный код проекта SimSwap, который доступен для изучения любому желающему в репозитории GitHub [5], а также является практической реализацией другого исследования [6].

В результате переписывания аппаратно-зависимых фрагментов кода проект можно запустить на любой процессорной архитектуре, которая поддерживается фреймворком PyTorch, в частности на процессоре с ядрами ARM Cortex-A53 (рис. 1). Отечественный процессор Байкал-М разработан на базе старшей модели данной линейки процессоров, с ядрами ARM Cortex-A57 соответственно, поэтому измененный исходный код из проекта SimSwap также может быть запущен на любом оборудовании с данным вычислительным устройством.

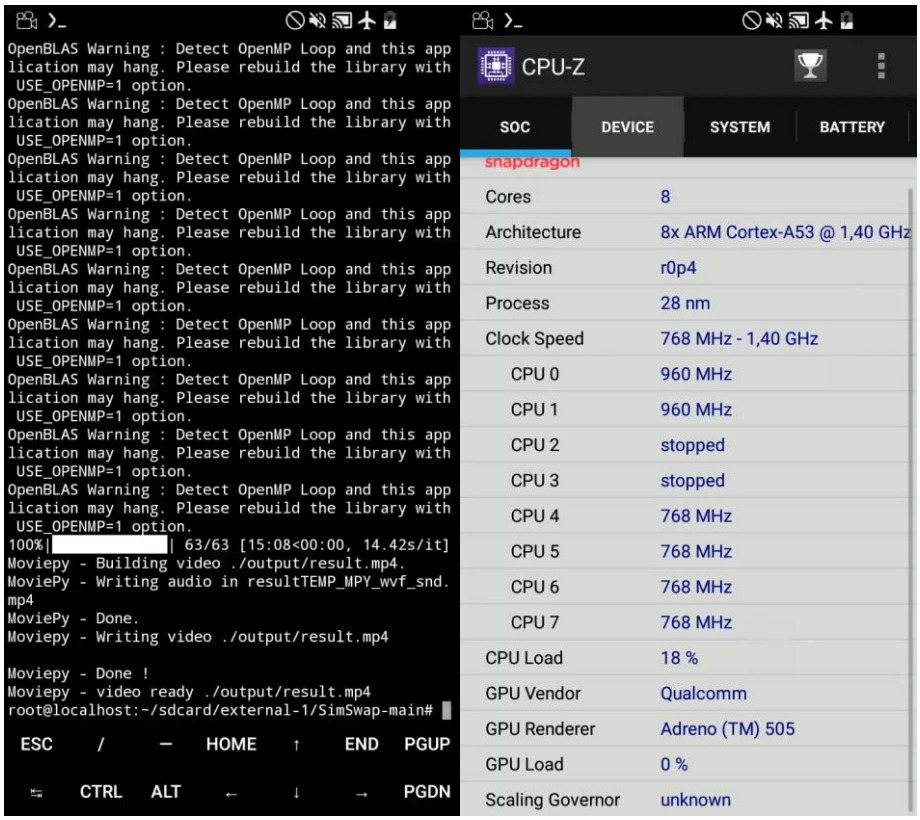


Рис. 1. Запуск проекта SimSwap на процессоре ARM Cortex-A53

Наличие видеокарты теперь необязательно, однако ее использование в программном проекте способно значительно повысить производительность тестового стенда.

Таким образом, в процессе изменения исходного кода проекта SimSwap получилось значительно увеличить количество поддерживаемых архитектур, а также добавлена возможность использования нейросетевых моделей на любой архитектуре, которая поддерживается фреймворком PyTorch. Результаты исследования увеличивают количество возможных комплектующих, которые можно использовать в составе тестового стенда для обучения и применения нейросетевых моделей, что частично компенсирует ущерб от возможных санкций, дефицита полупроводников и значительно уменьшает финансовые и материальные затраты, потому что на момент исследования (осень 2021 года) любое бюджетное устройство на базе ARM-процессоров стоит значительно дешевле, чем отдельная видеокарта NVIDIA с поддержкой технологии CUDA или ROCm-совместимая видеокарта AMD и нет никаких очевидных предпосылок к возможности возникновения диаметрально противоположной ситуации.

СПИСОК ЛИТЕРАТУРЫ

1. Сметанина О.Н., Сазонова Е.Ю., Андрушко Д.Ю. Программно-аппаратный комплекс для оценки надежности с использованием искусственного интеллекта // Современные наукоемкие технологии. – 2020. – № 7. – С. 90-97. DOI: https://doi.org/10.17513/snt.38140
2. Андрушко Д.Ю. Программно-аппаратный комплекс для мониторинга информации в социальных сетях // Этнополитический и религиозный экстремизм в россии: социально-культурные истоки, угрозы распространения в информационной среде, методы противодействия. Сборник материалов Всероссийской молодежной научной школы-конференции – 2020. – С. 136-142. DOI: https://doi.org/10.17513/snt.38140
3. Guzide O., Sloboda S. Is Apple’s new M1 chip a gamechanger in computing? //Proceedings of the West Virginia Academy of Science. – 2021. – Т. 93. – №. 1.
4. Российские процессоры [Электронный ресурс] // URL: https://ruxpert.ru/Российские_микропроцессоры (дата обращения: 10.09.2021).
5. SimSwap: An Efficient Framework For High Fidelity Face Swapping [Электронный ресурс] // URL: https://github.com/neuralchen/SimSwap (дата обращения: 10.09.2021).
6. Renwang Chen, Xuanhong Chen, Bingbing Ni, and Yanhao Ge. 2020. SimSwap: An Efficient Framework For High Fidelity Face Swapping. In Proceedings of the 28th ACM International Conference on Multimedia (MM '20). Association for Computing Machinery, New York, NY, USA, 2003–2011. DOI: https://doi.org/10.1145/3394171.3413630

УДК 004.657

М. А. БАДАЕВА
Badmasha16@gmail.com
Науч. руководв. – доц. Ю. И. ВАЛИАХМЕТОВА

Уфимский государственный авиационный технический университет

ПРОБЛЕМА РАСЧЕТА ИНСОЛЯЦИИ С ПРИМЕНЕНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Аннотация. В работе приводится описание терминологии проблемы расчета инсоляции в жилых помещениях и сравнительный анализ методов расчета инсоляции. Показана актуальность рассматриваемой тематики, современного состояния проблемы в области расчета инсоляции в жилых помещениях. Отмечены аспекты решаемой проблемы, выявленные при анализе подходов, моделей и методов, используемых информационных технологий, инструментальных средств и программных решений проблемы.
Ключевые слова: инсоляция жилых помещений; методы расчета инсоляции; инсографик; коэффициент естественной освещенности.

Введение

Различные экономические и социальные причины привели в прошлом к неправильному использованию земли: появились неудачные архитектурные решения, такие как, например:

– улица-коридор, на которой здания расположены по прямой сплошной линии;

– наличие смотрящих друг на друга глухих стен;

– высота домов больше ширины пространства между фасадами.

Это привело к антисанитарным условиям с точки зрения инсоляции и естественного освещения.

Спустя некоторое время, с появлением новых социально-экономических условий, здания начали строить все дальше друг от друга, вокруг технически оснащенных зданий появились зеленые насаждения, структурные единицы были созданы таким образом, что фасады и помещения получили удовлетворительные условия инсоляции и естественного освещения. Но появилась опасность расточительства по отношению к земле. В этот момент и возникла задача расчета инсоляции в жилых помещениях.

С другой стороны, в современном мире большие задачи, стоящие перед градостроителями, обязывают не только расширить масштабы и повысить темпы строительства жилых районов, но также пересмотреть методы и приемы их планировки и застройки с тем, чтобы в соответствии с общим планом развития народного хозяйства страны можно было бы эффективно переустраивать старые и строить новые города, здания и сооружения на базе новейших достижений науки.

Инсоляция или облучение прямым солнечным светом жилых помещений обладает положительным воздействием на организм человека, поэтому при застройке новых районов города и проектировании зданий поставлено ограничение по инсоляции. В последнее время нормы по инсоляции снижаются. В СССР норма составляла 3 часа в день, в нормах с 2010 года она составляет 2, а в некоторых случаях 1,5 часа в день и допускается прерывистое облучение.

Причиной снижения нормы инсоляции в жилых помещениях стала высокая плотность застройки. Города расширяются, высота зданий непрерывно растет вместе с ростом и популяризацией новых информационных технологий. Противостояние между снижением продолжительности облучения за счет увеличения плотности застройки и сохранением продолжительности облучения для обеспечения необходимых санитарно-гигиенических условий в помещениях жилых зданий выливается в выступления специалистов в научных изданиях и средствах массовой информации.

Количественная мера инсоляции – продолжительность облучения прямым солнечным светом, не является однозначной количественной мерой. Облучение помещений солнечным светом равной продолжительности в утренние, околополуденные или вечерние часы суток принесет в эти помещения различную по величине солнечную энергию, и, соответственно, приведет к различному уровню санитарно-гигиенического воздействия на микрофлору жилых помещений.

Таким образом, исследование инсоляции жилых помещений является весьма актуальной проблемой.

Базовые методы расчета инсоляции. Современный метод расчета.

Инсографик (инсоляционная линейка) и его применение.

Инсографик или инсоляционная линейка (далее – ИЛ) — проекция модели видимой траектории движения солнца на горизонтальную плоскость, то есть двухмерная интерпретация трехмерной модели движения солнца относительно расчетной точки (условного наблюдателя).

Расчет инсоляции выполняется «ручным» методом с использованием инсографика по официальной методике, изложенной в ГОСТ Р 57795-2017 «Методы расчета продолжительности инсоляции». Метод расчета по инсографику (инсоляционной линейке) достаточно прост, нагляден и применим в большинстве проектных ситуаций.

В общем случае расчетную продолжительность инсоляции определяют три фактора:

– ориентация фасада, на котором располагается расчетный светопроем. Данный фактор определяется так называемой «инсоляцией на фасаде», показывающей потенциально возможную инсоляцию на поверхности фасада с исследуемым окном (проемом) без учета всех видов затенения – собственного затенения конструкциями окон и элементами фасада и затенения противостоящими объемами.

– теневой угол светопроема – потери света за счет выступов конструкции самого окна и за счет прилегающих элементов фасада (балконы, лоджии, карнизы, навесы, пилястры, фасадные выступы);

– внешнее затенение противостоящими объектами.

На инсоляционной линейке нанесена временная и высотная шкалы. Временная шкала представлена радиальными линиями, соответствующими азимутальным углам положения солнца в течение дня в определенный момент времени. Радиальные временные линии в зависимости от точности графика могут быть проведены через 10; 15 или 30 минут. Линии, соответствующие часовым

интервалам, имеют на периферии графика отметки — время (час суток) и угловую высоту стояния солнца. Точка схода линий временной шкалы образует центр графика. Высотная шкала представлена дугами с шагом 1; 5 или 10 метров, пересекающими линии временной шкалы. Дуги высотной шкалы показывают высоту объекта, конец тени от которого в соответствующий момент времени будет попадать в центр графика. Центр графика соответствует нулевой отметке высотной шкалы.

Инсографик строится по солнечному времени, не совпадающему с поясным временем в конкретном населенном пункте и, соответственно, со временем восхода и захода, которое показывают поисковые системы и калькуляторы тени, представленные в интернете. Отличительной особенностью ИЛ является его симметрия относительно полуденного луча (ось графика). ИЛ строят на определенную пару дат (в зависимости от географической зоны – северной, центральной или южной) и для определенной географической широты.

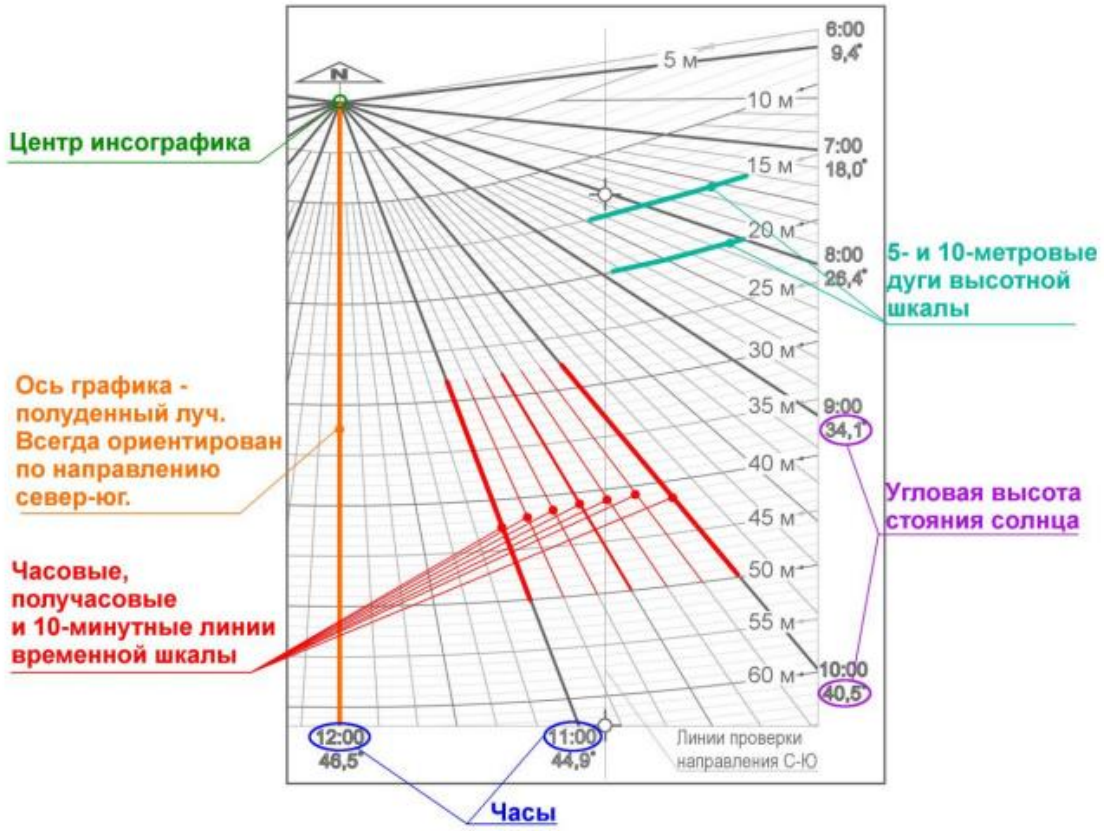


Рис. 1. Инсоляционная линейка

Подход к подсчету освещения

Стоит признать, что метод расчета инсоляции, наиболее популярный в настоящее время, значительно выигрывает в плане эффективности и временных затрат у метода, который применялся специалистами в XX веке.

В руководстве по проектированию естественного освещения зданий 1976г. изложен метод расчета естественного освещения в здании с помощью формул. Все показатели буквально считались вручную вплоть до количества попадаемых в жилое помещение лучей. Один из основных показателей – коэффициент естественной освещенности.

Коэффициент естественной освещенности – отношение естественной освещенности, создаваемой в некоторой точке заданной плоскости внутри помещения светом неба (непосредственным или после отражений), к одновременному значению наружной горизонтальной освещенности, создаваемой светом полностью открытого небосвода; выражается в процентах.

С помощью этого коэффициента производится нормирование естественного и совмещенного освещения в помещениях, коэффициент применяется при проектировании зданий и сооружений и в настоящее время.

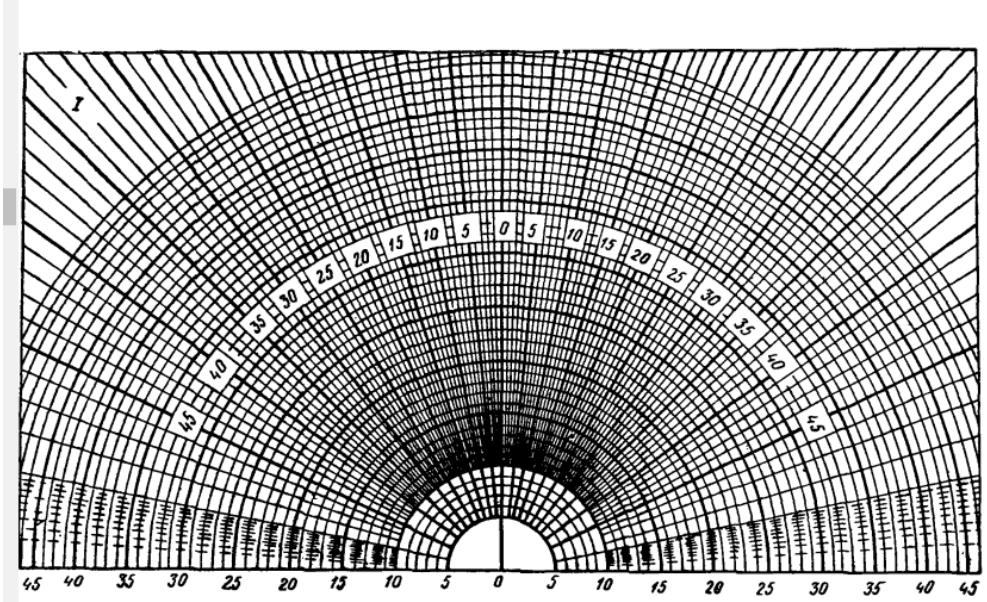


Рис. 15. График *I* для подсчета количества лучей n_1 и n_1', проходящих через световой проем на характерном поперечном разрезе помещения при боковом освещении (цифры на полуокружности обозначают количество лучей, на нижней горизонтальной линии — номера полуокружностей)

Рис. 2.

Заключение

Проблема в настоящее время заключается в том, что при достаточно большом скачке информационных технологий (в области строительства появились: Autodesk Revit, ArchiCAD) расчет инсоляции все еще производится вручную. Данные технологии позволяют проектировать и визуализировать застройки, но не позволяют в полной мере учитывать важные показатели и коэффициенты. Такой подход увеличивает вероятность возникновения человеческого фактора и ошибок в процессе расчетов, поэтому актуальность проблемы инсоляции в ближайшей перспективе будет высока.

СПИСОК ЛИТЕРАТУРЫ

1. Ю.Б.Поповский. РАСЧЕТЫ ИНСОЛЯЦИИ В ЖИЛЫХ ПОМЕЩЕНИЯХ с применением инсографика для 55^0 с.ш. Учебно-методическое пособие по выполнению расчетно-графической работы по архитектурной светологии.// URL: https://marhi.ru/fpkp/doc/20-21/Raschet_Insolyatsii_Posobie_MArkhI_Popovskiy.pdf
2. В.А. Каратаев, Е.В. Адонкина, М.Г. Тен, С.А. Нефедов. Инсоляция помещений и территорий застройки.// URL: http://www.ng.sibstrin.ru/adonkina/insol/Karataev.pdf
3. Н. М. Гусев, Н. Н. Киреев. Руководство по проектированию естественного освещения зданий. // Науч.-исслед. ин-т строит, физики Госстроя СССР. Стройиздат. 1976г. 96 с.

УДК 004.657

Е. Ю. БАРУДКИНА
katerina.barudkina@mail.ru
Науч. руководов. – д-р техн. наук, проф. В. Е. ГВОЗДЕВ

Уфимский государственный авиационный технический университет

КОМПЛЕКСНЫЙ АНАЛИЗ СОСТОЯНИЯ РАСПРЕДЕЛЕННЫХ ДИНАМИЧЕСКИХ СИСТЕМ (ПРИРОДНО-ТЕХНИЧЕСКИХ)

Введение

Территориальные системы являются разновидностью распределенных сложных систем. В управлении их состоянием на разных уровнях (стратегическом, тактическом, операционном) задействованы разные государственные и негосударственные структуры, которые имеют собственные представления о ценностях и возможных путях их достижения. Это обстоятельство является причиной различия в целях управления и, как следствие, различия в подходах и технологиях изучения, сбора, передачи, систематизации и хранения данных, которые в различных ракурсах характеризуют состояние территориальной системы.

Комплексный анализ территориальных систем включает среди прочих получение ответа на следующий вопрос: насколько различаются результаты, получаемые относительно одного и того же параметра состояния (либо группы параметров) как в территориальном, так и во временном аспектах.

Для изучения и анализа была выбрана геморрагическая лихорадка с почечным синдромом, и ее распространение в регионах Республики Башкортостан за последние 10 лет. В качестве показателя взято количество заболевших на 1000 человек в каждом отдельном регионе.

Геморрагическая лихорадка с почечным синдромом (ГЛПС) – природно-очаговое вирусное заболевание, характерными признаками которого являются лихорадка, интоксикация, повышенная кровоточивость и поражение почек.

Анализ данных за длительный период позволит выявить неявные закономерности, и использовать результаты анализа в качестве информационной под-

держки при реализации превентивного подхода в управлении территориальными системами.

В начале был произведен алгоритм построения абсолютной шкалы, так, как только шкалы, построенные по абсолютной шкале, можно использовать для сопоставления состояний территорий в различных временных срезах.

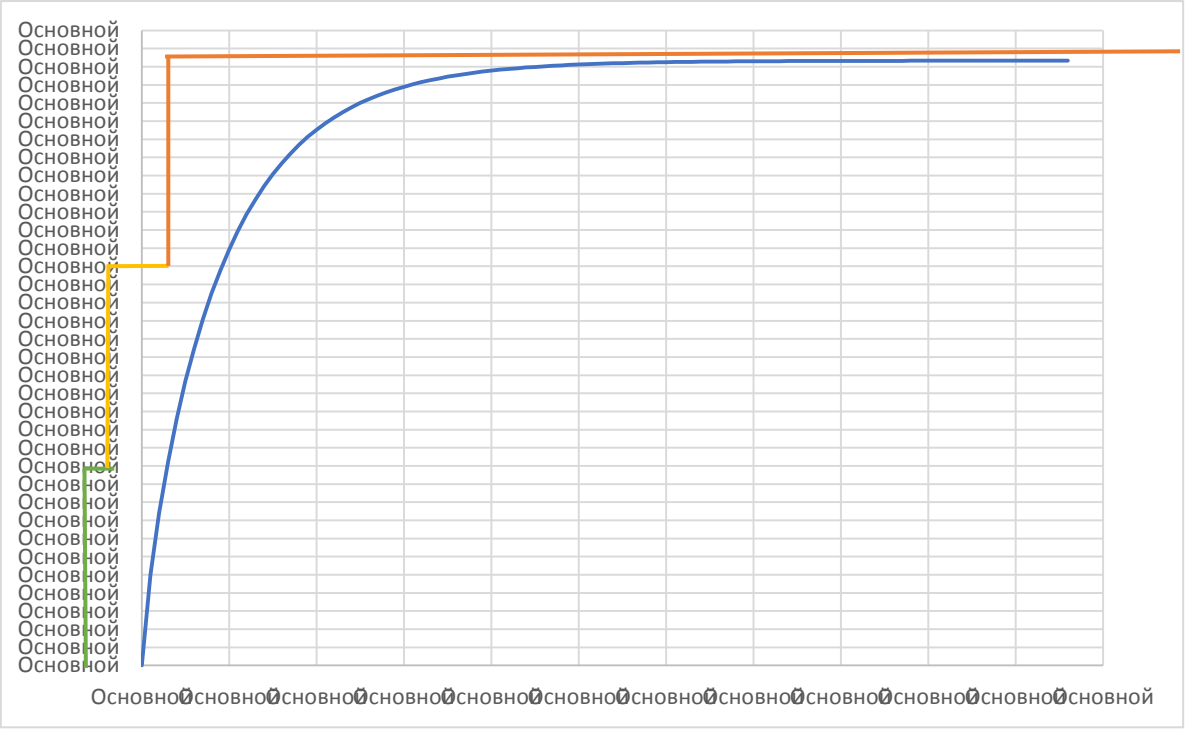


Рис. 1. Гамма-распределение

Далее произвели анализ изменчивости состояния территориальных систем в целом.

Для этого, используя составленную классификационную шкалу, подсчитали все состояния районов в каждом году. Данные приведены в таблице 1.

Таблица 1

Количество состояний районов

	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018
нет зарегистрированных случаев	6	13	10	6	16	6	6	12	9	10
низкий уровень заболеваемости	12	16	16	9	21	7	7	11	12	17
средний уровень заболеваемости	17	19	15	20	13	16	27	20	21	18
высокий уровень заболеваемости	19	6	13	19	4	25	14	11	12	9

По каждому году построили гистограмму, где по оси у откладывается количество районов, а по оси х уровень заболеваемости.

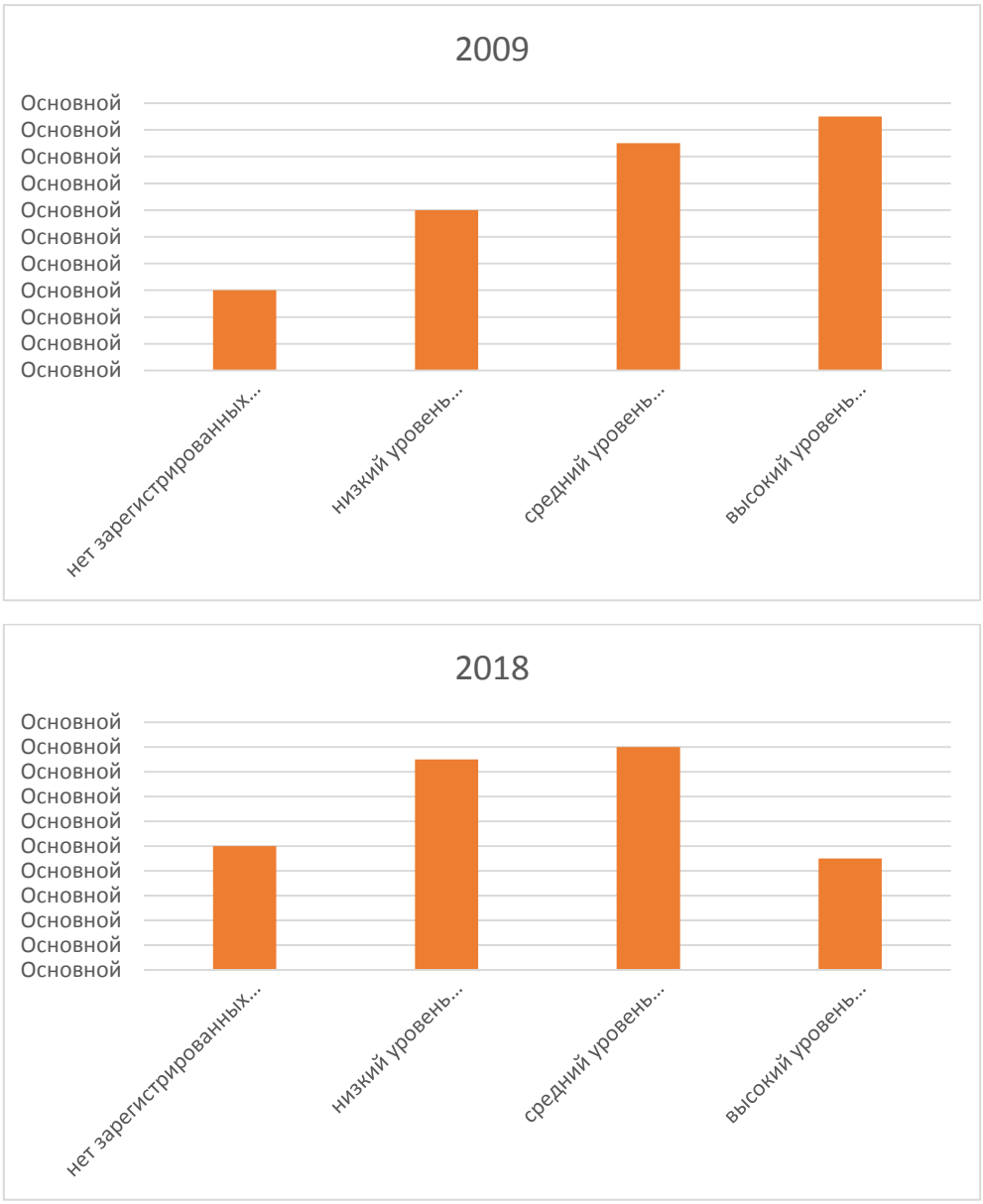


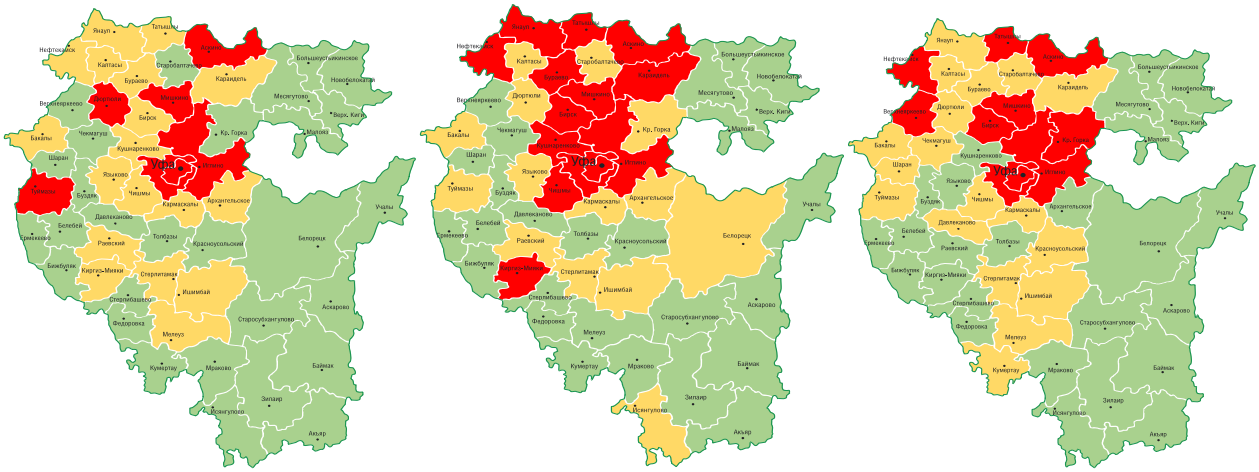
Рис. 2. Гистограммы построенные по результатам районирования территориальной системы

Ниже в качестве примера представлена таблица, сформированная на основе полученных в ходе исследований гистограмм. Цифры выше главной диагонали соответствует случаю, когда в качестве теоретического закона распределения выбирались гистограммы, соответствующие в таблице годам, проиндексированным по оси ординат. Числа, расположенные ниже главной диагонали, соответствуют годам, проиндексированным по оси абсцисс.

Таблица 2

	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018
2009	-	18,630	6,130	1,279	36,200	4,037	9,281	9,981	5,020	10,072
2010	33,146	-	9,701	35,051	4,816	69,472	22,867	5,859	8,441	2,307
2011	5,636	5,736	-	9,098	11,660	17,806	16,339	3,937	3,577	1,893
2012	1,450	22,556	11,256	-	46,959	3,139	4,210	9,813	5,129	15,241
2013	67,588	5,522	23,998	73,126	-	126,526	55,660	21,781	27,843	11,185
2014	5,074	34,741	20,061	3,011	62,869	-	12,403	17,126	13,394	27,442
2015	9,061	26,680	19,643	4,172	59,069	13,124	-	10,743	6,690	21,738
2016	9,359	4,679	4,220	9,182	17,329	23,073	7,723	-	0,982	4,170
2017	5,845	6,302	3,242	5,881	20,575	18,357	5,131	1,214	-	3,373
2018	14,237	2,014	2,337	16,698	8,708	36,149	14,760	3,184	3,071	-

Ниже приведены картографические материалы, соответствующие 2010, 2011 и 2018 годам.



2010 год 2011 год 2018 год

Рис. 3.

Заключение

Анализируя полученные результаты, в случае выбора уровня доверия 0.9, можно заключить, что схожими являются состояния, соответствующие 2009 и 2012 годам; 2010, 2011 и 2018 годам; 2016 и 2017 годам.

Отнесение каждого из участков территориальной системы к одному из классов состояний при условии, что разным характеристикам ставится в соответствии одно и тоже число классов, обеспечивает, с одной стороны, сопоставимость оценок состояния по частным характеристикам, с другой стороны,

возможность формирование комплексных оценок состояния. В рамках предлагаемого подхода можно увеличивать число частных характеристик, то есть число точек зрения на состояние территориальной системы.

СПИСОК ЛИТЕРАТУРЫ

1. Реймерс Н.Ф. Природопользование: Словарь-справочник. – М.: Мысль, 1990. – 637 с.
2. Викторов А.С. Рисунок ландшафта. – М.: Мысль, 1986. – 179 с.
3. Гузаиров М.Б., Гвоздев В.Е., Ильясов Б.Г., Колоденкова А.Е. Статическое исследование территориальных систем – М.: Машиностроение, 2008. – 187 с.
4. Вентцель Е.С. Теория вероятностей. – М.: Наука, 1969. – 576 с.
5. Айвазян С.А., Бухштабер В.М., Енюков И.С., Мешалкин Л.Д. Прикладная статистика. Классификация и снижение размерности. – М.: Финансы и статистика, 1989. – 607 с.
6. Губанов В.А., Захаров В.В., Коваленков А.Н. Введение в системный анализ. – Л.: Изд-во ЛГУ, 1988. – 232 с.
7. Дэйвисон М. Многомерное шкалирование: Методы наглядного представления данных / Пер. с англ. В. С. Каменского. – М.: Финансы и статистика, 1988. – 254 с
8. Мильков Ф.Н. Физическая география: современное состояние, закономерности, проблемы. – Воронеж, 1981. – 136 с.
9. Михайлов Н.И. Физико-географическое районирование. – М.: МГУ, 1985. – 184 с.
10. Розенберг Г.С., Шитиков В.К., Брусиловский П.М. Экологическое прогнозирование (функциональные предикторы временных рядов). – Тольятти, 1994. – 182 с.
11. Федина А.Е. Физико-географическое районирование. – М.: МГУ, 1981. – 128 с.

УДК 004.657

Н. С. ВАСИЛЬЕВ
krankenmorder@gmail.com
Науч. руководитель – канд. техн. наук, доц. О. С. НУРГАЯНОВА

Уфимский государственный авиационный технический университет

ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИИ ПАРСИНГА В РАЗРАБОТКЕ НОВЫХ МАТЕРИАЛОВ

Аннотация. Парсинг – это автоматизированный сбор неструктурированной информации, ее преобразование и выдача в структурированном виде. Парсинг включает в себя множество аспектов: выборка необходимой информации с сайта-источника, распознавание и преобразование информации, создание структурированного хранилища.
***Ключевые слова*:** парсинг; распознавание; структуризация; патент; хранилище.

Целью нашего исследования является парсинг. Парсинг – это сбор информации из интернета по разным критериям в автоматическом режиме. Задача состоит в написании программы-парсера, которая создает определенную выборку из необходимых нам патентов сплавов и организует из них первичное неструктурированное хранилище. В дальнейшем происходит распознавание полученной выборки патентов и создание конечного структурированного хранилища с процентным содержанием химических элементов сплавов. После получения данной конечной базы данных перед нами открывается много путей в разработке новых материалов, которые могут быть использованы во многих областях: от медицины до авиации.

Существует несколько способов создания программы или скрипта парсера. Принцип его действия зависит от наших целей. Парсер ищет на указанном нами сайте или страницах данные, соответствующие заданным нами параметрам, собирает полученную информацию, с которой производится первоначальная систематизация. Для написания парсера может применяться практически любой язык программирования, например PHP, C++, R или Python.

Независимо от выбора языка программирования, принцип действия парсера остается схож. Происходит формирование запросов в виде кода к XHTML-документам (страницы сайта) или их отдельным элементам. Далее парсер из-

влекает необходимую нам информацию, указанную в коде-запросе (картинки, заголовки, текст) и сохраняет ее. Сохранение происходит в первичное неструктурированное хранилище в виде таблицы. Оно состоит из ссылки на патент, его номера, формата (png, jpg, txt) и основных меток, позволяющие узнать краткое содержание патента.

Следующей основной подзадачей является распознавание загруженных патентов. Происходит обработка изображения в несколько этапов: загрузка изображения, предварительная фильтрация, бинаризация и векторизация. Основная задача предварительной фильтрации – улучшить качество изображение: убрать шумы и восстановить контрастность без потерь в детализации. Бинаризация – получение черно-белого изображения, где черный цвет отвечает наличию «краски», а белый – ее отсутствию. Процесс бинаризации производится для правильной работы ряда алгоритмов, которые не работают с распознаванием полутонов. Само же распознавание патента происходит при помощи нейронной сети с использованием однослойной сети Кохонена. Принцип работы нейронной сети таков, что, получив на входной слой нейронов новое изображение, сеть реагирует импульсом того или иного нейрона. Так как все нейроны поименованы значениями букв, следовательно, среагировавший нейрон несет ответ распознавания. Для правильной настройки нейронной сети ей необходимо пройти обучение. Модуль обучения берет изображение патента из обучающей выборки и направляет его сети. Сеть анализирует все позиции черных пикселей и выравнивает коэффициенты входов, минимизируя ошибку совпадения. Каждому нейрону сопоставляется свое изображение символа. Последним шагом на этапе распознавания является структуризация. Происходит финальная обработка и последующее получение корректных графов и меток.

Последней основной подзадачей в теме парсинга является задача структурирования. После извлечения текста из различных форматов патентов и получения необходимого процентного содержания химических элементов у сплавов, следует структурировать полученную информацию для возможных после-

дующих взаимодействий с ними. После структуризации, мы получаем базу данных с патентами, разбитыми на несколько параметров. Благодаря созданию базы данных, нам открывается возможность производить различные действия для решения задачи разработки новых материалов.

СПИСОК ЛИТЕРАТУРЫ

1. Абрамова Т. А. Разработка парсинг-системы для получения скрытых ссылок со страниц социальных сетей / Т. А. Абрамова // Вестник Пензенского государственного университета. – 2016. - №3(15). – с. 41 – 47.
2. Тюрланд М. Веб-парсинг на PHP, вторая редакция, 4627 University Dr Fairfax, VA 22030 USA, musketeers.me, LLC. 2019, 22 с.

УДК 004.9

А. И. ВАХИТОВА
vahitova98@bk.ru
Науч. руководов. – ст. преп. М. С. ДЕМЧЕНКО

Уфимский государственный авиационный технический университет

ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИЙ «ИНДУСТРИИ 4.0» В ПРОВЕДЕНИИ ПРОФОРИЕНТАЦИИ ШКОЛЬНИКОВ

***Аннотация*.** Статья посвящена проблеме проведении профориентации школьников. Рассматриваются ключевые компоненты цифровой трансформации промышленного производства в контексте Индустрии 4.0 и как они могут помочь будущим выпускникам с определением будущей профессии. В частности, рассматриваются технологии, используемые в рекламе, как возможность узнать увлечения пользователя системы для составления общей картины интересов. Также доказывается мысль об необходимости использования новейших технологий обзором принадлежности школьников к поколению зумеров.
***Ключевые слова*:** профориентация; школьник; индустрия 4.0; теория поколений; цифровые технологии; тестирование.

Проведение профориентации с получением эффективного результата задача не из легких. При использовании обычных тестов можно получить определенные выводы, но не будет полной картины. Как дополнение необходимо также проведение беседы с психологом. Но в таком случае возникает проблема в нехватке специалистов для каждого пользователя, так как программа должна быть рассчитана как минимум для всех выпускников региона. В данном случае необходимо использовать что-то, что позволит помочь каждому, например современные информационные технологии.

Основным материалом исследования будет та часть общества для кого необходима система профориентационных работ – будущие абитуриенты ВУЗов и ССУЗов. Для понимания как она должна быть построена необходимо изучить характерные особенности данной группы. В данную категорию попадают люди, родившиеся в 2004 и в последующие годы. Исходя из адаптированной для России американской теории поколений, можно сделать вывод, что мы имеем дело с поколением Z (рожденные 2000–2011 гг.) и всем известный факт, что такие дети «рождаются со смартфоном в руках».

Необходимо выделить важные особенности для этого поколения:

- для них не существует шаблонов и ограничений, принципов и устойчивых взглядов

- некоторые из них уже пытались открыть свой бизнес.

- в воспитании принимают участие не только родители, но, и различные блогеры из YouTube, Tik Tok, Instagram

- привычного для прошлого поколения детства с друзьями во дворе, у них нет.

Для поколения Z уже с самого рождения общение с компьютером происходит «на ты». Имена Маруся, Алиса, Олег они ассоциируют не с какими-то конкретными людьми (приятелями, друзьями), а с более знакомыми для них роботами-помощниками. А ведь такой инструмент как голосовой помощник может помочь решить некоторые вопросы, связанные с проблемой проведения тестирования среди будущих абитуриентов.

Человечество живет во время бурного развития информационных и коммуникационных технологий, вследствие чего часто сталкивается с изменениями и в обычной жизни. Все эти изменение связанные с широким распространением всемирной сети Интернет вызванные четвертой промышленной революцией. Индустрия 4.0, начавшая во второй половине двадцатого века, вызвала новые явления и процессы – цифровизацию и цифровую экономику, что находит отражение в изменении промышленности.

В Индустрии 4.0 основными направлениями выделяют:

– Аддитивное производство;

– Большие данные, облачные вычисления;

– Виртуальная реальность;

– Искусственный интеллект.

Последний пункт особенно выделяют как одно из самых перспективных направлений цифровых технологий

Революция не обошла стороной и сферу образования. Во многих школах привычные для всех бумажные дневники уже потеряли свою актуальность, так как идет переход на электронные. Также никого не удивишь тестирующими программами. Большое влияние цифровых технологий на процесс обучения весь мир прочувствовал, столкнувшись с пандемией в 2020 году. Как ученикам младших классов, так и преподавателям с высоким стажем работы выпал шанс опробовать возможности компьютерных технологий. Даже после того, как все постепенно вернулись на учебу в офлайн режиме, задания для проверки знаний, которые проверяет компьютер, не потеряли своей актуальности.

Возникает вопрос: необходим ли искусственный интеллект для проведения профориентации школьников. Ведь, казалось бы, в таком нелегком вопросе как выбор будущей профессии, вряд ли может помочь бездушный робот.

Такое явление, как реклама в Интернете, появилось не так давно, но при этом используемые технологии имеют высокий темп в усовершенствовании. Многие пользователи сети замечают, что получают рекламу того, в чем заинтересованы. Происходит ощущение, что кто-то подслушивает за человеком и специально высылает то, что ему надо. Если этот феномен рассматривать простым взглядом, то да – за нами следят, но происходит это намного сложнее. Здесь используется инструмент ремаркетинга. Из справочного раздела Google можно узнать, что он способствует в воспроизведении нужной рекламы тем, кто уже посещал сайт или пользовался приложением. Пользователи могут получить рекламное объявление при просмотре иных сайтов, или по запросам схожих товаров.

Дело в том, что мы оставляем «цифровой след». «Цифровой след» – это совокупность информации, размещаемой пользователем о себе в сети Интернет. Т. е. когда люди оставляют комментарии под фотографиями звезд, делают заказ в интернет-магазинах, заводят страницу в социальной сети, указывая персональные данные (имя, фамилия, дата рождения, номер телефона, место работы и т. д.), то не задумываясь вносят в интернет крупицы информации. Но если

это как-то можно контролировать, например, уменьшить активность во всемирной сети, то феномен «цифровая тень» обыграть не получится. «Цифровая тень» – информация, которая накапливается неявно: маршруты передвижений, видеозаписи камер наблюдений и т. д. Сбор информации продолжается и тогда, когда мы не взаимодействуем с телефоном. Наш гаджет сам подключается к роутерам заведений и организаций, встречающихся на пути.

Такие технологии нас пугают. Но в современном мире мы имеем один выход – успокоиться и свыкнуться с мыслью, что это норма для жизни в цифровой эпохе.

Для чего нужен сбор информации? Ответ прост: для того, чтобы угодить покупателям. Ведь главная задача рекламы – помочь в выборе. Каждый сайт, который мы посещаем, создает небольшие текстовые документы, в которых записываются наши действия. Эти документы называются cookies. Затем все это собирается на веб-сервер. Алгоритмы машинного обучения анализируют собранные материалы и выдает рекламу, которая вероятнее всего заинтересует пользователя.

Почему бы данную способность роботов не использовать и для проведения профориентации? С помощью cookie-файлов можно собрать информацию о школьнике в течение определенного времени. Затем также с помощью машинного алгоритма выявить его интересы и предпочтения.

Плюсами такой системы будут следующие:

– при прохождении теста школьник может задуматься и дать ошибочный ответ, но в случае, когда используется подобная система, вероятность ошибки уменьшается;

– система рассчитана на большое количество пользователей;

– система имеет меньше затрат для результата;

– система использует больше информации.

Но в такой системе есть и минусы:

– как и в случае с рекламой, может произойти утечка информации из-за злоумышленников;

– есть вероятность использования интересов не только тестируемого, но и членов семьи или того, кто также пользуется роутером;

– для анализа нужна выборка, собранная за большое количество времени.

Как же тогда будет работать система? Школьники будут как можно раньше получать свой личный кабинет. Далее система будет собирать cookie-файлы. Также пользователь системы должен будет проходить несколько видов тестирования на профориентацию. После сбора всей информации система начнет подбирать специальности. Вдобавок в некоторых случаях будет использоваться помощь экспертов. Как результата ученики школ получат специальный набор, который включает: профессии, которые наиболее подходят; учебные заведения, в которых можно получить необходимое образование; список предметов, которые изучается в определенном учебном заведении; список дополнительных курсов; олимпиады. Хорошим дополнением будет ролик от каждого предложенного учебного заведения, в котором будет рассказываться об направлении подготовки от трех лиц: преподавателя, студента, выпускника. Это все необходимо для того, чтобы будущий абитуриент мог наглядно представить результаты теста. Все это будет находиться на портале электронного образования Республики Башкортостан (Рис. 1).

Рис. 1. Модель системы профориентации

Предлагаемая модель имеет множество преимуществ. Но так ли она хороша в использовании? Если попытаться систематизировать все действия, то

можно обойтись без использования информационных систем, сам школьник может без тестов и помощи от взрослых выбрать нужную специальность. В таком случае не стоит забывать, что существует множество направлений и даже в рамках Уфимских университетов специальности с одинаковыми названиями имеют разные учебные планы. Так, не имеющий полного представления абитуриент может запутаться и выбрать неверный путь. Система же поможет и подберет именно нужный ВУЗ (ССУЗ), кроме того предложит ту специальность, которая не была рассмотрена из-за непонятного наименования.

Таким образом в ходе исследования была построена модель проведения профориентации, которая включает в себя привычные виды анкетирования и тестирования. Вдобавок была рассмотрена технология, используемая в рекламах, которая поможет дополнить общую картину внутреннего мира выпускника, от чего выбор профессионального пути будет наиболее точной. Следовательно, появиться специалист, который ценит свою работу. В свою очередь если он окончил учебное заведение на бюджетном месте, то государственное финансирование получит положительный результат.

СПИСОК ЛИТЕРАТУРЫ

1. Бояркина Л.А. Бояркин В.В. Цифровой след и цифровая тень как производные персональных данных [Электронный ресурс] // Сборники конференций ниц социосфера. 2016. № 62.
2. Дугар-Жабон Т. З., Симакина М. А. Таргетинг и ретаргетинг как инструменты маркетинга // Научные труды Московского гуманитарного университета. 2019. № 4.
3. Зверева Екатерина Анатольевна Особенности медиапотребления "поколения Y" и "поколения Z" // Социально-гуманитарные знания. 2018. №8.
4. Московченко В.М., Столяров Д.О., Горбунов А.А., Белянин В.И. Анализ технологий защиты от идентификации веб-браузеров // NBI-technologies. 2018. №1.
5. Шишкунова В.А. Теория поколения: понятие и характеристика // Актуальные проблемы авиации и космонавтики. 2017. №13.

УДК 004.89

К. Р. ГАЛЛЯМУТДИНОВА, Д. А. КИСТАНОВА
s_kamill@mail.ru, d.kistanova@mail.ru
Науч. руководов. – канд. техн. наук, доц. Е. Ю. САЗОНОВА

Уфимский государственный авиационный технический университет

ЗАДАЧА СЕГМЕНТИРОВАНИЯ ПРЕДЛОЖЕНИЙ РЫНКА ТУРИСТИЧЕСКИХ УСЛУГ НА ОСНОВЕ ИНТЕЛЛЕКТУАЛЬНЫХ ТЕХНОЛОГИЙ

Аннотация. В статье рассматриваются вопросы сегментационного исследования с целью изучения объектов и их последующей кластеризации на примере предложений рынка туристических услуг. Сегментация объектов на основе их значимых характеристик, с одной стороны, позволяет сузить поиск решений, с другой стороны, при интерпретации результатов сегментации формализовать рекомендации.
***Ключевые слова*:** задача кластеризации; методы кластеризации; методы сбора информации; самоорганизующиеся карты Кохонена; алгоритм ClOPE; алгоритм MST.

Введение

В настоящее время одной из популярных обсуждаемых тем является тема закрытых границ. Пандемия COVID-19 показала, как сильно закрытие границ может повлиять на экономику стран, в том числе, на туристическую отрасль. По оценкам ЮНВТО, в январе – августе 2020 г. число международных туристических прибытий в мире сократилось на 700 млн., что составляет 70 % от общего рынка. На рисунке 1 приведены изменения динамики туристического движения в различных странах.

	январь	февраль	март	апрель	май	июнь	июль	август	янв.–авг. 2020 г.
Америка	0	3	–50	–94	–93	–92	–88	–88	–65
Европа	5	2	–61	–98	–96	–88	–72	–69	–68
Ближний Восток	6	–1	–63	–99	–99	–99	–96	–94	–69
Африка	2	1	–43	–99	–99	–99	–96	–94	–69
АТР	–9	–54	–82	–98	–99	–98	–96	–96	–79
Мир	**–1**	**–16**	**–65**	**–97**	**–97**	**–91**	**–81**	**–79**	**–70**

Рис. 1. Динамика международных прибытий по географическим регионам в годовом выражении, в %

В России сокращение количества туров за границу привела к тому, что многие туроператоры создали новые направления внутри России. Однако, нужно отметить, что за 10 месяцев 2020 года внутренний туризм подорожал для населения России в среднем на 1.7% в годовом выражении. Таким образом, можно утверждать, что рынок предложений внутреннего туризма находится в постоянном развитии, в связи с чем, актуальными проблемами являются вопросы выявления новых закономерностей, цифровизации и развитии технологий, которые при подготовки эффективных мер помогут оптимизировать процессы, происходящие на рынке туристических предложений.

Планирование тура является трудоемким процессом, так как необходимо предусмотреть множество факторов: сезон, актуальность направления, транспорт, питание, перелет, проживание и другие не менее важные факторы. Также, как и в других индустриях, в сфере туризма цены формируются по некоторым признакам, которые влияют на скорость реализации предложений. Множество исследования проводится для выявления основных признаков, влияющих на цены туров, оценки рыночной активности, выявления сегментов покупателей.

В статье авторами проводиться анализ рынка предложений туристических услуг с учетом факторов, которые влияют на ценообразование объектов. Для анализа рынка туристических услуг необходимо получить реальные данные о туристических предложениях в проверенном источнике, сохранить результат сбора информации в удобном виде для чтения, провести предобработку каждой выборки, выделить основные значащие характеристики, разбить полученную информацию с помощью наилучшего из рассматриваемых алгоритма кластеризации и вывести результаты исследования в удобном для пользователя формате.

Постановка задачи сегментирования предложений рынка туристических услуг

Требуется собрать следующую информацию о турах: туроператор, отправная точка, информация об отеле (количество звезд, рейтинг, услуги и удоб-

ства в отеле, расстояние до аэропорта), тип питания, город проживания, цена, количество ночей и др. Для сбора информации предлагается написать скрипт для извлечения данных из веб-страницы в структурированном виде. После сбора данных необходимо разработать математическое и программное обеспечение для задачи анализы рынка предложений туристических услуг. Под анализом рынка понимается сегментация туров на группы, при этом объединяются в группы схожие объекты. Задача сегментации туров сводится к задаче кластеризации объектов.

Подход к решению задачи сегментирования предложений рынка туристических услуг

Структура решения задачи отображена в виде контекстной диаграммы методологии IDEF0 (рис. 2). Входными данными являются: URL-страница – это адрес (ссылка), указывающий точное местоположение веб-ресурса в интернете, в данном случае: сайта Слетать.ру, требования к туру, например город отдыха, тип отеля, удобства в номерах, данная информация вводится пользователем. Выходными данными являются: графическое отображении сегментации туров, рекомендации для пользователя.

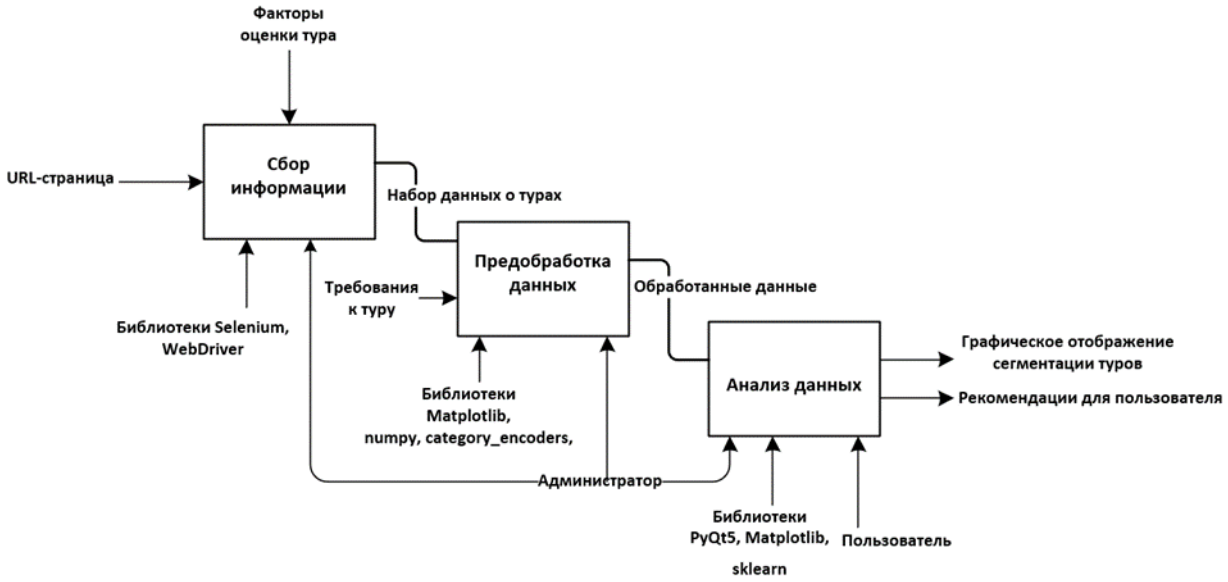


Рис. 2. Структура решения задачи анализа предложений рынка туристических услуг

Для получения данных был использован гибридный метод сбора информация, а именно был разработан парсер. Для разработки были использованы следующие технологии: язык разработки – Python, среда разработки - Python 3.8 IDE PyCharm, библиотеки - selenium и webdriver_manager.

После того, как сбор данных осуществлен необходимо осуществить анализ данных, который состоит из 3 этапов: предобработка данных, обработка данных, в данном случае кластеризация данных, интерпретация результатов. В таблице 1 представлены изменения характеристик набора данных до и после этапа предобработки. На этапе обработки данных авторами были реализованы следующие методы: самоорганизующаяся карта Кохонена, алгоритмы CLOPE и MST. Набор данных был разделен на 10 выборок, в зависимости от города вылета. С помощью меры Силуэт в каждой выборке был использован свой метод кластеризации.

Таблица 1

Результаты предобработки данных

Этап	*Инструменты и методы*	*Данные до*	*Данные после*
Очистка данных	RapidMiner Excel RStudio	• 33 атрибута • 669136 объектов	• 17 атрибутов • 53046 объектов
Нормализация	Python		•
Преобразование типов значений	Python Метод OneHotEncoder	• 12 атрибутов с категориальными значениями • 5 атрибутов с числовыми значениями	• 17 атрибутов с числовыми значениями
Корреляция	Python	17 атрибутов	• 17 атрибутов

Этап интерпретации данных позволила разработать рекомендательную систему для туристических агентов.

Вычислительный эксперимент и анализ результатов

Для выполнения эксперимента использовался ЭВМ со следующими характеристиками: ОС Windows 10 x64; процессор AMD A6; 4 ГБ ОЗУ 9-220.

Целью эксперимента является выявление лучшего алгоритма кластеризации для каждой выборки. Для оценки качества структуры кластеров была использована мера Силуэт. Значение силуэта показывает, насколько объект похож на свой кластер по сравнению с другими кластерами. Сначала силуэт определяется отдельно для каждого объекта, затем считается оценка для всей кластерной структуры.

$$Sil(\mathrm{C}) = \frac{1}{N} \sum_{c_k \in C} \sum_{x_i \in c_k} \frac{b(x_i, c_k) - a(x_i, c_k)}{max\{a(x_i, c_k), b(x_i, c_k)\}}$$

Среднее расстояние от данного объекта до объектов из того же кластера:

$$a(x_i, c_k) = \frac{1}{|c_k|} \sum_{x_j \in c_k} \|x_i - x_j\|$$

Среднее расстояние от данного объекта до объектов из ближайшего кластера:

$$b(x_i, c_k) = min_{c_l \in C \setminus c_k} \{ \frac{1}{|c_l|} \sum_{x_j \in c_l} \|x_i - x_j\| \}$$

Данная величина лежит в диапазоне [-1,1]. Значения, близкие к -1, соответствуют варианту кластеризации с высокой дисперсией, значения, близкие к нулю, говорят о том, что кластеры пересекаются и накладываются друг на друга, значения, близкие к 1, соответствуют "плотным" четко выделенным кластерам. Таким образом, чем больше силуэт, тем более четко выделены кластеры. В таблице 2 приведен фрагментов результата эксперимента.

Таблица 2

Фрагмент результата вычислительного эксперимента

	SOM	MST	CLOPE
Москва	0,77	**0,83**	0,74
Уфа	**0,86**	0,77	0,75
Санкт-Петербург	0,77	**0,81**	0,73
…	…	…	..
Екатеринбург	**0,79**	0,76	0,75
Нижний Новгород	**0,88**	0,84	0,81

В результате оценки качества структуры кластеров алгоритм сетей Кохонена оказался более эффективен для выборок: Уфа, Хабаровск, Краснодар, Ека-

теринбург, Нижний Новгород, алгоритм MST – для выборок: Москва, Санкт-Петербург, Новосибирск, Казань, алгоритм CLOPE – для выборки Ростов. Таким образом, можно сделать вывод, что предложенные алгоритмы для кластеризации туристических предложений довольны эффективны.

Заключение

Авторами статьи приведена содержательная постановка задачи сегментирования предложений рынка туристических услуг. Разработана методика к анализу предложений рынка туристических услуг, которая включает этап сбора данных с помощью парсинга и этап сегментирования данных на основе кластерного анализа. Разработано математическое обеспечение для анализа предложений рынка туристических услуг. В качестве методов кластеризации были выбраны самоорганизующаяся карта Кохонена, алгоритмы CLOPE и MST. Для оценки качества метода выбрана мера Силуэт.

Результаты исследования, приведенные в статье, получены в рамках выполнения грантов РФФИ 19-07-00709 и государственного задания No FEUE-2020-0007.

СПИСОК ЛИТЕРАТУРЫ

1. Нейский И.М. Классификация и сравнение методов кластеризации [Электронный ресурс] // Интеллектуальные технологии и системы. Сборник учебно-методических работ и статей аспирантов и студентов. – М.: НОК «CLAIM», 2006. – Выпуск 8. – С. 130-142. URL: http://it-claim.ru/Persons/Neyskiy/Article2
2. Самоорганизующаяся карта Кохонена [Электронный ресурс] // Википедия: Электронная свободная энциклопедия. - URL: https://ru.wikipedia.org/wiki/Карта_Кохонена
3. Анализ рынка туристских услуг [Электронный ресурс] // Сайт учебных материалов – URL:https://works.doklad.ru/view/yeIjTzUxK18.html
4. Фридман А. Рынок туризма как объект маркетингового исследования [Электронный ресурс] // Фридман А. - URL: http://aleksandrfridman.ru/tourbusiness/tourmarketing/tourism_as_market_research_object.html
5. Юсупова Н. И., Сметанина О. Н., Ионис А. Г., Сазонова Е. Ю. Технологии Data Mining для оценки регионального уровня развития отрасли информационно-коммуникационных технологий. Научный журнал "Современные наукоемкие технологии ". М.: Издательский Дом «Академия Естествознания», 2019. – Т. 8. –С.36-42. – 1357 KB. – URL: https://top-technologies.ru/pdf/2019/8/37627.pdf (дата обращения: 09.09.2021).
6. Юсупова Н. И. Технологии искусственного интеллекта и машинного обучения в задачах семантического представления и анализа данных: монография // Н. И. Юсупова, О.Н. Сметанина, М. М. Гаянова и др. – М.: "Издательство "Инновационное машиностроение", 2020. – 242 с.

УДК 519.86; 692.522.2; 693.554.32

В. И. ЗИНОВ
ufaaaaaaaa@gmail.com
Науч. руководв. – канд. техн. наук, доц. Ю. И. ВАЛИАХМЕТОВА

Уфимский государственный авиационный технический университет

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ЗАДАЧИ РАЗМЕЩЕНИЯ АРМАТУРНЫХ СТЕРЖНЕЙ В ФОНОВОМ АРМИРОВАНИИ ПЛИТЫ ПЕРЕКРЫТИЯ ПРИ ПРОЕКТИРОВАНИИ ЗДАНИЯ

Аннотация. В статье рассматривается проблема размещения арматурных стержней в основном армировании плиты перекрытия регулярным шагом. Проведен обзор проблемы, построена математическая постановка задачи, учитывающая необходимость раскроя арматуры и нормативные ограничения.
***Ключевые слова*:** математическая модель; задача раскроя и размещения; автоматизация процесса армирования; армирование плит перекрытия.

1. Введение

Процесс возведения здания включает в себя не только непосредственное строительство здания, но и этап его проектирования. Именно на этапе проектирования оптимизация имеет наибольший экономический эффект: использование математических методов для решения практических задач до стройки является одним из определяющих подходов в последующей экономии времени и стройматериалов.

Фоновое армирование плиты перекрытия представляет собой сетку арматурных стержней, раскладываемых вдоль каждой стороны плиты перекрытия с некоторым постоянным шагом. Фоновое армирование - это армирование воспринимающее, основные эксплуатационные (средние) и возможные случайные воздействия и нагрузки на плиту перекрытия. Однако, при строительстве высотных зданий с большой площадью плит перекрытия, возникает ситуация, при которой исходной длины арматурных стержней не хватает для покрытия всей стороны перекрытия. Поэтому одна линия сетки формируется не одним арматурным отрезком, а несколькими, состыкованными по длине друг с другом. Выбор длин арматурных отрезков и размещение этих отрезков в сетке для каждого такого набора является важной практической задачей в проектировании и

строительстве здания на этапе армирования перекрытий, которая сильно влияет на смежные и последующие задачи и этапы.

2. Описание проблемы

Имеется перекрытие, которое необходимо покрыть фоновой арматурой. Будем рассматривать простую формулировку задачи, в которой перекрытие представляет собой прямоугольник. Кроме того, определен некоторый регулярный шаг фонового армирования, с которым арматурные стержни кладутся вдоль стороны перекрытия. При этом предполагается, что исходные арматурные стержни меньше, чем любая из сторон плиты перекрытия. Поэтому арматура может класться в одну линию внахлест, длина стыков константна.

Важно учитывать, что арматурные отрезки получаются из исходных стержней некоторой константной длины путем раскроя последних, а значит следует выбирать размеры арматурных отрезков таким образом, чтобы минимизировать раскройные остатки.

Условия, предъявляемые задачей:

– Стыки, создаваемые соседней арматурой, должны отстоять друг от друга вдоль одной параллели по крайней мере на половину длины стыка;

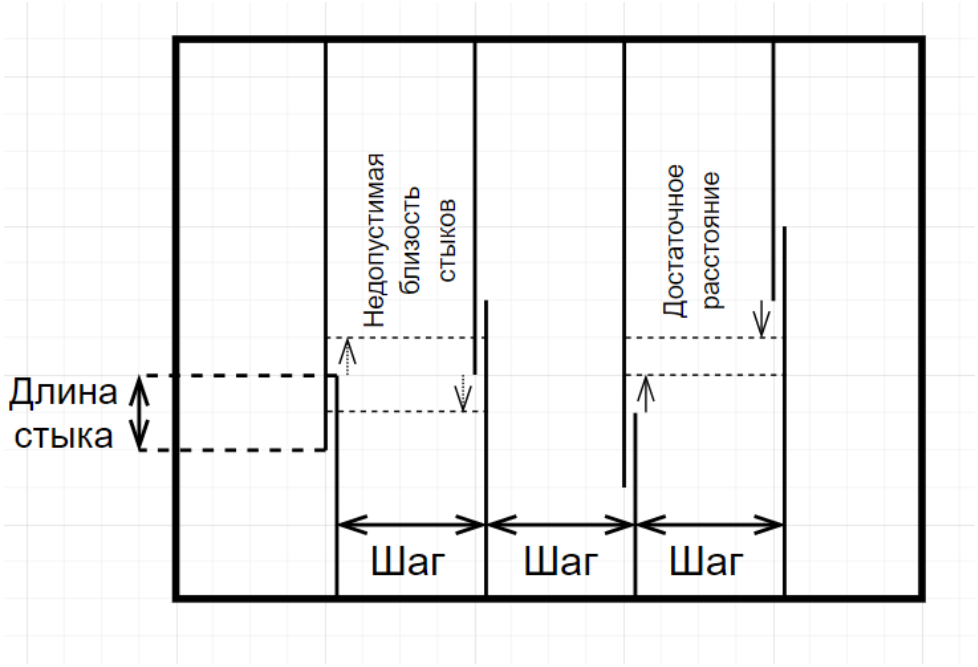


Рис. 1. Пример возможных взаиморасположений двух стыков соседствующих наборов

– Армирование кладется вдоль обеих сторон плиты перекрытия.

Необходимо составить карты размещения арматурных стержней таким образом, чтобы покрыть плиту перекрытия с учетом установленных условий, при минимизации суммарной длины неиспользуемых остатков от раскроя выбранных арматурных стержней.

3. Математическая постановка задачи

Пусть имеется прямоугольное перекрытие $P =< H, W >$, где H, W – линейные размеры перекрытия.

Обозначим за ζ константное значение длины исходных арматурных стержней (чаще всего = 11700 мм).

Обозначим за ω константное значение шага размещения арматуры по стороне перекрытия. Примем этот шаг как вдоль стороны H, так и вдоль стороны W. Тогда, количество линий, по которым размещается арматура вдоль сторон, определим как $q^H = \left\lfloor \frac{H}{\omega} \right\rfloor$ вдоль стороны H и $q^W = \left\lfloor \frac{W}{\omega} \right\rfloor$ вдоль стороны W.

Далее индексы отношения к конкретной стороне плиты перекрытия будут опущены с целью избежания нагромождения формул.

Определим карты размещения как $y_k = \{b_{1k}, b_{2k} \dots b_{\mu k}\}$ – набор арматурных отрезков, размещаемых на одной линии, где b_{jk} – количество арматурных отрезков типоразмера j в карте k. Каждой карте ставится в соответствие значение υ_k – количество линий вдоль стороны, в которых был использован набор арматурных отрезков -ой карты.

Типоразмеры определяются по значению длины арматурного отрезка w_j, $j = 1..\mu$, где μ – количество типоразмеров.

Совокупность примененных карт размещения назовем множеством размещения арматуры $Y = \{y_1, y_2 \dots y_\sigma\}$, где σ – количество составленных карт размещения.

Порядок следования в карте не определяется, но учитывается необходимость стыковки арматурных отрезков внахлест и длина стыков. Длину стыка обозначим за ρ.

За последовательность расстановок обозначим $\bar{Y} = (\overline{y_s^{(k)}})_{s=1}^{\sum_{k=1}^{\sigma} \upsilon_k}$, где $\overline{y_s^{(k)}} = (w_{jm})_{m=1}^{\sum_{j=1}^{\mu} b_{jk}}$ – некоторая расстановка арматурных отрезков карты размещения k, поставленная по стороне перекрытия на шаге s; w_{jm} – длина арматурного отрезка типоразмера j, стоящего на позиции m в расстановке. При этом:

- $\forall \bar{k} = 1..\sigma: \left|\overline{y_{s=1..\sum_{k=1}^{\sigma} \upsilon_k}^{(\bar{k})}}\right| = \upsilon_{\bar{k}}$, т.е. количество расстановок карты размещения $\bar{k}$ в последовательности расстановок $\bar{Y}$ должно быть равно количеству линий, по которым размещается арматура из карты $\bar{k}$;
- $\forall \bar{\jmath} = 1..\mu: \left|\bar{\jmath}_{m=1..\sum_{j=1}^{\mu} b_{jk}}\right| = b_{\bar{\jmath}k}$, т.е. количество арматурных отрезков типоразмера $\bar{\jmath}$ в любой расстановке $\overline{y_s^{(k)}}$ должно быть равно количеству отрезков этого типоразмера, заявленных в соответствующей карте размещения y_k.

Необходимо найти последовательность расстановок карт размещения таким образом, чтобы:

$$\left\lfloor \frac{\sum_{i=1}^{n} w_j}{\zeta} \right\rfloor \to min;$$

При условиях:

- $\sum_{k=1}^{\sigma^H} \upsilon_k^H = q^H$; $\sum_{k=1}^{\sigma^W} \upsilon_k^W = q^W$ – количество расстановок по стороне должно быть равно количеству шагов вдоль соответствующей стороны;
- $\sum_{j=1}^{\mu}(b_{jk}^H \cdot (w_j - \rho)) + \rho = W$; $\sum_{j=1}^{\mu}(b_{jk}^W \cdot (w_j - \rho)) + \rho = H$ – совокупная длина отрезков в карте размещения по стороне за вычетом длин стыков должна быть равна длине перпендикулярно лежащей стороны;
- Выполним следующий алгоритм для обеих сторон плиты перекрытия: $\forall s_1, s_2 \in [1, 2..\sum_{k=1}^{\sigma} \upsilon_k],\ s_1 \neq s_2$:

1. Составим множества интервалов стыков I_{s_1} и I_{s_2} следующим образом: $I_{\tilde{s}} = \{[\underline{I_{\tilde{s}}}^m, \overline{I_{\tilde{s}}}^m]\}$, где $\underline{I_{\tilde{s}}}^m = \underline{I_{\tilde{s}}}^{m-1} + w_{jm} - \rho$, $\underline{I_{\tilde{s}}}^0 = 0$ – нижние концы ин-

тервалов стыков; $\overline{I_{\tilde{s}}}^{m} = \underline{I_{\tilde{s}}}^{m-1} + w_{jm}$ – верхние концы интервалов стыков; $m = 1..(\sum_{j=1}^{\mu} b_{jk} - 1)$; при этом $(w_{jm})_{m=1}^{\sum_{j=1}^{\mu} b_{jk}} = \overline{y_{\tilde{s}}^{(k)}}$; $\tilde{s} = \{s_1, s_2\}$.

2. Трансформируем множества интервалов стыков в множества области недопустимой параллельности стыков I'_{s_1} и I'_{s_2} следующим образом: $I'_{\tilde{s}} = \{[\underline{I'_{\tilde{s}}}^{m}, \overline{I'_{\tilde{s}}}^{m}]\}$, где $\underline{I'_{\tilde{s}}}^{m} = \underline{I_{\tilde{s}}}^{m} - \frac{\rho}{2}$ – нижние концы интервалов зон; $\overline{I'_{\tilde{s}}}^{m} = \overline{I_{\tilde{s}}}^{m} - \frac{\rho}{2}$ – верхние концы интервалов зон; $m = 1..(\sum_{j=1}^{\mu} b_{jk} - 1)$; $\tilde{s} = \{s_1, s_2\}$.

3. Если условие $I_{s_1} \cap I'_{s_2} \vee I'_{s_1} \cap I_{s_2}$ выполняется, то стыки расстановок s_1 и s_2 лежат в недопустимой параллельности относительно друг друга.

4. Заключение

В работе была проанализирована проблема размещения арматурных стержней в плите перекрытия в качестве фонового армирования. Было составлено описание проблемы, была разработана математическая постановка задачи. Результаты работы могут быть использованы для последующего анализа задач армирования перекрытий: кроме фонового армирования, необходим анализ проблем усиления зон дополнительной нагрузки, торцов плиты, обрамления отверстий, учета каркасных арматурных стержней. Комплексное решение всех перечисленных проблем в сопряжении с задачей раскроя всех задействованных арматурных отрезков позволит в полной мере реализовать оптимизационные методы и сильно сократить нынешние затраты на армирование плит перекрытий в многоэтажных зданиях.

СПИСОК ЛИТЕРАТУРЫ

1. Струченков В.И. Прикладные задачи оптимизации : модели, методы, алгоритмы / Струченков В.И.. — Москва : СОЛОН-ПРЕСС, 2016. — 314 с. — ISBN 978-5-91359-191-3. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/53841.html (дата обращения: 14.09.2021). — Режим доступа: для авторизир. пользователей

2. СП 63.13330.2018. Бетонные и железобетонные конструкции. Основные положения : актуализированная редакция СНиП 52-01-2013 : издание официальное : утвержден приказом Министерства строительства и жилищно-коммунального хозяйства Российской Федерации от 19 декабря 2018 г. № 832/пр : дата введения 2019-20-06 / разработан – АО «НИЦ «Строительство» – НИИЖБ им. А.А. Гвоздева». – Москва, 2018. – 143 с. — URL:

https://www.srosp.ru/upload/files/doc/SP-63_.pdf (дата обращения: 15.09.2019). – Текст : электронный.
3. Мухачева Э.А., Мухачева А.С. Л. В. Канторович и задачи раскроя-упаковки: новые подходы для решения комбинаторных задач линейного раскроя и прямоугольной упаковки. Записки научных семинаров Санкт-Петербургского отделения математического института им. В.А. Стеклова РАН. 2004. Т. 312. № 11. С. 239-255.

УДК 004.051

Л. Ю. ЗИЯЗЕТДИНОВА
ziyazetdinova.l2001@gmail.com
Науч. руководитель – д-р техн. наук, проф. Г. Р.ШАХМАМЕТОВА

Уфимский государственный авиационный технический университет

АНАЛИЗ СОСТОЯНИЯ ИССЛЕДОВАНИЙ В ОБЛАСТИ РАСПОЗНАВАНИЯ РЕНТГЕНОВСКИХ И КТ СНИМКОВ С ПОМОЩЬЮ МЕТОДОВ ГЛУБОКОГО МАШИННОГО ОБУЧЕНИЯ

Аннотация. В статье приводится описание терминологии проблемы распознавания рентгеновских и КТ снимков с помощью методов глубокого машинного обучения, исследована актуальность задачи, проведен анализ современного состояния проблемы в области распознавания рентгеновских и КТ снимков. Отмечены аспекты решаемой проблемы, выявленные при анализе, в виде решаемых задач, подходов, моделей и методов, используемых информационных технологий, инструментальных средств и программных решений проблемы.
Ключевые слова: машинное обучение; нейронные сети; распознавание образов; обработка медицинских изображений; искусственный интеллект.

Введение

Болезни органов дыхания на сегодняшний день являются одной из основных причин смертности населения [1] и диагностика заболеваний легких на ранних этапах была и остается очень значимой. В связи с этим возникает потребность в регулярном мониторинге состояния легких для предупреждения или обнаружения заболевания, прежде чем оно нанесет значительный вред здоровью человека.

Рентгенография, являясь наиболее распространенным и доступным средством обследования, имеет важное клиническое значение при постановке диагноза. Но несмотря на все преимущества данного метода, выявление признаков заболевания по снимкам является достаточно сложной задачей, требующей участия высококвалифицированных специалистов, а также значительных временных затрат. Сложность обуславливается неполнотой и неточностью исходной информации, а именно наличием различных видов искажений в снимках: засвеченное изображение, наличие посторонних предметов и др.

В связи с этим в последние годы наиболее востребованной и перспективой областью реализации и применения методов глубокого машинного обучения, является направление, связанное с разработкой интеллектуальных систем в медицине. И особенно активно развивается область обработки и анализа визуальных изображений. Анализ медицинских снимков, таких как компьютерная томография (КТ), магнитно-резонансная томография (МРТ), рентгенография грудной клетки, с помощью методов глубокого машинного обучения позволяет добиться более персонифицированного и эффективного подхода в диагностике и лечении легочных заболеваний. Также преимуществами использования методов машинного обучения при распознавании снимков являются значительное сокращение временных затрат и оптимизированная нагрузка на медицинских сотрудников. На текущий момент накоплено огромное количество биомедицинских данных, которые сами по себе бессмысленны, но обработка и анализ этих данных с помощью методов машинного обучения могут значительно трансформировать клиническую практику.

В данной работе проведен анализ существующих на сегодняшний день методов машинного обучения, используемых при распознавании КТ и рентгеновских снимков.

Анализ современного состояния проблемы

Проблема модификации существующих и создания новых методов машинного обучения в области анализа и распознавания медицинских снимков широко освещается в исследованиях, как наших ученых, так и ученых за рубежом.

К примеру, в статье [2] рассматривается проектирование архитектуры *нейронной сети* для распознавания визуальных признаков заболеваний органов дыхания на медицинских изображениях. В частности, алгоритм автоматически обнаруживает снижение прозрачности тканей легких на рентгенограммах грудной клетки.

Применение *нейронных сетей* для классификации рентгенографических изображений больных пневмонией и COVID -19, а также описание классификатора, разработанного на базе наиболее простой нейронной сети, без использования готовых моделей других разработчиков и без предварительного обучения на сторонних данных, на основе только небольшого набора изображений представлено в работе [3]. Также искусственный интеллект на основе нейронных сетей различного типа используют для анализа цифровых диагностических изображений в области рентгенологии и радиологии [4].

Для того, чтобы классифицировать паталогические образования в интеллектуальных системах *автоматизированной обработки рентгеновских снимков* грудной клетки, Томакова Р.А. и др. [5] использовали метод многооконного спектрального преобразования.

В статье [6] рассмотрен опыт создания и внедрения информационной системы на базе искусственного интеллекта «Botkin.AI» для выявления узлов и очагов в легких по данным КТ. Описаны основные параметры математических моделей, разработанных для системы, представлены результаты пилотных проектов ее практического применения в нескольких регионах Российской Федерации. Приведены примеры ее применения для выявления узлов в легких различных размеров и локализации.

Поэтапное создание сверточной нейронной сети для распознавания рака на медицинских снимках, а точнее на КТ грудной клетки рассмотрено в работе [7].

Хамад Ю.А. и Симонов К.В. [8] разработали программу для ЭВМ «Программа *для обработки и анализа изображений компьютерной томографии и рентгенографии грудной клетки*», предназначенную для сегментации области легких и распознавания патологии с целью повышения скорости и точности скрининга патологий и оценки состояния пациента.

Разработанный набор эвристических оценок, используемый для обнаружения кластеров, соответствующих легочным долям на изображениях компью-

терной томографии, при диагностике заболеваний легких, представлен в работе [9].

В научной статье [10] приведены результаты работы по сравнению двух программ компьютер-ассистированной диагностики, созданных на основе различных *типов искусственного интеллекта*, и визуальной оценкой врачами-рентгенологами поражений легких на основе снимков компьютерной томографии грудной клетки пациентов с COVID-19.

Разработанная в ходе работ [11] система автоматизированной диагностики, основанная на двухуровневой архитектуре искусственных нейронных сетей, была обучена, протестирована и оценена специально по проблеме обнаружения заболевания легких, обнаруженных на оцифрованных рентгенограммах грудной клетки.

Keserci B. и др. [12] разработали компьютерную схему диагностики для автоматического обнаружения узелков легкого в цифровых рентгеновских снимках грудной клетки на основе комбинации морфологических признаков и вейвлет – преобразования. В их схеме метод искусственных нейронных сетей использовался для эффективного уменьшения ложных срабатываний с использованием комбинированных функций.

В ходе написания статьи [14] авторы провели исследование алгоритмов предобработки изображений с целью повышения качества распознавания объектов на медицинских снимках. Выполнили сравнение алгоритмов предобработки изображений на основе совокупности показателей качества распознавания объектов на изображениях. Описали преимущества и недостатки исследованных алгоритмов, определили подходы, позволяющие оптимизировать задачу предобработки изображений для распознавания объектов на медицинских снимках.

Результаты анализа существующих методов распознавания медицинских изображений были представлены в публикации [15]. Кроме того, была предло-

жена модификация алгоритма Собеля, учитывающая особенности медицинских изображений.

Содержание статьи [17] составляет краткий обзор различных способов машинного обучения, основанных на нейросетевых технологиях применительно к решению задач классификации изображений, пригодные для выделения и характеристики типа патологии в легких на медицинских снимках. В частности, демонстрируется идея, лежащая в основе матрицы совпадений уровня серого и описание компонентного анализа (PCA) в качестве одного из методов извлечения и сокращения признаков.

Авторы публикации [18] приводят детальный обзор применения методов и моделей искусственного интеллекта в диагностике легочных заболеваний на основе медицинских изображений. Рассматривают этапы интеллектуальной обработки диагностических данных.

Новая система компьютерного обнаружения, основанная на контекстной кластеризации, целью которой является помощь радиологам в раннем выявлении рака легких по результатам снимков компьютерной томографии. Вместо использования традиционного подхода с пороговым значением, в этой работе [19] используется контекстная кластеризация, которая дает более точную сегментацию легких по объему грудной клетки. После сегментации извлекаются характеристики GLCM и LBP, которые затем классифицируются с помощью трех разных классификаторов Random forest, SVM и k-NN.

Использование подхода, основанного на многомасштабной обработке и искусственных нейронных сетях (ИНС), для проектирования системы обнаружения узелков в легких на рентгенограммах грудной клетки предложена в статье [20]. Аналогичную проблему решают авторы статьи [21] с помощью модели глубокого обучения, которая использует несколько сверточных сетей для определения входного изображения.

Таблица 1 иллюстрирует краткие результаты анализа современного состояния исследований.

Таблица 1

Анализ исследований в области применения методов машинного обучения для распознавания R и КТ снимков

№	Статья	Решаемая задача	Используемые методы/ подходы / программные средства
1	Кульневич А.Д.., Сергеева Н.Д., Чугунов Р.А. Система раннего детектирования пневмонии на основе методов глубокого обучения	Распознавание визуальных признаков заболеваний органов дыхания на медицинских снимках	Алгоритм детектирования снижения прозрачности легких; Предобучение на изображениях набора данных Common Objects in Context, подход Transfer Learning; Нейронная сеть Masc R - CNN
2	Ефремцев В.Г., Ефремцев Н.Г., Тетерин Е.П., Тетерин П.Е., Базавлук Е.С.. Классификация рентгеновских изображений грудной клетки больных вирусной пневмонией и COVID-19 с помощью нейронных сетей.	Классификация рентгенографических изображений больных пневмонией и COVID -19	Метод перекрестной проверки и решетчатого поиска; Сверточная нейронная сеть,Python 3.7., библиотека opencv 4.2.0., Tensorflow 2.1.0
3	Томакова Р.А., Филист С.А., Дураков И.В. Программное обеспечение автоматизированной классификации рентгенограмм грудной клетки на основе гибридных классификаторов	Автоматическая классификация изображений рентгенограмм	Метод анализа амплитудных спектров Фурье в скользящем окне, аппроксимация гистограмм яркости в окне анализа; Классификатор на основе нейронных сетей прямого распространения
4	Дрокин И.С., Еричева Е.В., Бухвалов О.Л., Пилюс П.С., Малыгина Т.С., Синицын В.Е.. Опыт разработки и внедрения системы поиска онкологических образований с помощью искусственного интеллекта на примере рентгеновской компьютерной томографии легких	Выявление узлов в легких по данным КТ	Алгоритм выделения легких на базе сверточных нейронных сетей, алгоритм детектирования узлов/очагов на базе трехмерных сверточных сетей; Облачная платформа Botkin.AI

Продолжение табл. 1

5	Андреев В.В., Минаев Н.Ю. Сверточная нейронная сеть для распознавания рака легких на медицинских снимках	Распознавание рака на снимках КТ	Алгоритм по водоразделу (Watershed); 3D сверточная нейроннаясеть U-Net
6	Хамад Ю.А., Симонов К.В. Программа для обработки и анализа изображений компьютерной томографии и рентгенографии грудной клетки	Обработка и анализ КТ изображений и рентгенографии грудной клетки с целью повышения скорости и точности скрининга патологий	Классификатор вероятностной нейронной сети ; MATLAB
7	Максимова Е.И., Хаустов П.А. Алгоритм обнаружения образований в легких человека на снимках компьютерного томографа с использованием искусственной нейронной сети.	Обнаружение образований на изображениях КТ	Метод получения вектора входных признаков искусственной нейронной сети;
8	Xu X. W. Et al. Development of an improved CAD scheme for automated detection of lung nodules in digital chest images.	Обнаружение заболевания легких на оцифрованных рентгенограммах грудной клетки	Метод искусственных нейронных сетей
9	Keserci B., Yoshida H. Computerized detection of pulmonary nodules in chest radiographs based on morphological features and wavelet snake model .	Автоматическое обнаружение узелков в легких на цифровых рентгенограммах грудной клетки	Метод ложноположительного сокращения, основанный на вейвлет - преобразованиях
10	Junji Shiraishi 1, Feng Li, Kunio Doi Computer-aided diagnosis for improved detection of lung nodules by use of posterior-anterior and lateral chest radiographs.	Автоматическое обнаружение узелков в легких на боковых рентгенограммах грудной клетки	Метод граничных градиентов
11	Шагалова П.А., Ерофеева А.Д.,Орлова М.М.,Чистякова Ю.С., Соколова Э.С. Исследование алгоритмов предобработки изображений для повышения эффективности распознавания медицинских снимков.	Предобработка изображений с целью повышения качества распознавания объектов на медицинских снимках	Методы бинаризации, а именно Ниблэка, Бернсена, Оцу. Зака

Окончание табл. 1

12	Хамад Ю.А., Симонов К.В. , Кенц А.С. Алгоритмы сегментации и распознавания объектов на медицинских изображениях на основе шиарлет-преобразования и нейронных сетей.	Сегментация и распознавание объектов на медицинских изображениях	Метод ложноположительного сокращения, основанный на шиарлет – преобразованиях
13	Симонов К.В. , Зотин А.Г., Хамад Ю.А., Курако М.А., Кенц А.С. Алгоритмы обнаружения и классификации визуальных данных.	Обнаружение и классификация визуальных данных на медицинских изображениях	Матрица совпадений уровня серого, компонентный анализ
14	Baboo S.S., Iyyapparaj E. A classification and analysis of pulmonary nodules in CT images using random forest.	Распознавание рака легких на КТ снимках	Подход контекстной классификации; Классификатор Random forest, SVM, k-NN
15	Coppini G. Et al. Neural networks for computer-aided diagnosis: detection of lung nodules in chest radiograms.	Распознавание рака легких на рентгеновских снимках	Метод анализа ROC/FROC
16	Kieu P. N. Et al. Applying multi-cnns model for detecting abnormal problem on chest x-ray images.	Обнаружение аномальных сигналов на рентгеновских снимках грудной клетки	Метод синтеза результатов компонентов модели – правила Fusion

Анализ исследований в области распознавания рентгеновских и КТ снимков с помощью методов глубокого машинного обучения позволил выявить основные аспекты современного состояния проблем, возникающих при распознавании медицинских снимков с помощью методов машинного обучения, в частности:

– классы решаемых задач: распознавание визуальных признаков заболеваний органов дыхания на медицинских снимках; обработка и анализ КТ изображений и рентгенографии грудной клетки; автоматическая классификация изображений рентгенограмм; предобработка изображений с целью повышения качества распознавания объектов на медицинских снимках и др.;

– модели и методы, применяемые для решения: алгоритм детектирования снижения прозрачности легких; алгоритм выделения легких на базе сверточных нейронных сетей, алгоритм детектирования узлов/очагов на базе трехмерных сверточных сетей; метод перекрестной проверки и решетчатого поиска; метод анализа амплитудных спектров Фурье в скользящем окне, аппроксимация гистограмм яркости в окне анализа; алгоритм выделения легких на базе сверточных нейронных сетей, алгоритм детектирования узлов/очагов на базе трехмерных сверточных сетей; алгоритм по водоразделу (Watershed); метод получения вектора входных признаков искусственной нейронной сети; метод ложноположительного сокращения, основанный на вейвлет – преобразованиях; метод граничных градиентов; методы бинаризации, а именно Ниблэка, Бернсена, Оцу. Зака; метод Собеля).

Заключение

В ходе проведенного анализа современного состояния исследований в области распознавания рентгеновских и КТ снимков с помощью методов глубокого машинного обучения было выявлено, что распознавание патологических процессов в настоящее время является одной из наиболее важных задач обработки и анализа медицинских изображений. Точная диагностика патологий на ранних этапах их возникновения усложняется проблемой дефицита квалифицированных специалистов, а также высокой вероятностью врачебной ошибки. Традиционные методы изучения патологий в совокупности с системами поддержки принятия врачебных решений, в которых используются методы машинного обучения, позволяют решить ряд этих проблем.

СПИСОК ЛИТЕРАТУРЫ

1. Федеральная служба государственной статистики. URL: https://rosstat.gov.ru/folder/13721 (дата обращения: 14.07.2021)
2. Кульневич А.Д., Сергеева Н.Д., Чугунов Р.А., СИСТЕМА РАННЕГО ДЕТЕКТИРОВАНИЯ ПНЕВМОНИИ НА ОСНОВЕ МЕТОДОВ ГЛУБОКОГО ОБУЧЕНИЯ// ВЕСТНИК АмГУ 2018. №83 (35).
URL: https://cyberleninka.ru/article/n/sistema-rannego-detektirovaniya-pnevmonii-na-osnove-metodov-glubokogo-obucheniya (дата обращения: 14.07.2021).

3. Ефремцев В.Г., Ефремцев Н.Г., Тетерин Е.П., Тетерин П.Е., Базавлук Е.С.. Классификация рентгеновских изображений грудной клетки больных вирусной пневмонией и COVID-19 с помощью нейронных сетей// КОМПЬЮТЕРНАЯ ОПТИКА 2021. №1 (45). URL: https://cyberleninka.ru/article/n/klassifikatsiya-rentgenovskih-izobrazheniy-grudnoy-kletki-bolnyh-virusnoy-pnevmoniey-i-covid-19-s-pomoschyu-neyronnyh-setey(дата обращения: 14.07.2021).
4. Томакова Р.А., Филист С.А., Дураков И.В.. ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ АВТОМАТИЗИРОВАННОЙ КЛАССИФИКАЦИИ РЕНТГЕНОГРАММ ГРУДНОЙ КЛЕТКИ НА ОСНОВЕ ГИБРИДНЫХ КЛАССИФИКАТОРОВ// ЭКОЛОГИЯ ЧЕЛОВЕКА 2018. С 59–63 URL: https://cyberleninka.ru/article/n/programmnoe-obespechenie-avtomaticheskoy-klassifikatsii-rentgenogramm-grudnoy-kletki-na-osnove-gibridnyh-klassifikatorov (дата обращения: 14.07.2021).
5. Дрокин И.С., Еричева Е.В., Бухвалов О.Л., Пилюс П.С., Малыгина Т.С., Синицын В.Е.. ОПЫТ РАЗРАБОТКИ И ВНЕДРЕНИЯ СИСТЕМЫ ПОИСКА ОНКОЛОГИЧЕСКИХ ОБРАЗОВАНИЙ С ПОМОЩЬЮ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА НА ПРИМЕРЕ РЕНТГЕНОВСКОЙ КОМПЬЮТЕРНОЙ ТОМОГРАФИИ ЛЕГКИХ// ВРАЧ И ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ. 2019. №3. URL: https://cyberleninka.ru/article/n/opyt-razrabotki-i-vnedreniya-sistemy-poiska-onkologicheskih-obrazovaniy-s-pomoschyu-iskusstvennogo-intellekta-na-primere-rentgenovskoy/viewer (дата обращения: 14.07.2021).
6. Андреев В.В., Минаев Н.Ю. СВЕРТОЧНАЯ НЕЙРОННАЯ СЕТЬ ДЛЯ РАСПОЗНАВАНИЯ РАКА ЛЕГКИХ НА МЕДИЦИНСКИХ СНИМКАХ // COLLOQUIUM-JOURNAL. 2019. С 173-175. URL: https://www.elibrary.ru/item.asp?id=38523560 (дата обращения: 14.07.2021).
7. Хамад Ю.А., Симонов К.В. ПРОГРАММА ДЛЯ ОБРАБОТКИ И АНАЛИЗА ИЗОБРАЖЕНИЙ КОМПЬЮТЕРНОЙ ТОМОГРАФИИ И РЕНТГЕНОГРАФИИ ГРУДНОЙ КЛЕТКИ// ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ» (СФУ) 2020.
URL: https://www.elibrary.ru/item.asp?id=43965796 (дата обращения: 14.07.2021).
8. Максимова Е.И., Хаустов П.А. АЛГОРИТМ ОБНАРУЖЕНИЯ ОБРАЗОВАНИЙ В ЛЕГКИХ ЧЕЛОВЕКА НА СНИМКАХ КОМПЬЮТЕРНОГО ТОМОГРАФА С ИСПОЛЬЗОВАНИЕМ ИСКУССТВЕННОЙ НЕЙРОННОЙ СЕТИ //
ФУНДАМЕНТАЛЬНЫЕ ИССЛЕДОВАНИЯ 2016. №4 (2) С. 290-294. URL: https://www.elibrary.ru/item.asp?id=25953356 (дата обращения: 14.07.2021).
9. Борисов Д.Н., Кульнев С. В., Лемешкин Р. Н. ИСПОЛЬЗОВАНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ПРИ АНАЛИЗЕ ЦИФРОВЫХ ДИАГНОСТИЧЕСКИХ ИЗОБРАЖЕНИЙ// СОСТОЯНИЕ И ПЕРСПЕКТИВЫ РАЗВИТИЯ СОВРЕМЕННОЙ НАУКИ ПО НАПРАВЛЕНИЮ "ТЕХНИЧЕСКОЕ ЗРЕНИЕ И РАСПОЗНАВАНИЕ ОБРАЗОВ". 2019. С. 163-169 URL: https://www.elibrary.ru/item.asp?id=41824272 (дата обращения: 14.07.2021).
10. Филиппова А.Ю., Синицын В.Е. СРАВНЕНИЕ ПРОГРАММ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ДЛЯ КОЛИЧЕСТВЕННОЙ ОЦЕНКИ ПОРАЖЕНИЙ ЛЕГКИХ У ПАЦИЕНТОВ С COVID-19// Научно-образовательный журнал для студентов и преподавателей «StudNet»2021. №6. URL: https://cyberleninka.ru/article/n/sravnenie-programm-iskusstvennogo-intellekta-dlya-kolichestvennoy-otsenki-porazheniy-legkih-u-patsientov-s-covid-19 (дата обращения: 14.07.2021).
11. Xu X. W. et al. Development of an improved CAD scheme for automated detection of lung nodules in digital chest images //Medical Physics. – 1997. – Т. 24. – № 9. – С. 1395-1403. URL:https://pubmed.ncbi.nlm.nih.gov/9304567/ (дата обращения: 14.07.2021).
12. Keserci B., Yoshida H. Computerized detection of pulmonary nodules in chest radiographs based on morphological features and wavelet snake model // Medical Image Analysis. – 2002. – Т. 6. – № 4. – С. 431-447.URL:https://pubmed.ncbi.nlm.nih.gov/12494950/ (дата обращения: 14.07.2021).

13. Junji Shiraishi 1, Feng Li, Kunio Doi Computer-aided diagnosis for improved detection of lung nodules by use of posterior-anterior and lateral chest radiographs // Acad Radiol – 2007. – Т. 14. – № 1. – С. 28-37. URL: https://pubmed.ncbi.nlm.nih.gov/17178363/ (дата обращения: 14.07.2021).
14. Шагалова П.А., Ерофеева А.Д.,Орлова М.М.,Чистякова Ю.С., Соколова Э.С. ИССЛЕДОВАНИЕ АЛГОРИТМОВ ПРЕДОБРАБОТКИ ИЗОБРАЖЕНИЙ ДЛЯ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ РАСПОЗНАВАНИЯ МЕДИЦИНСКИХ СНИМКОВ // Труды НГТУ им. Р. Е. Алексеева 2020. №1(128) URL: https://cyberleninka.ru/article/n/issledovanie-algoritmov-predobrabotki-izobrazheniy-dlya-povysheniya-effektivnosti-raspoznavaniya-meditsinskih-snimkov/viewer (дата обращения: 14.07.2021).
15. Козарь Р.В.,Навроцкий А.А.,Гуринович А.Б. Методы распознавания медицинских изображений в задачах компьютерной диагностики// Известия Гомельского государственного университета имени Ф. Скорины 2020. №3 (120). URL: https://elib.gsu.by/bitstream/123456789/11756/1/Kozar_Recognition_methods_for_medical.pdf (дата обращения: 14.07.2021).
16. Хамад Ю.А., Симонов К.В. , Кенц А.С. АЛГОРИТМЫ СЕГМЕНТАЦИИ И РАСПОЗНАВАНИЯ ОБЪЕКТОВ НА МЕДИЦИНСКИХ ИЗОБРАЖЕНИЯХ НА ОСНОВЕ ШИАРЛЕТ-ПРЕОБРАЗОВАНИЯ И НЕЙРОННЫХ СЕТЕЙ // ИНФОРМАТИЗАЦИЯ И СВЯЗЬ 2020. №2 С. 35-45. URL: https://www.elibrary.ru/item.asp?id=42976411 (дата обращения: 16.07.2021).
17. Симонов К.В. , Зотин А.Г., Хамад Ю.А., Курако М.А., Кенц А.С. АЛГОРИТМЫ ОБНАРУЖЕНИЯ И КЛАССИФИКАЦИИ ВИЗУАЛЬНЫХ ДАННЫХ// ИНФОРМАТИЗАЦИЯ И СВЯЗЬ. 2019. №4 С. 55-63.URL: https://www.elibrary.ru/item.asp?id=41563759 (дата обращения: 16.07.2021).
18. Мелдо А.А., Уткин Л.В., Трофимова Т.Н. Искусственный интеллект в медицине: современное состояние и основные направления развития интеллектуальной диагностики// Лучевая диагностика и терапия. 2020. №1 (11). URL: https://radiag.bmoc-spb.ru/jour/article/view/475 (дата обращения: 16.07.2021).
19. Baboo S.S., Iyyapparaj E. A classification and analysis of pulmonary nodules in CT images using random forest// 2018 2nd International Conference on Inventive Systems and Control (ICISC). – IEEE, 2018. – С. 1226-1232. URL: https://ieeexplore.ieee.org/document/8399000 (дата обращения: 18.07.2021).
20. Coppini G. et al. Neural networks for computer-aided diagnosis: detection of lung nodules in chest radiograms //IEEE Transactions on Information Technology in Biomedicine. – 2003. – Т. 7. – №. 4. – С. 344-357 URL: https://ieeexplore.ieee.org/document/1263906 (дата обращения: 18.07.2021).
21. Kieu P. N. et al. Applying multi-CNNs model for detecting abnormal problem on chest x-ray images //2018 10th International Conference on Knowledge and Systems Engineering (KSE). – IEEE, 2018. – С. 300-305.URL: https://ieeexplore.ieee.org/document/8573404 (дата обращения: 18.07.2021).

УДК 550.8.053

И. С. ИВАНОВ
igor.ivanov.2413@gmail.com
Науч. руководитель – канд. техн. наук, проф. А. В. ВОРОБЬЕВ

Уфимский государственный авиационный технический университет

ЛИНЕЙНАЯ РЕГРЕССИЯ КАК МЕТОД ВОССТАНОВЛЕНИЯ И РЕТРОСПЕКТИВНОГО ПРОГНОЗА ВРЕМЕННЫХ РЯДОВ ГЕОИНДУЦИРОВАННЫХ ТОКОВ

Аннотация. В статье рассматривается линейная регрессия как метод восстановления и ретроспективного прогноза временных рядов геоиндуцированных токов. Были рассмотрены различные модели машинного обучения, для решения проблемы при которой геомагнитное поле вызывает геоиндуцированные токи на линиях электропередач, на электростанциях и других источниках электрического питания. Проведено исследование с оценкой точности моделей машинного обучения, проведено сравнение моделей по некоторым критериям, а также предложена модель с наиболее точным показателем спрогнозированного геоиндуцированного тока.
***Ключевые слова*:** геомагнитное поле; геомагнитные бури; геоиндуцированные токи; машинное обучение; линейная регрессия.

Введение

Геомагнитная буря является сильным возмущением геомагнитного поля, возникающих, как правило, вследствие солнечных вспышек, искажающих параметры невозмущенной магнитосферы и длящихся от нескольких часов до нескольких суток [1]. Доказано [2], что данное явление вызывает геоиндуцированные токи (ГИТ) в проводящих технологических конструкциях (трубопроводах, линиях электропередач (ЛЭП), трансокеанских кабелях, системах автоматики железных дорог и др.), которые влекут за собой аварийные ситуации в энергетических системах (линии электропередач — ЛЭП, релейные линии, трансформаторные подстанции)[3]. Так, в заземленных сетях во время геомагнитных бурь (ГМБ) наблюдались ГИТ до 200-300 А, когда токов с интенсивностью всего несколько ампер достаточно, чтобы вывести некоторые типы трансформаторов из линейного режима. Магнитная буря 13 марта 1989 г. явилась причиной выхода из строя силовых трансформаторов и каскадного отключения (блэкаута) линий электропередачи (ЛЭП) более, чем на 9 часов в провинции Квебек (Канада)[4].

В связи с этим прогнозирование геоиндуцированных токов при геомагнитных бурях около силовых трансформаторов в энергетических системах является актуальным, поскольку знание показателя ГИТ во время геомагнитных бурь на энергетических системах позволит в некоторой степени контролировать ГМБ, а также минимизировать ущерб нанесенный ГМБ на энергетических системах. В рамках данного исследования будет протестированы некоторые модели машинного обучения для наиболее точного прогноза геоиндуцированных токов основываясь на показателях вариации геомагнитного поля.

Исходные данные

Для обучения модели машинного обучения были взяты данные возмущений геоиндуцированных токов на ЛЭП в пункте «Выходной» (VKH) (географические координаты 68.83° N, 33.08° E), регистрация ГИТ происходит с разрешением по времени в 1 минуту. Поскольку в близости с данным пунктом наблюдения вариация геомагнитного поля невозможны, использованы данные магнитных станций IMAGE [www.geo.fmi.fi/image]. Использованы данные магнитных обсерваторий, ближайших к ГИТ-станции: IVA (географические координаты 68.56° N, 27.29° E, удаление 236 км), KEV (69.76° N, 27.01° E, удаление 260 км), SOD (67.37° N, 26.63° E, удаление 313 км) и ABK (68.35° N, 18.82° E, удаление 580 км) (с разрешением по времени в 1 минуту). Также в качестве характеристик космической погоды были использованы индексы AE, суббуревой SME и PCN (с разрешением по времени в 1 минуту). AE-индекс характеризует магнитную возмущенность в зоне в целом, безотносительно к месту появления возмущения. PCN-индекс характеризует геомагнитные возмущения в полярной шапке, обусловленные воздействием солнечного ветра и межпланетного магнитного поля на магнитосферу Земли.

Построение моделей

В рамках данной статьи для сравнения и выбора оптимальной модели машинного обучения были протестированы следующие алгоритмы линейной регрессии: линейная регрессия с L1-регуляризацией (регрессия наименьших уг-

лов, Lasso), линейная регрессия с L2-регуляризацией (гребневая регрессия, Ridge), а также линейная регрессия сочетающая в себе L1 и L2 регуляризации (ElasticNet). Для построения моделей линейной регрессии была использована библиотека Python – Scikit Learn [https://scikit-learn.org/stable/modules/linear_model.html].

Для повышения точности прогноза значения разрешения по времени в 1 минуту были усреднены до 15 минут. Точность прогноза каждой модели оценивалась по формуле средней квадратической ошибки (MSE)(формула 1).

$$\mathrm{M}SE = \frac{1}{n}\sum_{i=1}^{n}(y_i - \hat{y}_i)^2 \quad \#(1)$$

n – количество элементов; y – спрогнозированные данные; $\hat{y}$ – фактические данные.

В результате тестирования моделей на всех имеющихся данных мы пришли к следующим значениям MSE: Lasso – 0.2224, Ridge и ElasticNet – 0.1193. Регрессия с L1-регуляризацией из-за своей спецификации обнуляла минимальные коэффициенты, в следствии чего мы получаем снижение в точности прогноза. Алгоритм модели ElasticNet в большей степени (75%) основывался на L2-регуляризации, что делает его альтернативой Ridge-регрессии, отсюда исходит приблизительно одинаковые значения точности моделей. Таким образом можно прийти к выводу, что среди данных моделей машинного обучении наиболее подходящим может считаться модель Ridge-регрессии, поскольку L1-регуляризация снижает точность прогноза ГИТ.

17-18 марта 2015 года произошла геомагнитная буря в следствии чего значения ГИТ достигали отметки в 50 А, при таких значениях ГИТ могут выйти из строя элементы энергетической системы. Модель гребневой регрессии спрогнозировала ГИТ по данным вариаций геомагнитного поля, результат прогноза регрессии представлен на рисунке 1.

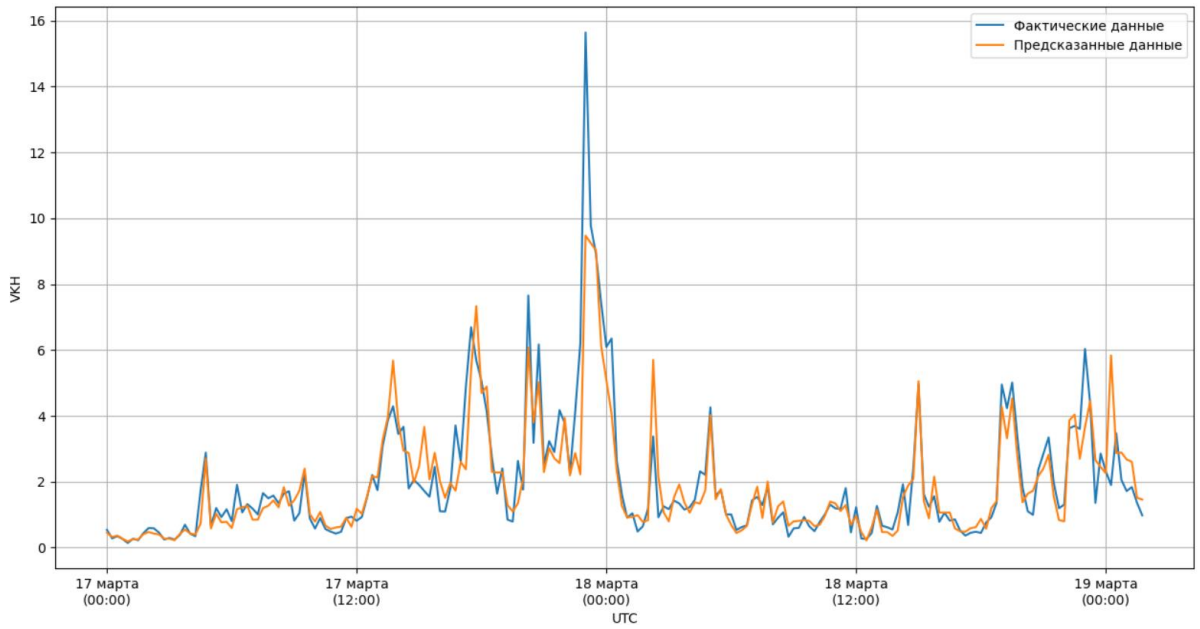


Рис. 1. График прогноза геоиндуцированных токов

По графику видно что модель прогнозирует ГИТ во время данной геомагнитной бури со средней точностью. Большая погрешность в точности ГИТ можно заметить в конце 17 марта, когда ГИТ на станции VKH достигала пикового значения в 16 А.

Заключение

Таким образом в ходе данного исследования были протестированы 3 модели машинного обучения, была выявлена их среднеквадратическая точность и предложена модель с наиболее низким показателем MSE. Также модель была протестирована на геомагнитной буре 17-18 марта 2015 года.

СПИСОК ЛИТЕРАТУРЫ

1. Воробьев А.В., Воробьева Г.Р. Визуализация геомагнитных вариаций в частотно-временной области информационного сигнала // Научная визуализация. 2019. Т. 11. № 2. С. 143-155

2. Воробьев А.В., Пилипенко В.А., Еникеев Т.А., Воробьева Г.Р., Христодуло О.И. Система динамической визуализации геомагнитных возмущений по данным наземных магнитных станций // Научная визуализация. 2021. Т. 13. № 1. С. 162-176.

3. Воробьев А.В., Пилипенко В.А., Еникеев Т.А., Воробьева Г.Р. Геоинформационная система для анализа динамики экстремальных геомагнитных возмущений по данным наблюдений наземных станций // Компьютерная оптика. 2020. Т. 44. № 5. С. 782-790.

4. Воробьев А.В., Пилипенко В.А., Еникеев Т.А., Воробьева Г.Р., Христодуло О.И. Система динамической визуализации геомагнитных возмущений по данным наземных магнитных станций // Научная визуализация. 2021. Т. 13. № 1. С. 162-176.

УДК 81'322.2

Р. И. КАРИМОВ
karirob@mail.ru
Науч. руководит. – доц., проф. Р. В. НАСЫРОВ

Уфимский государственный авиационный технический университет

NLP – ОБРАБОТКА ЕСТЕСТВЕННОГО ЯЗЫКА. ЛИНГВИСТИЧЕСКИЙ МЕТОД ОБРАБОТКИ ТЕКСТА

Аннотация. В данной работе представлен лингвистический метод обработки текста, который состоит из четырех этапов: графематический анализ, морфологически анализ, синтаксический анализ и семантический анализ.
Ключевые слова: NLP; обработки естественного языка; лингвистический метод.

NLP – обработка естественного языка является актуальным на сегодняшний день. NLP используется в разных сфера жизни. Основными направлениями является: распознавание речи, понимание естественного языка и генерация естественного языка. Основными методами обработки текстов естественного языка является: статический и лингвистический. Суть статического подхода в подсчете количество вхождений слов в документ. Недостатком данного подхода является то, что метод подсчитывает количество слов без учета связанности текста, эту проблему помогает решить лингвистический подход.[1]

Существует четыре этапа лингвистический анализ:

– Графематический анализ;

– морфологический анализ;

– синтаксический анализ;

– семантический анализ.

Рассмотри каждый из этих анализов подробней.

Графематический анализ выполняет начальный этап обработки текста, в результате анализа выделяет элементы структуры текста.

Выделение структурных элементов (абзацев) производится при помощи анализа большего текста следующим способом:

1. подсчет количества символов, которые определяют новый абзац:

– последовательность перевода строки и символа табуляции;

– последовательность перевода строки и двух или более символов пробелов;

– перевод строки, который не удовлетворяет предыдущим условиям.

2. подсчет отношения количества каждой последовательности в текстовом буфере к его размеру.

Задачи графематического анализа:

– выделение слов, разделителей и т.д.;

– разбиение текста на графы;

– выделение абзацев, заголовок, примечаний;

– определение в тексте границ предложений;

– распознавание сокращений, устойчивых оборотов и т.д.

Для определения границ предложений используется словарь сокращений, который содержит в информацию: текст сокращения, информацию о регистре букв в тексте, словосочетания, морфологические характеристики.[2]

Морфологический анализ представляет получение леммы или основы заданного токена или морфологических параметров.

Главной задачей является определить морфологический характер слова и словоформы, сильно завит от выбранного естественного языка.

Теперь разберем каждый из этих терминов.

Токен – это слово, которое отделено от других пребелом или другим знаком препинания. Пример: самолет, под, перелет, дом.

Лемма – это начальная форма слова, то есть без окончания. Изменение начальной формы слова при помощи добавления окончания называется «флексия». Пример: дом (начальная формы) добавляем флексию (а) и получаем новый токен (дома).

Грамматическими параметрами являются: часть речи, род, число, падеж, притяжательность и т. д. Пример: дом (сущ., муж. род, ед. ч., им. п.)

Словоформа – это группа, состоящая из токена, ее леммы и грамматических параметров. Пример: дома, дома (сущ., муж. род, ед. ч., им. п.), дома свя-

зан с начальной формы дом и имеет следующие параметры: (сущ., муж. род, множ. ч, им. п.)

Лексама – это множество слов, которые образованы от общей начальной формы. Примеры: начальная форма (лемма) дом, в этому случае лексемами будут дома, домах.

Синтаксический анализ представляет собой определение синтаксических зависимости слов в приложении.

Имеет две задачи: проверить, что предложение сформирована корректно и создать структуру(граф), наглядно показывающую синтаксические отношения между словами. Синтаксический анализатор использует словарь определенных слов (лексикон) и набор синтаксических правил (грамматика). Простой лексикон содержит только синтаксическую категорию каждого слова, простая грамматика описывает правила, которые указывают как синтаксические категории, могут быть объединены для формирования фраз разных типов. Не все системы NLP требуют полного разбора предложений.[3]

Пример: Колобок покатился в густой лес

Таблица 1

Лексикон

Слово	Категория
колобок	существительное
покатился	глагол
в	предлог
густой	прилагательное
лес	существительное

В Таблица 1

показан лексикон.

Таблица 2

Грамматика

Предложение	существительное глагол ГруппаСущ
ГруппаСущ	предлог ГруппаПрилагСущ
ГруппаПрилагСущ	прилагательное существительное

В Таблица представлена грамматика.

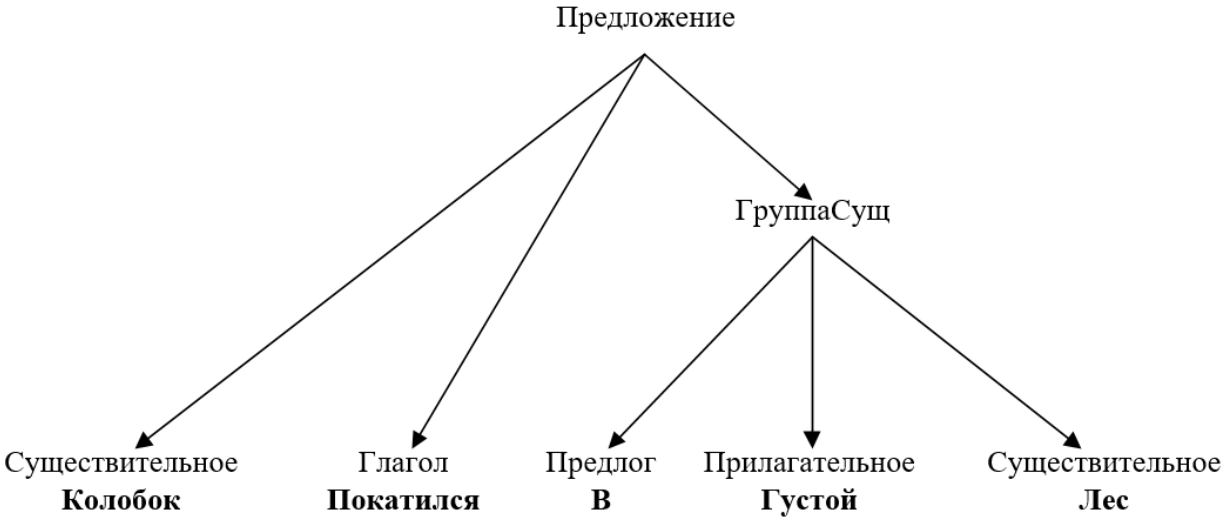


Рис. 1. Синтаксический анализ предложения

На рисунке 1 представлен синтаксический анализ предложения.

Семантический анализ – определение смыслового понимания текста

Конечной целью системы обработки естественного языка является «понимание» текста. Данный этап зависит от результатов предыдущих этапов системы и лексической информации.

Модели семантического анализа текста

Тезаурус – словарь, в котором представлены семантические отношения между лексическими значениями. С помощью тезаурусу можно понять смысл слов не только с определения, но и сопоставляя с другими понятиями и группами. В большинстве случае в тезаурус записываются синонимы, антонимы, гиперонимы, паронимы и т. д. [4]

Семантическая сеть представляет из себя граф, в которой имеются концепты предметов, событий, состояний и с представлено отношение между концепций.

Фреймовые модели – это структура, которая описывает понятия или ситуации, состоящая из характеристик ситуации и их значения. Данная модель является элементом семантической сети.

Онтологическая модель – это подробное описание предметной области, которое можно использовать для формулировки утверждений общего характера. Данная модель помогает создавать понятия, которые в будущем будут пригодны для машинной обработки.[4]

СПИСОК ЛИТЕРАТУРЫ

1.Обзор методов автоматической обработки текстов на естественном языке/ Белов С.Д., Зрелова Д.П., Зрелов П.В., Кореньков В.В.// Системный анализ в науке и образовании -2020. -№3. -С. 8-22.
2. Ерина И.С., Попов А.А. Анализ метода обработки естественного языка // MODERN SCIENCE -2020. -№7-1. -С 393-402.
3.Автоматическая обработка текстов на естественном языке и анализ данных: Учебное пособие / [Большакова Е.И и д.р.] - — М.: Изд-во НИУ ВШЭ, 2017. — 269 с.
4. Черницова Л.В. Методы и модели семантического анализа текста// Методы и модели семантического анализа текста-2017. -№11 -С 171 – 173

УДК 004.89

Е. А. КОРОВИН, С. А. ЧИГЛИНЦЕВА
arkvinst@gmail.com, s_chiglintseva@inbox.ru
Науч. руководитель – канд. техн. наук, доц. Е. Ю. САЗОНОВА

Уфимский государственный авиационный технический университет

ЗАДАЧА СЕГМЕНТИРОВАНИЯ ОБЪЕКТОВ НЕДВИЖИМОСТИ НА ОСНОВЕ ИНТЕЛЛЕКТУАЛЬНЫХ МЕТОДОВ

Аннотация. В статье рассматривается задача сегментирования объектов недвижимости на основе интеллектуальных методов. Проведен анализ предметной области, который показал, что рынок недвижимости сложный по структуре и ценообразованию. Проведена сегментация рынка недвижимости Уфы на основе кластерного анализа. Для сегментирования первичного и вторичного жилья были использованы самоорганизующиеся карты Кохонена.
***Ключевые слова*:** задача кластеризации; методы кластеризации; методы сбора информации; самоорганизующиеся карты Кохонена.

Введение

В настоящее время рынок недвижимости играет важную роль в сфере экономики. В процессе исследования были затронуты такие актуальные вопросы, как выявление особенностей рынка недвижимости, определение рыночной стоимости объектов, предоставление рекомендации для повышения, либо снижения цены объектов недвижимости. Авторами предлагается решить задачу сегментирования объектов недвижимости с целью повышения эффективности сделок за счет выявления новых знаний. Решение задачи сегментирования состоит из двух частей, а именно задачи сбора информации для анализа рынка недвижимости и анализ рынка недвижимости на основе собранных данных. Решение первой задачи представляет собой изучение HTML-кода страницы, написания скрипта для извлечения данных, запуск скрипта, сохранение данных в структурированном виде. Этапы решения второй задачи включают приведение данных к единому формату, кластеризация данных, отображению кластеров.

Постановка задачи сегментирования объектов недвижимости

Требуется собрать данные об объектах недвижимости, а именно информацию о вторичном и первичном жилье города Уфы.

Следующие характеристики объектов недвижимости рынка первичного и вторичного жилья были собраны: цена (руб.), район (географическое местоположение), номер этажа, количество этажей в доме, тип дома (панельный, кирпичный, монолитный), общая площадь (м²), жилая площадь (м²), площадь кухни (м²), детские сады (наличие/отсутствие), школы (наличие/отсутствие), балкон/лоджия, парковка (наличие/отсутствие), ипотека (наличие/отсутствие), наличный расчет (наличие/отсутствие), рассрочка (наличие/отсутствие), сертификат (наличие/отсутствие), магазин (наличие/отсутствие).

Для сбора информации был написан скрипт для извлечения данных из веб-страницы в структурированном виде [1,2]. После сбора данных необходимо разработать математическое и инструментальное программное обеспечение для задачи сегментирования объектов недвижимости, которая может быть сведена к задаче кластеризации [3,4].

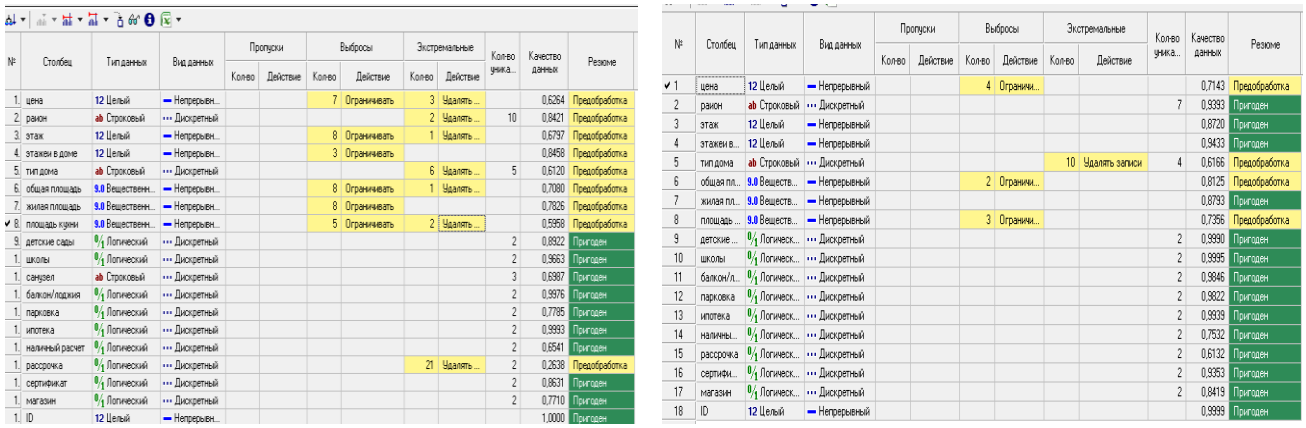
Решение задачи сегментирования объектов недвижимости

Для решения задачи сегментирования объектов недвижимости предлагается использовать самоорганизующиеся карты Кохонена. Выбор обосновывается тем, что данная нейронная сеть – это мощный самообучающийся механизм кластеризации, позволяющий отобразить результаты в виде компактных и удобных для интерпретации двумерных карт. Самоорганизующиеся карты Кохонена используется для поиска закономерностей в больших массивах данных, что позволяет проводить разведочный анализ данных, отличающийся от классических статистических процедур, в ходе которых проверяется некоторый набор выдвинутых гипотез, а также визуализировать многомерные входные данные.

Для решения задачи сегментации объектов недвижимости было применено инструментальное средство Deductor Studio [5,6].

На этапе предобработки данных было обнаружено несколько выбросов (выходящих за границы 3-сигма) и экстремальных значений (выходящий за

границы 5-сигма). Для улучшения качества данных и их пригодности были удалены все экстремальные значения (рис. 1).



№	Столбец	Тип данных	Вид данных	Пропуски		Выбросы		Экстремальные		Кол-во уника...	Качество данных	Резюме
				Кол-во	Действие	Кол-во	Действие	Кол-во	Действие			
1	цена	12 Целый	Непрерывн...			7	Ограничивать	3	Удалять ...		0,6264	Предобработка
2	район	ab Строковый	Дискретный					2	Удалять ...	10	0,8421	Предобработка
3	этаж	12 Целый	Непрерывн...			8	Ограничивать	1	Удалять ...		0,6797	Предобработка
4	этажей в доме	12 Целый	Непрерывн...			3	Ограничивать				0,8458	Предобработка
5	тип дома	ab Строковый	Дискретный					6	Удалять ...	5	0,6120	Предобработка
6	общая площадь	9.0 Вещественн...	Непрерывн...			8	Ограничивать	1	Удалять ...		0,7080	Предобработка
7	жилая площадь	9.0 Вещественн...	Непрерывн...			8	Ограничивать				0,7826	Предобработка
8	площадь кухни	9.0 Вещественн...	Непрерывн...			5	Ограничивать	2	Удалять ...		0,5958	Предобработка
9	детские сады	0/1 Логический	Дискретный							2	0,8922	Пригоден
10	школы	0/1 Логический	Дискретный							2	0,9663	Пригоден
11	санузел	ab Строковый	Дискретный							3	0,6987	Пригоден
12	балкон/лоджия	0/1 Логический	Дискретный							2	0,9976	Пригоден
13	парковка	0/1 Логический	Дискретный							2	0,7785	Пригоден
14	ипотека	0/1 Логический	Дискретный							2	0,9993	Пригоден
15	наличный расчет	0/1 Логический	Дискретный							2	0,6541	Пригоден
16	рассрочка	0/1 Логический	Дискретный					21	Удалять ...	2	0,2638	Предобработка
17	сертификат	0/1 Логический	Дискретный							2	0,8631	Пригоден
18	магазин	0/1 Логический	Дискретный							2	0,7710	Пригоден
19	ID	12 Целый	Непрерывн...								1,0000	Пригоден

№	Столбец	Тип данных	Вид данных	Пропуски		Выбросы		Экстремальные		Кол-во уника...	Качество данных	Резюме
				Кол-во	Действие	Кол-во	Действие	Кол-во	Действие			
1	цена	12 Целый	Непрерывный			4	Ограничи...				0,7143	Предобработка
2	район	ab Строковый	Дискретный							7	0,9393	Пригоден
3	этаж	12 Целый	Непрерывный								0,8720	Пригоден
4	этажей в...	12 Целый	Непрерывный								0,9433	Пригоден
5	тип дома	ab Строковый	Дискретный					10	Удалять записи	4	0,6166	Предобработка
6	общая пл...	9.0 Веществ...	Непрерывный			2	Ограничи...				0,8125	Предобработка
7	жилая пл...	9.0 Веществ...	Непрерывный								0,8793	Пригоден
8	площадь ...	9.0 Веществ...	Непрерывный			3	Ограничи...				0,7356	Предобработка
9	детские ...	0/1 Логическ...	Дискретный							2	0,9990	Пригоден
10	школы	0/1 Логическ...	Дискретный							2	0,9995	Пригоден
11	балкон/л...	0/1 Логическ...	Дискретный							2	0,9846	Пригоден
12	парковка	0/1 Логическ...	Дискретный							2	0,9822	Пригоден
13	ипотека	0/1 Логическ...	Дискретный							2	0,9939	Пригоден
14	наличны...	0/1 Логическ...	Дискретный							2	0,7532	Пригоден
15	рассрочка	0/1 Логическ...	Дискретный							2	0,6132	Пригоден
16	сертифи...	0/1 Логическ...	Дискретный							2	0,9353	Пригоден
17	магазин	0/1 Логическ...	Дискретный							2	0,8419	Пригоден
18	ID	12 Целый	Непрерывный								0,9999	Пригоден

а *б*

Рис. 1. Результат этапа «Предобработка данных»:
а – «Первичное жилье»; б – «Вторичное жилье»

На этапе обработки данных согласно статистической информации была изменена значимость полей по главным и второстепенным признакам, на которые обращают внимание покупатели, выбирая недвижимость, так наибольшей значимостью обладают следующие характеристики: цена, район, типа дома, номер этажа и общая площадь квартиры.

На рисунке 2 представлены параметры обучения карт Кохонена. В настройках параметров карты Кохонена были заданы шестиугольные ячейки размером 24x18, чтобы получить наглядное отображение кластеров. Способом начальной инициализации карты была выбрана инициализация из собственных векторов – начальные веса нейронов карты будут проинициализированы значениями подмножества гиперплоскости, через которую проходят два главных собственных вектора матрицы ковариации входных значений обучающей выборки. Радиус обучения в начале обучения взят равным 8, так как он должен быть достаточно большой – примерно половина или меньше размера карты (максимальное линейное расстояние от любого нейрона до другого любого нейрона), а в конце 0,1.

В качестве функции соседства была выбрана Гауссова функция соседства, в которой обучение проходит более плавно и равномерно, так как одновременно изменяются веса всех нейронов, что может дать лучше результат, чем, если бы использовалась ступенчатая функция.

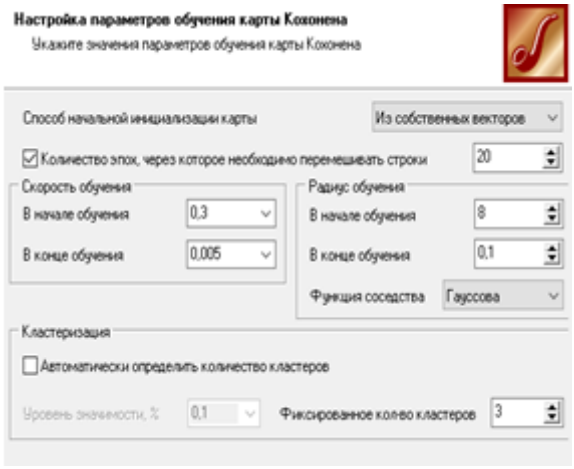


Рис. 2. Параметры обучения карт Кохонена

Для анализа всей карты авторами были применены: матрица расстояний для визуализации структуры кластеров, полученных в результате обучения карты; матрица ошибок квантования для отображения среднего расстояния от расположения примеров до центра ячейки; матрица плотности попадания для отображения количества объектов, попавших в ячейку.

Получившиеся карты Кохонена имеют четкое разделение на кластеры (рис. 3-4). Разделение на кластеры являются адекватным.

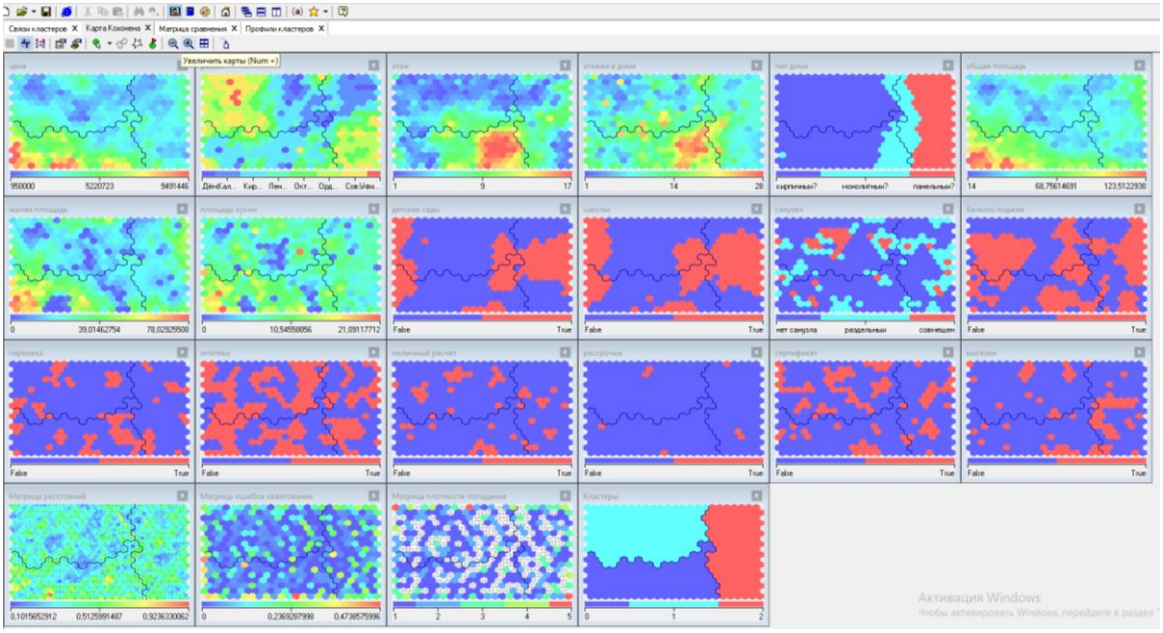


Рис. 3. Карта Кохонена для первичного жилья

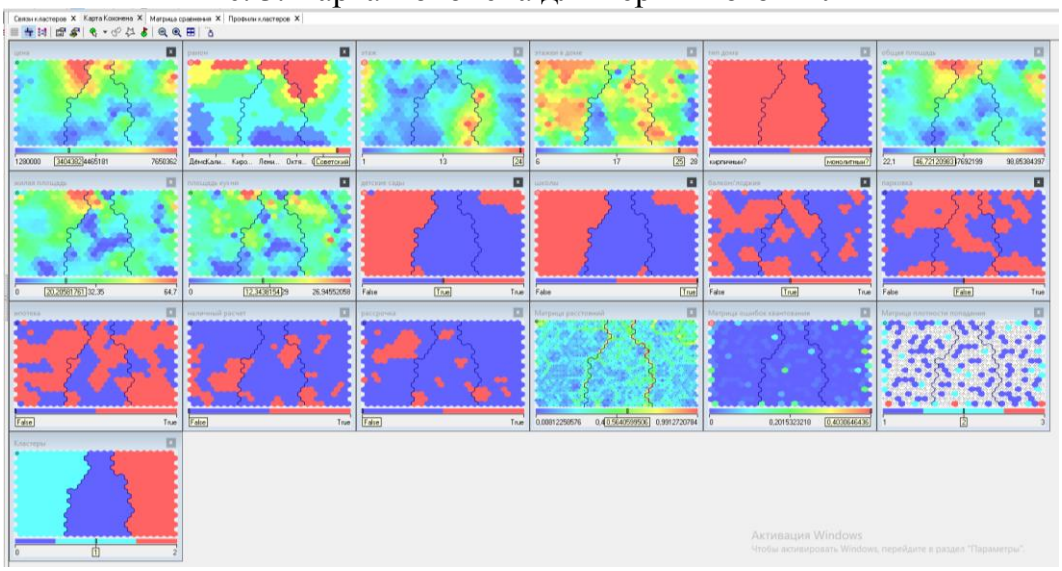


Рис. 4. Карта Кохонена для вторичного жилья

С помощью профилей кластеров и визуализатора Куб в ПП Deductor Studio были интерпретированы сегменты в первичном и вторичном жилье. Фрагмент интерпретации приведен в таблице 1.

Таблица 1

Характеристика кластеров

Кластер	*Характеристика*
Кластер "Элитное жилье"	Характеризуется: высокой средней общей (среднее значение ~ 76 м²) и жилой (среднее значение ~ 35 м²) площадью с большим отрывом по сравнению с двумя остальными кластерами, то же самое касается и цены (средняя цена ~ 6 млн. руб, диапазон от 2,049 млн. руб. до 9,491 млн.руб.). Местоположение преимущественно в Кировском (42%) и Октябрьском (20%)

	районах, так же в высокий показатель преобладания этих квартир в Ленинском районе (14 из 30 случаев). Дом отличается многоэтажностью, а квартира - расположением на высоком этаже. Из всех кластеров – самый высокий уровень наличия парковочных мест, средним уровнем наличия школ и детских садов поблизости. Тип дома преимущественно кирпичный и монолитный. Данный сегмент можно назвать "Элитное жилье".
...	…
Кластер "Жилье комфорт»	Характеризуется: чуть выше средней общей (среднее значение ~ 49 м²) и жилой (среднее значение ~ 25 м²) площадью. Стоимость квартир тоже невысокая (средняя цена ~ 3,1 млн. руб, диапазон от 1,2 млн.руб до 6,3 млн.). Местоположение преимущественно в Октябрьском (22%), Калининском (22%) и Советском (18%) районах. Тип дома преимущественно панельный. Квартиры отличаются расположением на среднем этаже (в среднем 5-й этаж). Из всех кластеров – средний уровень наличия парковочных мест, школ и детских садов поблизости. Данный сегмент можно назвать "Жилье комфорт".

На основе полученных кластеров и их интерпретации авторами были разработаны продукционные правила. Фрагмент продукционных правил представлен далее:

Правило 1. Если цена объекта повышенная, то он имеет большую общую площадь и развитую инфраструктуру поблизости.

Правило 2. Если объект имеет большую общую площадь и развитую инфраструктуру поблизости, то его цена будет повышенной.

Правило 3. Если цена объекта заниженная, то он имеет малую общую площадь и отсутствие развитой инфраструктуры поблизости.

Правило 4. Если объект расположен в Ленинском районе, то его цена будет завышенной.

Правило 5. Если объект расположен в Демском районе, то его цена будет заниженной.

Правило N. Если объект обладает многоэтажностью, то его цена преимущественно будет завышена.

Заключение

Авторами статьи приведена содержательная постановка задачи сегментирования объектов недвижимости. Был проведен анализ рынка недвижимости,

который включает сегментирование данных на основе кластерного анализа. Для сегментирования первичного и вторичного жилья были использованы самоорганизующиеся карты Кохонена. Авторами также проведена интерпретация кластеров и разработаны продукционные правила.

Результаты исследования, приведенные в статье, получены в рамках выполнения грантов РФФИ 19-07-00709 и государственного задания No FEUE-2020-0007.

СПИСОК ЛИТЕРАТУРЫ

1. Математическое и программное обеспечение задачи анализа рынка недвижимости на основе интеллектуальных технологий : Выпускная квалификационная работа / Якупова Айсылу Вазировна.— Уфа, 2020 .— с.104 .— Текст: электронный. — 02.03.03-Математическое обеспечение и администрирование информационных систем
2. Якупова А. В., Сметанина О. Н., Сазонова Е. Ю. Подход к решению задачи сегментирования на основе интеллектуальных технологий // Сборн. трудов V Международная научно-техническая конференция «МАВЛЮТОВСКИЕ ЧТЕНИЯ» посвященная 95-летию со дня рождения член-корр. РАН, д.т.н., профессора Рыфата Рахматулловича Мавлютова, Уфа, Россия, 2020, Том 5, С. 208-213
3. Нейский И.М. Классификация и сравнение методов кластеризации [Электронный ресурс] // Интеллектуальные технологии и системы. Сборник учебно-методических работ и статей аспирантов и студентов. – М.: НОК «CLAIM», 2006. – Выпуск 8. – С. 130-142. URL: http://it-claim.ru/Persons/Neyskiy/Article2
4. Юсупова Н. И. Технологии искусственного интеллекта и машинного обучения в задачах семантического представления и анализа данных: монография // Н. И. Юсупова, О.Н. Сметанина, М. М. Гаянова и др. – М.: "Издательство "Инновационное машиностроение", 2020. – 242 с.
5. Практикум [Р.120] Карты Кохонена в Deductor Studio [Электронный ресурс]. Режим доступа: https://docplayer.ru/27573133-Praktikum-p-120-karty-kohonena-v-deductor-studio.html (дата обращения: 14.09.2021)
6. Самоорганизующиеся карты Кохонена — математический аппарат. [Электронный ресурс]. Режим доступа: https://basegroup.ru/community/articles/som (дата обращения: 14.09.2021)

УДК 6.60.606, 004.032.26

О. О. МИРАСОВ
helgu76@gmail.com
Науч. руководов. – д-р техн. наук, проф. Г. Р. ШАХМАМЕТОВА

Уфимский государственный авиационный технический университет

АНАЛИЗ СОВРЕМЕННОГО СОСТОЯНИЯ ИССЛЕДОВАНИЙ В ОБЛАСТИ ОБРАБОТКИ ГЕНОМНЫХ ДАННЫХ МЕТОДАМИ МАШИННОГО ОБУЧЕНИЯ

Аннотация. В статье приводится анализ состояния научных исследований обработки геномных данных методами машинного обучения. Отмечены проблемы, решаемые при помощи нейронных сетей, а также используемые технологии, модели и средства.
Ключевые слова: машинное обучение; глубокое обучение; нейронные сети; искусственный интеллект; биоинформатика; ДНК; геномные данные.

Введение

С переходом в информационную эру данные стали одним из главнейших ресурсов, а извлечение необходимой информации — жизненно необходимым навыком для науки и бизнеса в XXI веке. И вполне закономерно, что машинное обучение стало активно развивающейся областью знаний.

Машинное обучение – это наука о компьютерных алгоритмах, которые могут автоматически улучшаться благодаря опыту и использованию данных. Алгоритмы машинного обучения создают модель на основе выборочных данных, чтобы делать прогнозы или решения, не будучи явно запрограммированными на это. Алгоритмы машинного обучения используются в самых разных задачах, в которых сложно или невозможно разработать традиционные алгоритмы для достижения поставленных целей, в том числе и в биоинформатике.

До появления машинного обучения алгоритмы биоинформатики нужно было программировать вручную; для таких задач, как предсказание структуры белка, это оказалось трудным. Методы машинного обучения, такие как глубокое обучение, могут изучать особенности наборов данных, вместо того, чтобы требовать от программиста определять их индивидуально. Алгоритм может дополнительно научиться объединять низкоуровневые функции в более абстракт-

ные и т. д. Этот многоуровневый подход позволяет таким системам делать сложные прогнозы при соответствующем обучении.

На данный момент методы машинного обучения позволяют решать проблемы в таких областях, как: геномика, протеомика, метагеномика. Отдельно можно выделить вычислительную геномику, занимающуюся прогнозированием точного расположения всех генов человека, изучающую раннее эмбриональное развитие человека при помощи анализа консервативных областей генома и т.д.

В данной работе на основе научных публикаций проведен анализ существующих методов машинного обучения в области анализа геномных данных.

Современное состояние проблемы

Задача заключается в построении алгоритмов и методов, позволяющих аннотировать вторичные структуры ДНК (РНК) известными геномными и эпигеномными разметками. Применяются методы машинного обучения, основанные на алгоритмах обучения без учителя, таких как кластеризация и методы понижения размерности, для компьютерной обработки и поисков зависимостей в организации вторичных структур в геноме. Результатом работы [1] стало создание универсальной структуры для хранения и обработки геномных данных, представленных в виде интервальных последовательностей, а также кластеризация, обработанных такой структурой, данных.

В статье [2] анализируются различные варианты нейронных сетей для предсказания последствии мутаций в клетках и для анализа геномных клеток и извлечения полезной информации для лечения разного вида болезней.

Область машинного обучения, направленная на разработку компьютерных алгоритмов, которые улучшаются с опытом, обещает позволить компьютерам помогать людям в анализе больших и сложных наборов данных. В [3] предоставляется обзор приложений машинного обучения для анализа наборов данных секвенирования генома, включая аннотацию элементов последовательности и эпигенетических, протеомных или метаболомных данных. Представляются соображения и повторяющиеся проблемы в применении контролируе-

мых, частично контролируемых и неконтролируемых методов машинного обучения, а также генеративного и дискриминативного подходов к моделированию.

Авторами [4] представляется пространственная кластеризация - новая методология неконтролируемой кластеризации для разделения больших, многодорожечных наборов геномных и эпигеномных данных на пространственно организованный набор различных комбинаторных поведений. Разрабатываем вероятностный алгоритм, который находит решения для пространственной кластеризации путем изучения модели HMM и определения наиболее вероятного геномного расположения кластеров.

В результате анализа [5] были определены классификаторы, точность которых может достигать 80%, и позволяющие идентифицировать биосинтетические ферменты и соответствующие им молекулярные особенности, связанные с активностью антибиотиков.

В [6] обсуждаются конкретные применения машинного обучения для выявления структурных особенностей в секвенированных геномах, прогнозирования взаимодействий между различными клеточными компонентами и прогнозирования функции генов и фенотипов организма. Также предлагаются стратегии стимулирования функциональных открытий с использованием подходов на основе машинного обучения на заводах.

В обзоре [7] сначала резюмируются основные классы проблем, для решения которых хорошо подходят системы искусственного интеллекта, и описываются клинические диагностические задачи, которые выигрывают от этих решений. Далее описываются на новые методы решения конкретных задач клинической геномики, включая вызов вариантов, аннотацию генома и классификацию вариантов, а также соответствие фенотипа генотипу. В заключение обсуждается будущий потенциал ИИ в индивидуальных медицинских приложениях, особенно для прогнозирования рисков при распространенных сложных заболеваниях, а также проблем, ограничений и предубеждений, которые необ-

ходимо тщательно решать для успешного развертывания ИИ в медицинских приложениях, особенно те, которые используют данные генетики и геномики человека.

Разные методы машинного обучения могут соответствовать базовым предположениям о данных; например, два популярных метода глубокого обучения, сверхточная нейронная сеть (CNN) и рекуррентная нейронная сеть (RNN), были разработаны для разных типов данных. Ни один вычислительный подход или правило не подходят для всех биологических вопросов. Скорее, каждый сложный биологический вопрос потребует определенных подходов к машинному обучению, например, опорной векторной машины, случайного леса и глубокой нейронной сети, а также комбинаций дисциплин, например информатика, статистика, физика, инженерия и биология. В статье [8] прогнозируется, что в будущем спрос на исследователей, способных применять машинное обучение к сложным биологическим данным, будет возрастать.

В работе [9] обсуждаются концепции моделей глубокого обучения в геномике, а также выделяются наиболее известные архитектуры машинного обучения в области биоинформатики.

В статье [10] дается обширный обзор различных работ, выполненных в последние годы в области выбора генов на основе машинного обучения, а также анализ его эффективности. В исследовании различные алгоритмы выбора функций подразделяются на контролируемое, неконтролируемое и полуконтролируемое обучение.

В [11] предлагается основанный на глубоком обучении метод DeepHE для прогнозирования основных генов человека путем интеграции функций, полученных из данных последовательностей и сети белок-белковых взаимодействий.

Авторами [12] были изучены и сравнены 12 репрезентативных методов прогнозирования генов заболевания на основе машинного обучения с точки зрения эффективности прогнозирования и времени выполнения.

Авторами [13] были изучены возможности использования нейронных сетей для решения проблем с диагностированием рака на уровне генов.

В статье [14] дается обзор механизмов классификации последовательностей генов с использованием методов машинного обучения, который включает краткие сведения о биоинформатике, обзор литературы и ключевые вопросы секвенирования ДНК с использованием машинного обучения.

В [15] предлагаются 165 новых генов рака, которые не обязательно имеют повторяющиеся изменения, но взаимодействуют с известными генами рака, и показывается, что они соответствуют основным генам на скринингах потери функции. А также предлагается метод, открывающий новые возможности в точной онкологии, применяемый для прогнозирования биомаркеров других сложных заболеваний.

Авторы [16] представляют модель глубокого обучения (DLM) для прогнозирования глубины секвенирования следующего поколения (NGS) на основе последовательностей ДНК-зондов.

В статье [17] применяются методы глубокого обучения для выявления ДНК-связывающие белки. ДНК-связывающие белки связаны со многими функциями на клеточном уровне, включая, помимо прочего, защитный механизм организма и транспортировку кислорода. Они связывают ДНК и взаимодействуют с ними. В прошлом ДНК-связывающие белки определяли с помощью экспериментальных лабораторных методов. Однако в последние годы исследователи используют контролируемое обучение для определения ДАД исключительно по последовательностям белков.

Геном человека на 98,5% состоит из некодирующих последовательностей ДНК, и большинство из них не имеют известной функции. Однако большинство вариантов, связанных с заболеванием, находится именно в этих регионах. Следовательно, очень важно предсказать функцию некодирующей ДНК. Авторами работы [18] предложена NCNet, которая объединяет глубокое остаточное обучение и сети обучения от последовательности к последовательности, для

прогнозирования сайтов связывания фактора транскрипции, которые затем можно использовать для прогнозирования некодирующих функций.

В [19] сравниваются три метода глубокого обучения: обычная сверточная нейронная сеть, сверточная нейронная сеть с долгой краткосрочной памятью (LSTM) и двойная повторяющаяся нейронная сеть.

В [20] представлен подход на основе алгоритма сверточной нейронной сети на основе алгоритма машинного обучения для процесса идентификации потенциальных генов-мишеней, прогнозирования miRNA, визуализации уникальных паттернов miRNA и проверки геномов.

Таким образом, был произведен обзор работ в области обработки геномных данных методами машинного обучения и можно сказать, что уже сейчас количество исследований по данному направлению велико и разнообразно, и с каждым годом оно будет расти.

Заключение

Анализ геномных данных с помощью методов машинного обучения сегодня является перспективным направлением, решающим многие задачи, такие как секвенирование генома, определение классификаторов, аннотирование вторичных структур ДНК и РНК. При этом ряд задач можно решить только методами машинного обучения – предсказывание функции некодирующей ДНК, прогнозирование задач гена. Несмотря на проблемы с качеством данных и модификацией методов машинного обучения для обработки геномных данных, это направление науки является сегодня актуальным и востребованным.

СПИСОК ЛИТЕРАТУРЫ

1. Петроченко Д.В., Попцова М.С. Извлечение смысла из геномных данных методами машинного обучения // выпускные квалификационные работы НИУ ВШЭ 2018. URL: https://www.hse.ru/edu/vkr/219430444
2. А. К. Таскина, А. А. Муравьёва, А. С. Ельсукова, В. С. Фишман Методы машинного обучения в биологии // «Природа» №9, 2020 URL: https://elementy.ru/nauchno-populyarnaya_biblioteka/435560/Priroda_9_2020
3. Libbrecht, M., Noble, W. Machine learning applications in genetics and genomics. Nat Rev Genet 16, 321–332 (2015). https://doi.org/10.1038/nrg3920
4. Jaschek R., Tanay A. (2009) Spatial Clustering of Multivariate Genomic and Epigenomic Information. In: Batzoglou S. (eds) Research in Computational Molecular Biology. RECOMB

2009. Lecture Notes in Computer Science, vol 5541. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-02008-7_12
5. J. Chem. Inf. Model. 2021, 61, 6, 2560–2571, Publication Date:May 27, 2021, URL: https://doi.org/10.1021/acs.jcim.0c01304
6. Mahood EH, Kruse LH, Moghe GD. Machine learning: A powerful tool for gene function prediction in plants. Appl Plant Sci. 2020;8(7):e11376. Published 2020 Jul 28. URL: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7394712/
7. Dias, R., Torkamani A. Artificial intelligence in clinical and genomic diagnostics. Genome Med 11, 70 (2019). https://doi.org/10.1186/s13073-019-0689-8
8. Xu, C., Jackson, S.A. Machine learning and complex biological data. Genome Biol 20, 76 (2019). https://doi.org/10.1186/s13059-019-1689-0
9. Koumakis L., Deep learning models in genomics; are we there yet?, Computational and Structural Biotechnology Journal, Volume 18, 2020, ISSN 2001-0370, https://doi.org/10.1016/j.csbj.2020.06.017
10. Nivedhitha M., Durai Raj Vincent P. M., Srinivasan Kathiravan, Chang Chuan-Yu, Machine Learning Based Computational Gene Selection Models: A Survey, Performance Evaluation, Open Issues, and Future Research Directions, Frontiers in Genetics, vol. 11, 2020 URL: https://www.frontiersin.org/article/10.3389/fgene.2020.603808
11. Zhang X, Xiao W, Xiao W (2020) DeepHE: Accurately predicting human essential genes based on deep learning. PLOS Computational Biology 16(9): e1008229. https://doi.org/10.1371/journal.pcbi.1008229
12. Duc-Hau Le, Machine learning-based approaches for disease gene prediction, Briefings in Functional Genomics, Volume 19, Issue 5-6, September-November 2020, Pages 350–363, https://doi.org/10.1093/bfgp/elaa013
13. Pronier E., Predicting Gene Expression with Machine Learning URL: https://owkin.com/histogenomics/predicting-gene-expression-using-machine-learning/
14. P. Dixit and G. I. Prajapati, "Machine Learning in Bioinformatics: A Novel Approach for DNA Sequencing," 2015 Fifth International Conference on Advanced Computing & Communication Technologies, 2015, pp. 41-47, doi: 10.1109/ACCT.2015.73..
URL: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7079049&isnumber=7079031
15. Schulte-Sasse, R., Budach, S., Hnisz, D. et al. Integration of multiomics data with graph convolutional networks to identify new cancer genes and their associated molecular mechanisms. Nat Mach Intell 3, 513–526 (2021). https://doi.org/10.1038/s42256-021-00325-y
16. Zhang, J.X., Yordanov, B., Gaunt, A. et al. A deep learning model for predicting next-generation sequencing depth from DNA sequence. Nat Commun 12, 4387 (2021). https://doi.org/10.1038/s41467-021-24497-8
17. Shadman Shadab, Md Tawab Alam Khan, Nazia Afrin Neezi, Sheikh Adilina, Swakkhar Shatabda, DeepDBP: Deep neural networks for identification of DNA-binding proteins, Informatics in Medicine Unlocked, Volume 19, 2020, 100318, ISSN 2352-9148, https://doi.org/10.1016/j.imu.2020.100318
18. Zhang H, Hung C-L, Liu M, Hu X and Lin Y-Y (2019) NCNet: Deep Learning Network Models for Predicting Function of Non-coding DNA. Front. Genet. 10:432. doi: 10.3389/fgene.2019.00432
19. Hemalatha Gunasekaran, K. Ramalakshmi, A. Rex Macedo Arokiaraj, S. Deepa Kanmani, Chandran Venkatesan, C. Suresh Gnana Dhas, "Analysis of DNA Sequence Classification Using CNN and Hybrid Models", Computational and Mathematical Methods in Medicine, vol. 2021, Article ID 1835056, 12 pages, 2021. https://doi.org/10.1155/2021/1835056
20. Wang, G., Pu, P. & Shen, T. An efficient gene bigdata analysis using machine learning algorithms. Multimed Tools Appl 79, 9847–9870 (2020). https://doi.org/10.1007/s11042-019-08358-7

УДК 004.00

О. А. МОЛОКОВИЧ, П. Е. ДАДОНОВ
o.molokovich@ya.ru, ozf_dad@mail.ru
Науч. руководов. – д-р техн. наук, проф. Н. И. ЮСУПОВА

Уфимский государственный авиационный технический университет

ПРИМЕНЕНИЕ ОНТОЛОГИЧЕСКОГО ПОДХОДА ДЛЯ РЕШЕНИЯ ПРИКЛАДНЫХ ЗАДАЧ (ПО МАТЕРИАЛАМ НАУЧНОЙ ШКОЛЫ УГАТУ)

Аннотация. В данной статье описаны основные понятия и преимущества онтологического подхода к моделированию предметной области. Приведен краткий обзор применения онтологического подхода к решению различных задач ученными УГАТУ.
***Ключевые слова*:** онтология; база знаний; система поддержки принятия решений.

Введение

Одним из инструментов обеспечения интеллектуальной поддержки принятия решений является онтологический анализ, суть которого заключается в описании предметной области (ПО) в терминах сущностей, отношений между ними, и действий над сущностями. Таким образом, онтология представляет собой формализацию знаний о предметной области, что позволяет обрабатывать их вычислительными средствами (хранить, передавать, проверять и выполнять логический вывод).

В данной статье приведен краткий обзор применения онтологического подхода (ОП) к решению различных задач ученными Уфимского государственного авиационного технического университета (УГАТУ).

Анализ возможностей онтологического подхода

Онтология – это модель ПО, система, элементами которой являются:

– Экземпляр – простейшая единица онтологии, находится на самом нижнем уровне модели и представляет собой реальный или абстрактный подлежащий классификации объект (строение, символ, число).

– Атрибут – свойство объекта.

– Концепт (понятие, класс) – коллекция или абстрактная группа объектов. Классы могут быть включены в другие классы, составляя иерархию понятий.

– Отношение – зависимость между объектами онтологии (класс-подкласс, часть-целое, род-вид, временные, пространственные, причинно-следственные и др.), при построении онтологии инженеры могут определять свои собственные типы зависимостей.

– Функциональный термин - сложная структура, состоящая из отношений, может быть использован вместо отдельного термина в утверждении.

– Ограничение – формальное описание того, что должно быть истинным, чтобы какое-либо утверждение было принято в качестве входных данных.

– Правило - утверждение в форме «если-то», описывающее логические выводы, которые можно сделать из утверждения.

– Аксиомы - утверждения в логической форме (в том числе и правила), составляют описываемую онтологией теорию.

– Событие - изменение атрибутов или отношений.

Описание ПО с помощью ОП позволяет сформировать единое информационное пространство, обеспечивает полноту знаний через накопление опыта экспертов, единое понимание терминологии и структуры ПО, а также облегчает поиск информации и повышает эффективность принятия решений. Область применения, роль и типы онтологий показаны на рисунке 1.

Инструменты данного подхода используются в разных научных школах [1-5]. Известны исследования зарубежных ученых, посвященные проблемам очистки данных, извлекаемых поисковой системой из веб-страниц в сети интернет [6], систематизации и оптимизации анаэробных технологий переработки отходов [7], получения и структурирования знаний о виртуализации аппаратных сред вычислительных систем для разработки методологии классификации виртуализированных систем [8].

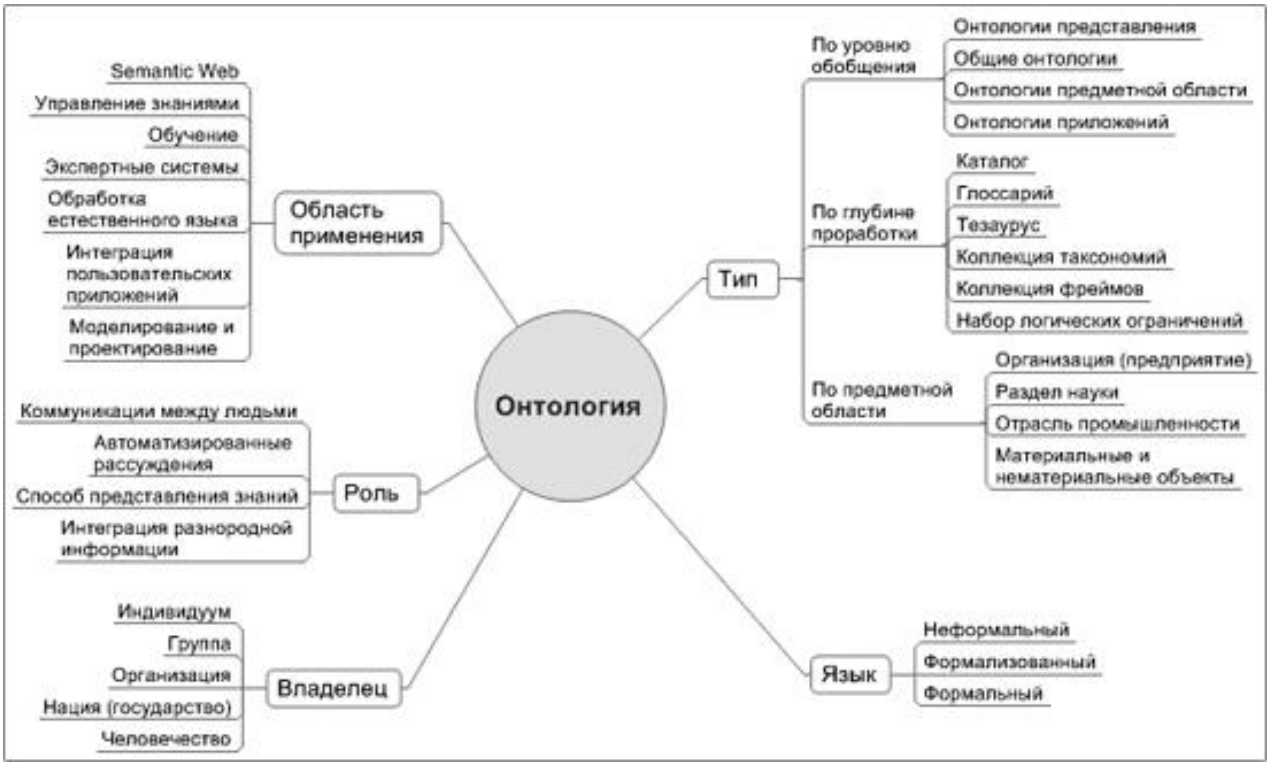


Рис. 1. Область применения, роль и типы онтологий [Ю. А. Балыбердин, лекция «Онтологический инжиниринг», МАИ]

Среди отечественных исследователей можно выделить Д.Г. Корнеева и др, исследование которых было нацелено на определение возможностей использования онтологического подхода к построению инновационных автоматизированных систем управления образованием, включающих построение индивидуальных траекторий обучения [9]. Нагоев З.В. и др. сформировали основные принципы автоматического построения онтологий интеллектуальных агентов на основе мультиагентных нейрокогнитивных архитектур, разработали мультиагентный алгоритм синтеза поведения интеллектуального агента, нацеленного на автономное формирование недостающих элементов онтологий пространственного расположения объектов и описали алгоритм формирования таких онтологий [10]. Ломов П.А. и Малоземова М.Л. предложили высокоавтоматизированную технологию пополнения онтологии с помощью обучения и последующего применения нейросетевой языковой модели для выявления потенциальных экземпляров классов онтологии из текстов предметной области [11].

Научная школа УГАТУ

Список приложений онтологического подхода в научной школе УГАТУ обширен. В [12] разработана методология построения информационной системы поддержки принятия решений (ИСППР) в процессе управления сложными объектами в критических ситуациях. В основе методологии лежит объектно-когнитивный анализ предметной области, интегрирующий методы и результаты объектно-ориентированного анализа, онтологического анализа и семантической сети представления знаний.

В [13] представлен подход к автоматизации управления сложными системами в проблемных ситуациях, предложена иерархическая структура системы, включающая базу знаний с различными моделями представления знаний на разных уровнях поддержки принятия решений, а также механизм вывода рекомендаций с использованием предметных, универсальных и метазнаний. Работа [14] посвящена этой же тематике, но концепция функционирования интеллектуальной СППР предусматривает использование Информационного банка данных наукоемких технологий Республики Башкортостан.

В [15] обсуждается проблема повышения качества принимаемых стратегических решений в управлении промышленным предприятием, на основе онтологического подхода предложено определять соответствие между методами и задачами управления и выбирать метод решения задачи управления на основе прецедентов. В соответствии с онтологическим подходом в [16, 17] рассматривается иерархическая структура знаний в области организационного управления, а также ее реализация с применением существующих методов и средств онтологического анализа и искусственного интеллекта.

Анализ процесса управления рисками технологического процесса производства пищевых продуктов позволил разработать [18, 19] его объектную и онтологическую модели и интегрировать их на базе онтологии. Разработанная гибридная онтология позволяет осуществить поиск информации с использовани-

ем различных видов запросов, а представленная модель сети Байеса оценить [19] риск в технологическом процессе.

Ряд исследований посвящено различным аспектам разработки программного обеспечения. Ученые УГАТУ предложили структуру ИСППР на основе онтологии и правил поддержки принятия решений в организационном управлении [20, 21], а также подход [22] к управлению человеческими ресурсами нацеленный на повышение качества планирования и продвижения персонала для улучшения процессов проектирования и производительности сотрудников. Работа [23] посвящена повышению эффективности проектов по разработке программного обеспечения за счет применения онтологической базы знаний, содержащей информацию о прецедентах проблемных ситуаций. Оценка эффективности СППР дается на основе прогноза выполнения проекта с учетом ограничений по расписанию, используемым ресурсам и функциональности конечного продукта. Прогноз состояния проекта на целевые даты дается на основании временных рядов его показателей. В [24] уделяется внимание совместному формированию требований к программному проекту. Предлагается использовать подход, основанный на онтологическом анализе предметной области. В [25] можно ознакомиться с применением ОП к описанию требований к СППР для оценки качества государственных услуг на этапе ее проектирования. Применение данного подхода позволяет решить проблемы отсутствия ясности, искажения требований при их изложении на естественном языке. Разработанная онтология способствует повышению эффективности взаимодействия заинтересованных лиц в процессе работы системы и ее интеграции с другими информационными ресурсами. В статье [26] обосновывается необходимость онтологического и динамического моделирования технологического процесса тестирования программного обеспечения при создании информационных систем. Целью такого моделирования является разработка базы знаний для поддержки принятия решений в возникающих в ходе разработки программного обеспече-

ния в проблемных ситуациях, требующих коллективного обсуждения в условиях ограниченных ресурсов.

Онтологический подход также нашел свое применение в вопросах надежности. В [27, 28] рассмотрена проблема определения ассоциативных отношений между причинами, характеристиками и последствиями возникновения сбоев, и правилами распознавания нештатных ситуаций на основе результатов онтологического проектирования. Распознавание нештатной ситуации осуществляется с помощью интеллектуальных методов диагностики, использующих знания, представленные в форме правил и в форме прецедентов.

Ученые университета разработали онтологию услуг для системы моментальных платежей и программное обеспечение для работы с данной онтологией в виде репозитория и модуля создания услуг. Новизна для систем моментальных платежей заключается в применении онтологий для создания единого информационного пространства для всех участников процесса оказания услуг финансового посредничества [29]. В [30] исследователи представили практическую реализацию задачи интеграции данных на примере системы управления транспортом и управления человеческими ресурсами. Авторы представили глобальную онтологию и фрагменты локальных онтологий системы управления транспортом и управления человеческими ресурсами.

В УГАТУ была разработана программа для выгрузки информации из онтологической базы знаний, реализованной с помощью редакторов онтологий на основе языка OWL (Ontolingua, OntoStudio, OilEd и Protégé), в сторонние программные продукты, ее функционал также обеспечивает загрузку файлов формата owl, визуальное представление данных и формирование базы данных [31].

Разработка, верификация и сопровождение онтологий сложный и трудоемкий процесс. Несмотря на это, область применения ОП в научной школе УГАТУ широка. Ученые университета внесли вклад в развитие управления сложными системами, в том числе в критических ситуациях, управление программными проектами и производством, обеспечение надежности, коллектив-

ное принятие решений, инновационную деятельность [32, 33], и образование [34-37].

Заключение

В статье приведен краткий обзор применения ОП в научной школе УГАТУ. Анализ публикаций показывает активное использование инструментов онтологического анализа исследователями университета. Решение различных прикладных задач с его использованием имеет давнюю историю и характеризуется хорошими результатами: была решена научно-техническая проблем разработки концептуально-технических основ, информационного и алгоритмического обеспечения поддержки принятия решений по управлению сложными динамическими объектами в условиях неопределенности с использованием инженерии знаний; повышение оперативности принятия решений в среднем на 29%, а также более высокое качество принимаемых коллективных решений при управлении взаимодействующими процессами выполнения строительных подрядных работ с помощью СППР, основанной на технологии управления знаниями в Semantic Web и разработанной на основе учеными концепции ученых УГАТУ [38].

Результаты исследований, приведенные в статье, получены в рамках выполнения грантов РФФИ 18-07-00193, 19-07-00709 и государственного задания № FEUE-2020-0007.

СПИСОК ЛИТЕРАТУРЫ

1. A free, open-source ontology editor and framework for building intelligent systems // URL: https://protege.stanford.edu/, 10.09.2021.
2. Raúl García Castro, Asuncion Gomez-Perez, York Sure-Vetter. Benchmarking the RDF(S) Interoperability of Ontology Tools // Proceedings of the Nineteenth International Conference on Software Engineering & Knowledge Engineering (SEKE'2007), Boston, Massachusetts, USA, July 9-11, 2007.
3. Prathyusha Kanakam, Raghu Varma Edarapalli, S Mahaboob Hussain. Collation of Diverse Ontology Tools // International journal of computer sciences and engineering 7(2):144-147 doi: 10.26438/ijcse/v7i2.144147.
4. Буракова Е.Е., Боргест Н.М., Коровин М.Д. Языки описания онтологий для технических предметных областей // Вестник Самарского государственного аэрокосмического университета им. академика С.П. Королёва (национального исследовательского университета). 2014. № 3 (45). С. 144-158.

5. Tobias Kuhn. Attempto Controlled English as ontology language systems // URL: https://www.researchgate.net/publication/228638589_Attempto_Controlled_English_as_ontology_language , 10.09.2021.
6. Jing Ting Wong Jer, Lang Hongjer Lang Hong. A novel ontology tool for data cleaning // Conference on uncertainty modelling in knowledge engineering and decision making (flins 2016) doi: 10.1142/9789813146976_0063.
7. Shulipa Yelyzaveta O., Yelizaveta Chernysh, Leonid Plyatsuk, Manabu Fukui. Ontological Tools in Anaerobic Fermentation Technologies: Bioinformation Database Applications // Journal of Engineering Sciences 7(1) doi: 10.21272/jes.2020.7(1).h1.
8. Florin Postolache. Ontology tool for knowledge acquisition in a virtualised ict infrastructure // Scientific Bulletin of Naval Academy 19(1) doi: 10.21279/1454-864X-16-I1-081.
9. Корнеев Д.Г., Гаспариан М.С., Микрюков А.А. Онтологический подход к моделированию инновационных процессов на примере распределенной образовательной сети вуза // Открытое образование. 2019. Т. 23. № 5. С. 4-13.
10. Нагоев З.В., Бжихатлов К.Ч., Пшенокова И.А., Нагоева О.В., Аталиков Б.А., Чеченова Н.А., Малышев Д.А. Автономный синтез пространственных онтологий в системе принятия решений мобильного робота на основе самоорганизации мультиагентной нейрокогнитивной архитектуры // Известия Кабардино-Балкарского научного центра РАН. 2020. № 6 (98). С. 68-79.
11 Ломов П.А., Малоземова М.Л. Обучение и применение нейросетевой языковой модели для пополнения онтологии // Труды Кольского научного центра РАН. 2020. Т. 11. № 8 (11). С. 38-45.
12. Черняховская Л.Р. Поддержка принятия решений при управлении сложными объектами в критических ситуациях на основе инженерии знаний: дис. д-ра техн. наук. Уфа, 2004 // URL: https://www.elibrary.ru/item.asp?id=16035580, 10.09.2021.
13. Черняховская Л.Р., Шкундина Р.А., Нугаева К. Онтологический подход к разработке систем поддержки принятия решений // Вестник Уфимского государственного авиационного технического университета. 2006. Т. 8. № 4. С. 68-77.
14. Черняховская Л.Р., Кружков В.Н., Дикова Ф.А. Онтологический подход к разработке системы поддержки принятия решений с использованием информационного банка данных наукоемких технологий Республики Башкортостан // Информационные ресурсы России. 2009. №1(107). С. 25-28.
15. Гузаиров М.Б., Черняховская Л.Р., Старцева Е.Б., Нугаева К.Р., Муксимов П.В. Информационно-аналитическая поддержка принятия решений при реализации стратегической программы развития предприятия // Мехатроника, автоматизация, управление. 2007. № 9. С. 27-32.
16. Черняховская Л.Р., Старцева Е.Б., Владимирова И.П., Малахова А.И. Управление принятием решений в организационном управлении с применением правил // Вестник Уфимского государственного авиационного технического университета. 2012. Т. 16. № 3 (48). С. 53-55.
17. Черняховская Л.Р., Федорова Н.И., Владимирова И.П. Информационная поддержка принятия решений на основе онтологического анализа аналитических моделей и методов // Информационные технологии интеллектуальной поддержки принятия решений. Proceedings of the 2nd International Conference “Information Technologies for Intelligent Decision Making Support” and the Intended International Workshop “Robots and Robotic Systems”. General Program Chair: Guzairov Murat (USATU, Ufa, Russia); General Chair Woman: Yusupova Nafisa (USATU, Ufa, Russia). 2014. С. 1-4.
18. Черняховская Л.Р., Атнабаева А.Р. Онтологический инжиниринг управления рисками в производственном процессе с целью обеспечения безопасности пищевых продуктов // Современные наукоемкие технологии. 2018. № 8. С. 161-166.
19. Гвоздев В.Е., Черняховская Л. Р., Малахова А. И., Атнабаева А. Р. Аналитическая поддержка оценки рисков на основе интегрированной онтологии производственного технологи-

ческого процесса // Информационные технологии интеллектуальной поддержки принятия решений (ITIDS'2018). Труды VI Всероссийской конференции (с приглашением зарубежных ученых). 2018. С. 18-22.
20. Черняховская Л.Р., Малахова А.И. Интеллектуальная поддержка принятия решений в организационном управлении разработкой программных проектов // Вестник Уфимского государственного авиационного технического университета. 2013. Т. 17. № 5 (58). С. 195-199.
21. Черняховская Л.Р., Малахова А.И. Разработка моделей и методов интеллектуальной поддержки принятия решений на основе онтологии организационного управления программными проектами // Онтология проектирования. 2013. № 4 (10). С. 42-52.
22. Гвоздев В.Е., Черняховская Л.Р., Мухаметьянова Р.И., Владимирова И.П. Стратегическое управление проектами на основе прогнозирования эффективности персонала организации с использованием интеллектуального анализа данных // Проблемы управления и моделирования в сложных системах. Труды XIX Международной конференции. Под редакцией Е.А. Федосова, Н.А. Кузнецова, В.А. Виттиха. 2017. С. 399-403.
23. Черняховская Л.Р., Никулина Н.О., Бармина О.В. Оценка эффективности поддержки принятия решений при реализации проекта по разработке программного обеспечения // Информационные технологии интеллектуальной поддержки принятия решений (ITIDS'2018). Труды VI Всероссийской конференции (с приглашением зарубежных ученых). 2018. С. 16-22.
24. Гвоздев В.Е., Черняховская Л.Р., Малахова А.И., Ровнейко Н.И. Интеллектуально-аналитическая поддержка принятия коллективных решений при управлении программными проектами // Проблемы управления и моделирования в сложных системах. Труды XVI Международной конференции. Институт проблем управления сложными системами, Самарский научный центр Российской академии наук; Под ред.: Е.А. Федосова, Н.А. Кузнецова, В.А. Виттиха. 2014. С. 204-212.
25. Chernyakhovskaya L.R., Galiullina A.F. Development of requirements for a decision support system aimed at quality assessment of public services provided based on the ontological approach // Biznes-informatika. 2017. № 1 (39). С. 36-47.
26. Черняховская Л.Р., Никулина Н.О., Малахова А.И., Гайткулов Р.Т. Моделирование технологического процесса тестирования программного обеспечения для представления и обработки знаний в области диагностики ошибок // Информационные и математические технологии в науке и управлении. 2018. № 2 (10). С. 52-60.
27. Черняховская Л.Р., Никулина Н.О., Федорова Н.И., Малахова А.И. Разработка системы диагностических знаний с использованием интеллектуального анализа данных // Проблемы управления и моделирования в сложных системах. Труды XIX Международной конференции. Под редакцией Е.А. Федосова, Н.А. Кузнецова, В.А. Виттиха. 2017. С. 519-525.
28. Черняховская Л.Р., Никулина Н.О., Давлиева А.С. Интеллектуальные методы диагностики и прогнозирования состояний сложных технических систем на основе онтологической модели // Информационные технологии интеллектуальной поддержки принятия решений. Труды V Всероссийской конференции (с приглашением зарубежных ученых). 2017. С. 83-86.
29. Котельников В.А., Богданова Д.Р., Юсупова Н.И. Онтологический репозиторий услуг системы моментальных платежей // Онтология проектирования. 2019. Т. 9. № 3 (33). С. 333-344.
30. Юсупова Н.И., Сметанина О.Н., Рассадникова Е.Ю. Методы и средства онтологического инжиниринга в системах поддержки принятия решений транспортного менеджмента // Проблемы управления и моделирования в сложных системах. Труды XX Международной конференции. Под редакцией Е.А. Федосова, Н.А. Кузнецова, С.Ю. Боровика. 2018. С. 396-401.
31. Сметанина О.Н., Климова А.В., Кириллов О.Ю. Knowledgebase to database (KBTODB) // Свидетельство о регистрации программы для ЭВМ RU 2017618612, 04.08.2017. Заявка № 2017615537 от 06.06.2017.

32. Черняховская Л.Р., Васильев В.И., Гвоздев В.Е., Никулина Н.О., Малахова А.И., Вульфин А.М., Бежаева О.Я. Методы и модели поддержки принятия решений при управлении инновационными проектами в производственно-экономических системах. Москва, 2021.
33. Черняховская Л.Р., Никулина Н.О., Низамутдинов М.М., Малахова А.И., Мухаметьянова Р.И. Методическое обеспечение интеллектуального анализа характеристик инновационной деятельности // Современные наукоемкие технологии. 2020. № 11-2. С. 313-319.
34. Пудалова Е.И., Черняховская Л.Р. Разработка корпоративного образовательного портала с применением онтологического инжиниринга // XII всероссийское совещание по проблемам управления ВСПУ-2014. Институт проблем управления им. В.А. Трапезникова РАН. 2014. С. 9469-9473.
35. Черняховская Л.Р., Салаватова А.Р. Модель управления качеством дополнительного профессионального обучения на основе онтологического анализа // Proceedings of the 2nd International Conference. 2014. С. 171-175.
36. Давлетбаева А.Р., Черняховская Л.Р. Применение моделей и методов интеллектуальной поддержки принятия решений для обеспечения результативности процесса дистанционного обучения // Информационные технологии и системы. Труды Четвертой Международной научной конференции. Ответственные редакторы: Ю.С. Попков, А.В. Мельников. 2015. С. 84-86.
37. Юсупова Н.И., Сметанина О.Н., Климова А.В. Организация информационной поддержки принятия решений при управлении образовательным маршрутом на основе онтологии // Информационные технологии и системы. Труды Четвертой Международной научной конференции. Ответственные редакторы: Ю.С. Попков, А.В. Мельников. 2015. С. 109-111.
38. Низамутдинова Р.И. Система поддержки принятия коллективных решений при управлении взаимодействующими деловыми процессами в промышленности: дис. к.т.н. Уфа, 2011 // URL: https://www.dissercat.com/content/sistema-podderzhki-prinyatiya-kollektivnykh-reshenii-pri-upravlenii-vzaimodeistvuyushchimi-d/, 10.09.2021.

УДК 004.021

Д. А. ПОЛОНСКИЙ, А. О. ФЕДОСОВА
kHRYSTALq@gmail.com, fedos_anastasiya@bk.ru
Науч. руководов. – канд. техн. наук, доц. Р. В. НАСЫРОВ

Уфимский государственный авиационный технический университет

ПРЕДОБРАБОТКА ТЕКСТА ДЛЯ РЕШЕНИЯ NLP (NATURAL LANGUAGE PROCESSING)

Аннотация. Рассматриваются методы предварительной обработки текста для дальнейшей работы с алгоритмами машинного обучения.
Ключевые слова: предобработка; NLP; natural language processing; токенизация; стоп-слова; лемматизация; стемминг.

Предобработка текста переводит текст на естественном языке в формат удобный для дальнейшей работы. Предобработка состоит из различных этапов, которые могут отличаться в зависимости от задачи и реализации.

Как правило, первым шагом обработки текста является нормализация. Эта операция, в результате которой тексты приводятся к нужному регистру, удаляются знаки пунктуации (обычно реализуется как удаление из текста символов из заранее заданного набора), удаляются числа (или приводятся к другому формату), удаляются пробельные символы. Нормализация необходима для унификации методов обработки текста [1].

Следующим шагом является токенизация, которая заключается в разбиении длинных строк на более короткие. Обычно используется токенизация по словам.

В случае разбиений на предложения нужно просто найти точку, вопросительный или восклицательный знак. Но в русском языке существует сокращения, в которых есть точка, например, *к.т.н.* – кандидат технических наук или *т.е.* – то есть. Вследствие этого могут возникать ошибки, но Python-библиотека NLTK позволяет избежать этой проблемы.

Рассмотрим пример:

```
>>> from nltk.tokenize import sent_tokenize
```

>>> text = "Мой научный руководитель – доцент и к.т.н., т.е. он имеет множество публикаций. А также грантов и научных проектов."

>>> sent_tokenize(text, language="russian")

[' Мой научный руководитель – доцент и к.т.н., т.е. он имеет множество публикаций.', ' А также грантов и научных проектов.']

Функция *sent_tokenize* разбила исходное предложения на два, несмотря на присутствие слов к.т.н. и т.е.

Помимо разбиения на предложения в NLTK можно в качестве токенов использовать слова:

>>> from nltk.tokenize import sent_tokenize, word_tokenize

>>> text = "Мой куратор тоже к.т.н. По образованию он инженер-проектировщик."

>>> word_tokenize(text, language="russian")

['Мой ', 'куратор ', 'тоже', 'к.т.н.', '.', 'По', 'образованию', 'он' 'инженер-проектировщик', '.']

Здесь к.т.н. и инженер-проектировщик были определены как отдельные слова.

После токенизации важным шагом является удаление стоп-слов. Стоп-слова – это слова, которые не несут смысловой нагрузки. В русском языке, например: союзы, предлоги [1].

Библиотека NLTK также имеет список стоп-слов, всего в него входит 151 слово. Некоторые из них: и, в, во, не, что, он, на, я, с, со, как, а, то, все, чтоб, без, будто, впрочем, хорошо, перед, иногда, лучше, чуть, том, нельзя, такой, им, более, всегда, конечно, всю, между.

Поскольку это список, то к нему можно добавить дополнительные слова или, наоборот, удалить из него те, которые будут информативными для вашего случая. Например, для последующего исключения слов из токенизированного текста можно написать следующее:

for token in tokens:

```
    if token not in stop_words:
        filtered_tokens.append(token)
```

Следующим шагом является стемминг. Количество корректных словоформ, значения которых схожи, но написания отличаются суффиксами, приставками, окончаниями и прочим, очень велико, что усложняет создание словарей и дальнейшую обработку [2]. Стемминг позволяет привести слово к его основной форме. Суть подхода в нахождении основы слова, для этого с конца и начала слова последовательно отрезаются его части. Правила отсекания для стеммера создаются заранее, и чаще всего представляют из себя регулярные выражения. В Python-библиотеке NLTK для этого есть *SnowballStemmer*, который поддерживает русский язык:

```
>>> from nltk.stem import SnowballStemmer
...
>>> snowball = SnowballStemmer(language="russian")
>>> snowball.stem("Хороший")
хорош
>>> snowball.stem("Хорошая")
хорош
```

Проблемы возникают со словами, которые значительно изменяются в других формах:

```
>>> snowball.stem("Хочу")
хоч
>>> snowball.stem("Хотеть")
хотет
```

В этом случае, следует использовать лемматизацию, так как "хочу" и "хотеть" – грамматические формы одного и того же слова.

Лемматизация является альтернативой стемминга [2]. Основная идея в приведении слова к словарной форме — лемме.

Например, для русского языка:

для существительных — именительный падеж, единственное число;

для прилагательных — именительный падеж, единственное число, мужской род;

для глаголов, причастий, деепричастий — глагол в инфинитиве несовершенного вида.

Отличие в том, что стеммер действует без знания контекста и, соответственно, не понимает разницу между словами, которые имеют разный смысл в зависимости от части речи. Однако у стеммеров есть и свои преимущества: их проще внедрить, они работают быстрее.

Например, *хочу, хотят, хотели* имеют начальную форму *хотеть*. В этом случае можем воспользоваться pymorphy2 – инструмент для морфологического анализа русского и украинского языков.

```
>>> import pymorphy2
>>> morph = pymorphy2.MorphAnalyzer()
>>> morph.parse("хочу")
```

[Parse(word='хочу', tag=OpencorporaTag('VERB,impf,tran sing,1per,pres,indc'), normal_form='хотеть', score=1.0, methods_stack=((<DictionaryAnalyzer>, 'хочу', 2999, 1),))]

Метод parse возвращает список объектов Parse, которые обозначают виды грамматических форм анализируемого слова. Такой объект обладает следующими атрибутами:

- *tag* обозначает набор граммем. В данном случае слово хочу – это глагол (VERB) несовершенного вида (impf), переходный (tran), единственного числа (sing), 1 лица (1per), настоящего времени (pres), изъявительного наклонения (indc);

- *normal_form* – нормального форма слова;

- *score* – оценка вероятности того, что данный разбор правильный;

- *methods_stack* – тип словаря распарсенного слова с его индексом.

По умолчанию объекты Parse сортированы в порядке убывания значения score. Поэтому из списка лучше всего брать 1-й элемент:

```
>>> morph.parse("хотеть")[0].normal_form
хотеть
>>> morph.parse("хочу")[0].normal_form
хотеть
>>> morph.parse("хотят")[0].normal_form
хотеть
```

Следовательно, мы получили одно слово из разных его форм.

Векторизация. Большинство математических моделей работают в векторных пространствах больших размерностей, поэтому необходимо отобразить текст в векторном пространстве. Основным подходом является мешок слов: для документа формируется вектор размерности словаря, для каждого слова выделяется своя размерность, для документа записывается признак насколько часто слово встречается в нем, получаем вектор. Наиболее распространенным методом для вычисления признака является TF-IDF (TF — частота слова, term frequency, IDF — обратная частота документа, inverse document frequency). TF вычисляется, как счетчиком вхождения слова. IDF обычно вычисляют как логарифм от числа документов в корпусе, разделенный на количество документов, где это слово представлено. Таким образом, если какое-то слово встретилось во всех документах корпуса, то такое слово не будет никуда добавлено.

СПИСОК ЛИТЕРАТУРЫ

1. Васильев, Ю.А. Обработка естественного языка. Python и spaCy на практике [Текст] / Ю.А. Васильев. – Санкт-Петербург: Питер, 2021. – 256 с.
2. Хобсон, Л. Обработка естественного языка в действии [Текст] / Л. Хобсон, Х. Ханнес, Х. Коул. – Санкт-Петербург: Питер, 2020 – 576 с.

УДК 004.657

Ю. М. ШАРИПОВА
jjuulliiyyee@gmail.com
Науч. руководв. – канд. техн. наук, проф. Г. Р. ШАХМАМЕТОВА

Уфимский государственный авиационный технический университет

ПРИМЕНЕНИЕ МЕТОДОВ МАШИННОГО ОБУЧЕНИЯ ДЛЯ ПОИСКА ПОТЕНЦИАЛЬНЫХ ПАТОГЕННЫХ МУТАЦИЙ В ГЕНОМЕ ЧЕЛОВЕКА

Аннотация. В статье проводится анализ проблемы применения методов машинного обучения для поиска потенциальных патогенных мутаций в геноме человека, актуальности рассматриваемой тематики, современного состояния проблемы в области применения методов машинного обучения для поиска потенциальных патогенных мутаций. Изучены аспекты решаемой проблемы, выявленные при анализе и структурировании собранных научных статей в виде решаемых задач, подходов, моделей и методов, используемых информационных технологий, инструментальных средств и программных решений проблемы.
***Ключевые слова*:** машинное обучение; медицина; геномные данные.

Введение

Машинное обучение — альтернативный подход к прогнозированию и классификации, способный решать проблемы гибким в вычислительном отношении способом. Поэтому *машинное обучение* используют очень активно, находя все больше областей для его применения.

Сегодня в обработке биомедицинских данных используются почти все виды *машинного обучения*: обучение с учителем, без учителя, с частичным привлечением учителя, с подкреплением. Наиболее активно *машинное обучение* в медицине используют для решения проблем, связанных с диагностикой заболеваний. Эти задачи относят к обучению с учителем или с частичным привлечением учителя. Кроме того, *машинное обучение* активно применяется в персонализированной медицине и для генерации данных различных исследований для анонимизации данных пациентов. В этих задачах сейчас все больше применяют обучение с подкреплением и обучение без учителя, в частности, генеративные состязательные сети. *Машинное обучение* в медицине начали изучать еще в 2000-х, и оно продолжает активно развиваться и в наши дни.

Одной из областей биологии, в которой востребованы методы *машинного обучения*, является *геномика*, — направление биологии, исследующее структуру и функцию нуклеотидных последовательностей геномов живых организмов в широком смысле. В тот момент, когда число параметров биологической системы и их комбинаций становится столь большим, что исключает возможность тестирования роли каждой из них простым перебором, мы входим в область применения методов *машинного обучения*.

В данной работе на основе научных публикаций проведен анализ применения существующих на сегодняшний день методов *машинного обучения*, используемых при работе с *геномными данными*.

Современное состояние проблемы

Список изученных статей открывает обзор [1], рассказывающий о нескольких алгоритмах *машинного обучения* и примеры их практического применения для решения задач генетики и *геномики*.

В следующей же работе [2] представлен краткий обзор некоторых решений, основанных на машинном обучении, применяемых для повышения качества анализа и преобразования результатов отдельных этапов секвенирования. Описаны ключевые группы биоинформатических задач в рамках секвенирования, приведены примеры реализованных алгоритмов с использованием *машинного обучения*. Кроме того, разработаны различные подходы к решению одной и той же задачи, при этом имеющие свои преимущества и недостатки.

Авторы статьи [3] кратко описывают современные методы анализа *геномных* и феномных данных в области психиатрии с использованием *машинного обучения*, а также обозначены возможные перспективы и существующие ограничения этого подхода.

В модели, представленной в работе [4], используется метод опорных векторов для поиска оптимального подмножества классификации локусов, а после - искусственная нейронная сеть (ИНС) для классификации пациентов по лихо-

радке денге. Предложенный метод классификации использует только маркеры генома.

Статья [5] посвящена разработке вычислительного подхода, в котором использовались данные нескольких общеклеточных фенотипических высокопроизводительных скринингов. Была создана база данных Pathway Genome. Кроме того, были разработаны байесовские модели *машинного обучения*, которые использовались для виртуального скрининга библиотек соединений.

Подход *машинного обучения* для классификации подтипов рака почки с использованием *геномных данных* предлагается в работе [6]. Созданная рекуррентная нейронная сеть применяется для классификации данного образца микроРНК на подтипы рака почки. Также используется алгоритм LSTM для группировки микроРНК.

В следующем представленном обзоре [7] описываются ключевые аспекты *машинного обучения*, подчеркивающие его практичность для аннотации генома, с иллюстративными примерами из ENCODE.

Геномные данные в качестве предикторов для выявления новых генов риска появления аутизма применяются в статье [8]. Задействованными методами становятся метод ансамбля, иначе forecASD, и классификатор Random forest.

В работе [9] производится мета-анализ семи больших наборов данных для прогнозирования фенотип-устойчивости по генотипу. Используются методы *машинного обучения* и алгоритмы SCM и RF.

Авторами статьи [10] *геномные данные* анализируются с помощью набора методов *машинного обучения*: штрафной логистической регрессии (LR), деревьев с градиентным усилением (GBT) и искусственной нейронной сети (NN). Кроме того, показателем, использованным для сравнения методов, была статистика площади под кривой ROC (AUC).

Преимущества и недостатки применения различных методов на конкретных наборах данных выявляются в работе [11]. Авторами поясняется, что кон-

тролируемое *машинное обучение* может повысить реальную ценность интерпретации бактериальных *геномных данных*, поскольку оно может обеспечить вероятностные результаты для важных фенотипов, чего очень трудно достичь с помощью других методов.

В обзоре [12] описываются доступные базы *геномных данных* и инструменты для их анализа, подробно рассматриваются алгоритмы *машинного обучения* и искуственная нейронная сеть. Наконец, авторы статьи указывают на проблемы *геномных данных* и *машинного обучения*, предоставляя прогноз будущих исследований.

Следующей работой представлен обзор [13] применения *машинного обучения* для анализа наборов данных секвенирования генома. Описываются проблемы в применении контролируемых, частично контролируемых и неконтролируемых методов *машинного обучения*, а также генеративного и дискриминативного подходов к моделированию. Наконец, приведены общие рекомендации, которые помогут выбрать определенные методы *машинного обучения* для их практического применения в анализе наборов генетических и *геномных данных*.

Ключевой задачей исследования [14] является восстановление метаболической сети организма на основе его геномной последовательности. Для этого используются: наивный байесовский метод, деревья решений, логистическая регрессия и алгоритм PathoLogic.

В статье [15] производится анализ сложных биологических данных с использованием *машинного обучения* и нейронной сети.

Применение *машинного обучения* в реконструкции и анализе метаболических моделей в масштабе генома с целью повышения их качества описывается в работе [16].

Исследование, приведенное в статье [17], демонстрирует многообещающий путь интеграции конвейера фенотипирования в геномное прогнозирование

и обеспечивает систематическую основу, предоставляющую надежное и быстрое фенотипирование с помощью наземных систем.

Машинное обучение применяется для сжатия данных митохондриального генома человека и в работе [18]. Кроме того, используется сверточная нейронная сеть и сеть долговременной краткосрочной памяти.

Авторами статьи [19] производится обзор непараметрических методов и методов *машинного обучения*, используемых в полногеномном прогнозировании, обсуждается их сходство, а также связь с некоторыми хорошо известными параметрическими подходами.

Целью работы [20] стало изучение комплексного подхода к машинному обучению и общегеномному анализу, нацеленного на прогнозирование вероятности появления большого депрессивного расстройства (БДР), используя *геномные данные* людей. Среди задействованных средств можно выделить методы *машинного обучения* и классификатор Random forest.

Заключение

Основное преимущество *машинного обучения* заключается в возможности генерирования и проверки множества гипотез на основе больших наборов, при обработке и анализе биомедицинских данных методами машинного обучения необходимо учитывать их специфику, особенно актуально это для генетических данных. Учитывая, насколько интенсивно развивается эта область, можно ожидать, что в ближайшее время использование подходов *машинного обучения* при обработке биомедицинских данных будет активно расширяться.

СПИСОК ЛИТЕРАТУРЫ

1. Таскина А.К., Муравьева А. А., Ельсукова А. С., Фишман В. С. МЕТОДЫ МАШИННОГО ОБУЧЕНИЯ В БИОЛОГИИ// Природа 2020. №9(1261). URL: https://www.elibrary.ru/item.asp?id=44061158
2. Смагин В. Д., Русакович А.Н. ПРИМЕНЕНИЕ МЕТОДОВ МАШИННОГО ОБУЧЕНИЯ В ЗАДАЧЕ СЕКВЕНИРОВАНИЯ ГЕНОМА// Системный анализ в науке и образовании 2021. №1. URL: https://www.elibrary.ru/item.asp?id=46254968
3. Нургалиев Т. И. ВНЕДРЕНИЕ АЛГОРИТМОВ МАШИННОГО ОБУЧЕНИЯ В АНАЛИЗ ГЕНОМНЫХ И ФЕНОМНЫХ ДАННЫХ В ОБЛАСТИ ПСИХИАТРИИ// Обозрение психиатрии и медицинской психологии имени В. М. Бехтерева 2019. №4–1. URL: https://www.elibrary.ru/item.asp?id=41419083

4. Caio Davi, Andre´ Pastor, Thiego Oliveira, Fernando B. de Lima Neto, Ulisses Braga-Neto, Abigail W. Bigham, Michael Bamshad, Ernesto T. A. Marques, Bartolomeu Acioli-Santos Severe Dengue Prognosis Using Human Genome Data and Machine Learning// IEEE Transactions on Biomedical Engineering (Volume: 66, Issue: 10, Oct. 2019). URL: https://ieeexplore.ieee.org/abstract/document/8633395
5. Ekins S, Lage de Siqueira-Neto J, McCall L-I, Sarker M, Yadav M, Ponder EL, et al. (2015) Machine Learning Models and Pathway Genome Data Base for Trypanosoma cruzi Drug Discovery// PLoS Negl Trop Dis 9(6): e0003878. doi:10.1371/ journal.pntd.0003878
6. Muhamed Ali, Ali, Hanqi Zhuang, Ali Ibrahim, Oneeb Rehman, Michelle Huang, and Andrew Wu. 2018. "A Machine Learning Approach for the Classification of Kidney Cancer Subtypes Using MiRNA Genome Data"// Applied Sciences 8, no. 12: 2422. https://doi.org/10.3390/app8122422
7. Yip, K.Y., Cheng, C. & Gerstein, M. Machine learning and genome annotation: a match meant to be? // Genome Biol 14, 205 (2013). https://doi.org/10.1186/gb-2013-14-5-205
8. Brueggeman, L., Koomar, T. & Michaelson, J.J. Forecasting risk gene discovery in autism with machine learning and genome-scale data. // Sci Rep 10, 4569 (2020). https://doi.org/10.1038/s41598-020-61288-5
9. Hicks AL, Wheeler N, Sánchez-Busó L, Rakeman JL, Harris SR, et al. (2019) Evaluation of parameters affecting performance and reliability of machine learning-based antibiotic susceptibility testing from whole genome sequencing data. //PLOS Computational Biology 15(9): e1007349. https://doi.org/10.1371/journal.pcbi.1007349
10. Romagnoni, A., Jégou, S., Van Steen, K. et al. Comparative performances of machine learning methods for classifying Crohn Disease patients using genome-wide genotyping data. //Sci Rep 9, 10351 (2019). https://doi.org/10.1038/s41598-019-46649-z
11. Nadejda Lupolova, Samantha J. Lycett, David L. Gally A guide to machine learning for bacterial host attribution using genome sequence data //Microb Genom. 2019 Dec; 5(12): e000317. Published online 2019 Nov 28. https://doi.org/10.1099/mgen.0.000317
12. Yingli Liu, Chen Niu, Zhuo Wang, Yong Gan, Yan Zhu, Shuhong Sun, Tao Shen,Machine learning in materials genome initiative: A review//Journal of Materials Science & Technology, Volume 57, 2020, Pages 113-122, ISSN 1005-0302 https://doi.org/10.1016/j.jmst.2020.01.067
13. Libbrecht, M., Noble, W. Machine learning applications in genetics and genomics. //Nat Rev Genet 16, 321–332 (2015). https://doi.org/10.1038/nrg3920
14. Dale, J.M., Popescu, L. & Karp, P.D. Machine learning methods for metabolic pathway prediction. //BMC Bioinformatics 11, 15 (2010). https://doi.org/10.1186/1471-2105-11-15
15. Xu, C., Jackson, S.A. Machine learning and complex biological data. //Genome Biol 20, 76 (2019). https://doi.org/10.1186/s13059-019-1689-0
16. Yeji Kim, Gi Bae Kim, Sang Yup Lee, Machine learning applications in genome-scale metabolic modeling//Current Opinion in Systems Biology, Volume 25, 2021, Pages 42-49, ISSN 2452-3100,https://doi.org/10.1016/j.coisb.2021.03.001
17. Zhang, J., Naik, H., Assefa, T. et al. Computer vision and machine learning for robust phenotyping in genome-wide studies. //Sci Rep 7, 44048 (2017). https://doi.org/10.1038/srep44048
18. Wang, R., Zang, T. & Wang, Y. Human mitochondrial genome compression using machine learning techniques. //Hum Genomics 13, 49 (2019). https://doi.org/10.1186/s40246-019-0225-3
19. Oscar González-Recio, Guilherme J.M. Rosa, Daniel Gianola Machine learning methods and predictive ability metrics for genome-wide prediction of complex traits //Livestock Science, Volume 166, 2014, Pages 217-231, ISSN 1871-1413, https://doi.org/10.1016/j.livsci.2014.05.036
20. Lin, E.; Kuo, P.-H.; Lin,W. -Y.; Liu, Y.-L.; Yang, A.C.; Tsai, S.-J. Prediction of Probable Major Depressive Disorder in the Taiwan Biobank: An Integrated Machine Learning and Genome-Wide Analysis Approach. //J. Pers. Med. 2021, 11, 597. https://doi.org/10.3390/jpm11070597

УДК 004.657

В. О. ЯКОВЛЕВ
vasya_anime@mail.ru
Науч. руководитель – канд. техн. наук, проф. Г. Р. ШАХМАМЕТОВА

Уфимский государственный авиационный технический университет

АНАЛИЗ СОВРЕМЕННОГО СОСТОЯНИЯ ИССЛЕДОВАНИЙ В ОБЛАСТИ РАСПОЗНАВАНИЯ СНИМКОВ ФУНКЦИОНАЛЬНОЙ ДИАГНОСТИКИ ЛЕГКИХ

Аннотация. В статье приводится анализ проблемы распознавания снимков функциональной диагностики, актуальности рассматриваемой тематики, современного состояния проблемы в области распознавания снимков функциональной диагностики. Отмечены аспекты решаемой проблемы, выявленные при анализе и структурировании собранных научных статей в виде решаемых задач, подходов, моделей и методов, используемых информационных технологий, инструментальных средств и программных решений проблемы
***Ключевые слова*:** распознавание снимков; функциональная диагностика;

Введение

Внезапная вспышка и распространение вируса COVID-19 в 2020 году послужили толчком для решения ряда биомедицинских задач, в том числе проблемы распознавания снимков функциональной диагностики. Функциональная диагностика представляет собой раздел диагностики, содержанием которого являются объективная оценка, обнаружение отклонений и установление степени нарушений функции различных органов и физиологических систем организма на основе измерения физических, химических или иных объективных показателей их деятельности с помощью инструментальных или лабораторных методов исследования.

Развитие алгоритмов машинного обучения предоставляет широкие возможности в области автоматизации решения биомедицинских задач. Компьютерная обработка биомедицинских изображений повышает точность анализа изображений, снижает роль человеческого фактора при принятии решений, позволяет оценить эффективность применения терапии и в целом улучшает качество жизни людей. Активно развиваются биомедицинские исследования в

области анализа и распознавания изображений, полученных при функциональной диагностике.

В данной работе на основе научных публикаций проведен анализ применения существующих на сегодняшний день методов для распознавания снимков функциональной диагностики.

Современное состояние проблемы

В [1] отмечено, что технологии, основанные на искусственном интеллекте (ИИ), включая машинное обучение, распознавание изображений и алгоритмы глубокого обучения, могут быть использованы для раннего обнаружения и диагностики инфекции COVID-19.

Описана алгоритмизация процесса распознавания состояний на основе специальных рентгеновских изображений в [2]. Предложен метод нейросетевого анализа. Для этого была реализована нейронная сеть, которая имеет возможность самообучаться. Использовались методы опорных векторов и дискриминантный анализ для сведения к минимуму вероятности ошибки экспертной системы.

Рассмотрены различные подходы машинного обучения в [3], используемые при прогнозировании распространения заболеваемости, и прогнозировании состояния пациентов при вирусе COVID-19. Отмечается, что в последние годы анализ медицинских изображений является одним из наиболее перспективных направлений исследования. Описываются наиболее широко известные алгоритмы для машинного обучения – случайный лес (Random Forest, RF) и машина опорных векторов (SVM); для глубокого обучения - сверточная нейронная сеть (CNN), длинная кратковременная память (LSTM), генеративные состязательные сети (GAN), остаточная нейронная сеть (Residual Neuralnetwork, ResNet), автоенкодер. Также отмечается, что были использованы математические и статистические модели при оценке человеческих потерь, а также в прогнозировании общего количества смертей до определенного периода или конца пандемии.

В [4] говорится о том, что для распознавания пневмонии, вызванной различными вирусами, широко применяется компьютерная томография с анализом полученных изображений методами глубокого обучения. Однако отмечается, что рентгенологическая диагностика, хотя и обладает меньше разрешающей способностью, является более распространенной из-за большей доступности рентгеновских аппаратов. Также отмечается, что в настоящее время появляются работы, в которых предлагается использовать нейронные сети, для обнаружения COVID-19 на основе анализа рентгенографических изображений (РИ). Описывается обучение сверточной нейронной сети на РИ, а также ее структура.

В [5] описывается процесс выявления патологических изменений в легких на основе совместного анализа радиологических отчетов и томографических изображений. Сравниваются подходы к автоматизации выделения области интереса на изображениях компьютерной томографии легких. Говорится, что метод Оцу позволяет выделить область легкого с достаточной степенью достоверности, а использование для этой задачи сверточных нейронных сетей не вполне оправдано. Также качестве альтернативы предлагается использовать технологию выделения областей интереса, которая основана на оптимизации критерия качества последующей классификации изображений компьютерной томографии легких. Сделан вывод, что повышение качества автоматической диагностики по цифровым изображениям за счет использования радиологических отчетов является крайне актуальной задачей.

Автор в [6] рассматривает проблемы и методы машинной классификации и распознавания рентгеновских снимков (CXR), а также вопросы совершенствования искусственных НС, которые используются для повышения качества классификации рентгенологических синдромов. Отмечается, что НС идеальны для распознавания заболеваний с использованием сканирования, поскольку нет необходимости предоставлять конкретный алгоритм для определения заболевания. Установлено, что современные методы обнаружения аномалий (болезней) в CXR имеют сложности с недостаточным количеством учебных данных, стан-

дартизации изображений и предварительной сегментацией учебного набора. Сформированы конкретные способы решения описанных проблем, с которыми сталкиваются НС при анализе данных. В качестве решения предложено использование методов глубоко обучения, а именно сверточных НС на основе обратного распространения ошибки и градиентного спуска с предварительной сегментацией тренировочной выборки и применения трансферного обучения для категоризации болезней на медицинских изображениях. Разработана архитектура интеллектуальной системы, которая имеет возможность распознавать аномалии в CXR на уровне врачей и рентгенологов используя среду глубинного обучения. Сделан вывод, что несмотря на многообещающие результаты интеллектуальных систем, серьезные проблемы остаются, особенно в том, что касается теоретической основы, которая бы четко объяснила способы определения оптимального выбора модели, типа и структуры для конкретной задачи или для глубокого понимания причин, по которым конкретная архитектура или алгоритм эффективны в этой задаче.

В [7] описывается идея, которая основана на методах поиска особых точек, которые применяются при распознавании лиц, сравнении изображений и т. д. Для ее реализации использовали один из методов компьютерного зрения - метод SURF (Speeded Up Robust Features). Метод SURF применяется для поиска характерных точек изображения. На выходе получается рентгеновское изображение с отмеченными на нем областями возможных патологий. Однако отмечается, что при всех достоинствах метода основной проблемой является его точность, здесь подразумевается не точность обнаружения патологии, а точность совпадения характерных точек.

Описано построение модели машинного обучения с помощью платформы ML.NET Model Builder в [8]. Отмечается, что для решения задачи распознавания, наиболее оптимальной оказалась модель глубинной нейронной сети (DNN – Deep Neural Network).

В [9] утверждается, что бурное развитие систем диагностики рака легкого на основе данных КТ обусловлено созданием сверхточных нейронных сетей (СНС). Описываются этапы процедуры обнаружения новообразований в легких на основе изображений КТ: сбор данных, предварительная обработка изображения, сегментация, обнаружение образований, сокращение числа ложноположительных случаев, классификация новообразований. Приведены примеры разработанных в настоящее время полностью автоматизированных систем диагностики рака легкого: Deep Lung и Nodule X. Сделаны выводы, что выступая в роли помощника, ИИ позволит диагносту принимать более обоснованные решения, избавит его от множества рутинных дел.

В [10] рассматривается процесс обучения нейросети (глубокая сверхточная нейросеть), архитектура разработанного модуля (Программный модуль представляет собой нейросеть глубокого обучения, построенную по технологии сверточной нейронной сети CNN), алгоритм его работы и структура нейросети, лежащей в его основе и анализирующей снимки. Приведены результаты вычислительных экспериментов по использованию модели для анализа реальной выборки данных. Сделан вывод, что проведенные эксперименты подтвердили перспективность использования нейросети для решения задачи машинного автоматического анализа флюорографических рентгеновских снимков на предмет выявления патологий. При этом повышение уровня доверия к сети уменьшает количество ошибок, но снижается эффективность использования системы. Подчеркивается, что для улучшения характеристик системы – уменьшения количества ошибок и повышения КПД – целесообразно использовать базу снимков большего размера для обучения нейросети

В [11] описан опыт решения задач по автоматизированной диагностике заболеваний органов грудной полости современными методами глубокого обучения. Для решения задачи обнаружения пневмонии по рентгеновским изображениям, были использованы две нейросетевых модели: RetinaNet и Mask R-CNN. В основе этих сетей использваны классические сверхточные нейронные

сети с “остаточными соединениями” (residual connections) - ResNet-50 и ResNet-101. Сделаны выводы, что удалось достичь показателей точности на уровне или даже превосходящих результаты опубликованных решений.

В [12] целью является проверка того, можно ли построить надежный классификатор на основе технологий глубокого обучения с помощью предварительно обученной глубокой сверточной нейронной сети, дообученной на сравнительно небольшом объеме данных, а также сравнить различные варианты предварительно обученных нейронных сетей на базе: DenseNet, EfficientNet, InceptionResNetV2, InceptionV3, MobileNet, MobileNetV2, MobileNetV3, NASNet, ResNet, ResNetV2, VGG, Xception. В данной работе классификация выполнялась по двум классам COVID-19 и норма, исходя из имеющихся в настоящее время в распоряжении авторов объема исходных данных для обучения. При этом, остальные возможные классы, например, пневмония, туберкулез и т.д. в настоящем исследовании не учитываются. Было проведено сравнение нейросетей и выявлены наиболее эффективные из них: DenseNet169, NASNetLarge, ResNet152V2.

[13] посвящена исследованию метода Transfer Learning при распознавании COVID-19 на рентгеновских снимках. Решается задача классификации изображений по 3 меткам: здоров, пневмония, COVID-19. В статье рассмотрен сбор данных, их предварительная подготовка и очистка, создание модели нейронной сети, еѐ обучение и анализ результатов. Использовалась сверточная нейронная сеть. Суть метода заключается в том, что используется нейронная сеть, предобученная классифицировать другие данные. Затем остается дообучить еѐ на собранном датасете. После чего сеть будет показывать хороший результат даже в случае небольшой обучающей выборки. В результате модель показала точность 85-89 процентов на тестовой выборке, что является хорошим показателем. При увеличении размеров тестового датасета возможно улучшение результата распознавания.

Основной задачей в [14] является выявление какой-либо закономерности расположения легочного рисунка. Метод состоит из нескольких ключевых этапов: бинаризация, кластеризация, классификация. Для классификации используется нейронная сеть.

В [15] проверяется информативность автоматического распознавания образований в легких при цифровой рентгенографии на примере одного из общедоступных диагностических алгоритмов. Описываются методы и материалы для достижения задачи. Основой стала сверточная нейронная сеть.

Рассматривается проблема автоматизированной дифференциации патологий на цифровых рентгенограммах грудной клетки в [16]. Представлены исследования, направленные на разработку алгоритма и анализ существующих моделей сверточной глубокой нейронной сети. Предложен усовершенствованный алгоритм автоматизированной идентификации патологических структур, в частности метод, основанный на применении нейронных сетей, позволяющих ускорить процесс диагностики заболеваний и снижающих долю повторных исследований. Сделан вывод, что данная нейронная сеть является достаточно широкой и может дать много признаков для распознавания. Но из-за большого количества признаков является самой требовательной к вычислительным ресурсам.

Изучаются возможности и перспективы применения ИИ в клинической практике. В [17] отмечается, что ИИ в этой области является очень перспективным направлением. Приводятся примеры использования ИИ в этой области:

В ноябре 2017 г. специалисты из Стэнфордского университета под руководством Эндрю ЫНа разработали алгоритм под названием CheXNet. В основе ИИ под названием CheXNet лежит сверточная нейросеть (СНС). Она содержит 121 слой и относится к так называемым глубоким нейронным сетям. Алгоритм CheXNet обучался на основе более 100 тыс. рентгенограмм грудной клетки с 14 разными патологиями. Во всех тестах ИИ превзошел человека как по критерию чувствительности, так и по критерию специфичности.

В 2018 г. компания Google продемонстрировала возможности ИИ для быстрой и эффективной обработки флюорографии органов грудной клетки. В основе алгоритма лежит сверточная НС, выделяющая на медицинских снимках области, требующие дополнительного внимания специалиста. Для обучения алгоритма использовали ChestX-ray8 — самую крупную открытую базу данных рентгенологических исследований грудной клетки, которую ведет Национальный институт здравоохранения США.

Многие отечественные компании стали разрабатывать собственные технологии ИИ. Наиболее успешными из них являются следующие:

1. Botkin.AI — платформа с ИИ, объединяющая расчетные алгоритмы с медицинскими задачами диагностики, анализа и прогнозирования. В основе ее работы лежит собственная запатентованная технология построения математических моделей, с помощью которой проводится диагностика и оцениваются риски заболеваний.

2. Платформа «Третье мнение» способна в онлайн-режиме распознавать оцифрованные мазки крови, рентгенограммы грудной клетки и флюорограммы, снимки с офтальмологической фундус-камеры и ортопантомограммы. Каждый снимок система получает после обработки и ручной разметки силами квалифицированного врача-специалиста. Компания заявляет, что по рентгенограммам грудной клетки они уже могут распознать 15–20 нозологий.

3. Проект «CareMentorAI» под названием «Второе мнение AI» является сервисом, способным определить на фронтальной проекции рентгена легких наличие или отсутствие патологий. ИИ распознает до 20 видов патологий и предоставляет подробную расшифровку рентгеновского снимка. Также в тестовом режиме новая нейросеть способна анализировать рентгенограмму голеностопа. Она размечает угол свода стопы и сравнивает его с нормой, определяя плоскостопие.

В [18] автор рассматривает задачи идентификации неоднородностей на цифровых изображениях, математическая модель построена на основе нейрон-

ного подхода. Задача интерпретации рентгеновских изображений решается в рамках нейросетевого подхода для каждого набора параметров из обучающего множества. Для идентификации векторной функции рассматривается двухслойная нейронная сеть прямого распространения с сигмоидальным скрытым слоем нейронов и линейным выходным слоем. Структура нейронной сети подбирается экспериментально. Разработан алгоритм нейросетевого классификатора, реализующего на аппаратном уровне принципы нейросетевой технологии для распознавания текстуры изображения. Метод оценки изображения учитывает статистику значений пикселей из локального множества, основан на исследовании гистограмм «зоны интереса» и эталона. Разработана методика, обеспечивающая выбор размера ячейки, при сканировании «зон интереса» на цифровых рентгенограммах. Гистограммный анализ изображения и сегментация текстур используется для повышения диагностического потенциала изображения. В качестве алгоритма обучения используется алгоритм обратного распространения ошибки.

В [19] описывается создание сверточной нейронной сети для решения задачи распознавания на рентгеновских снимках пневмонии, а также приводятся показатели точности распознавания пневмонии. Для разработки программы, в которой реализуется решение задачи распознавания пневмонии на рентгеновских снимках, использовались: язык программирования Python, библиотека Keras версии 2.2.4, библиотека Keras_metrics и библиотека matplotlib. В качестве метода оптимизации для решения задачи распознавания пневмонии применялся алгоритм RMSProp. Этот алгоритм основан на применении коэффициента ослабления, благодаря которому в RMSProp обучение нейронной сети не замедляется слишком быстро, не достигнув минимума функционала ошибки в отличие от других алгоритмов с адаптивной скоростью обучения.

Описывается общая архитектура системы для решения задачи классификации при обнаружении COVID-19 и других заболеваний легких. Автор [20] говорит, что архитектура состоит из набора нейронных сетей, которые исполь-

зуются для сегментации и последующей классификации изображений, загружаемых на клиентское веб-приложение, для получения отчета о классификации. Для сегментации использовалась сверточная нейронная сеть U-Net, созданная для сегментации биомедицинских изображений. Для классификации используется классическая архитектура сверточной нейронной сети, которая называется LeNet.

Заключение

В период пандемии остро встал вопрос об обработке большого количества данных (рентген и кт снимки легких), а также об качественной и быстрой классификации этих данных. Для решения этой задачи используются методы машинного обучения. Нейронные сети обучаются на больших объемах данных и, в последствии, дают свое предположение по новым схожим данным, что облегчает работу врачам, помогая им правильнее выдвинуть диагноз. Распознавание снимков функциональной диагностики является в настоящее время актуальной задачей, так как напрямую связана с пандемией и ее последствиями.

СПИСОК ЛИТЕРАТУРЫ

1. Макаров В.В., Блатова Т.А., Ворошилова Е.Ю. УСКОРЕННОЕ РАЗВИТИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ПЕРИОД ПАНДЕМИИ // Экономика и качество систем связи. 2021. №2 (20). URL: https://cyberleninka.ru/article/n/uskorennoe-razvitie-informatsionnyh-tehnologiy-v-period-pandemii (дата обращения: 18.07.2021).
2. Васильченко Владислав Алексеевич, Бурковский Виктор Леонидович, Данилов Александр Дмитриевич Алгоритмизация процесса распознавания состояний физиологических объектов на основе специальных рентгеновских изображений // КО. 2019. №2. URL: https://cyberleninka.ru/article/n/algoritmizatsiya-protsessa-raspoznavaniya-sostoyaniy-fiziologicheskih-obektov-na-osnove-spetsialnyh-rentgenovskih-izobrazheniy (дата обращения: 18.07.2021).
3. Хаджибаев Абдухаким Муминович, Адылова Фатима Туйчиевна, Касимов Хамит Махмудович, Шарипова Висолат Хамзаевна, Исхаков Нурбек Баркамолович РОЛЬ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ПРОГНОЗИРОВАНИИ ПРОБЛЕМ COVID-19: АНАЛИТИЧЕСКИЙ ОБЗОР // Вестник экстренной медицины. 2020. №4. URL: https://cyberleninka.ru/article/n/rol-iskusstvennogo-intellekta-v-prognozirovanii-problem-covid-19-analiticheskiy-obzor (дата о обращения: 18.07.2021).
4. В.Г. Ефремцев, Н.Г. Ефремцев, Е.П. Тетерин, П.Е. Тетерин, Е.С. Базавлук Классификация рентгеновских изображений грудной клетки больных вирусной пневмонией и COVID-19 с помощью нейронных сетей // КО. 2021. №1. URL: https://cyberleninka.ru/article/n/klassifikatsiya-rentgenovskih-izobrazheniy-grudnoy-kletki-bolnyh-virusnoy-pnevmoniey-i-covid-19-s-pomoschyu-neyronnyh-setey (дата обращения: 18.07.2021).

5. А.А. Слуднова, В.В. Шутько, А.В. Гайдель, П.М. Зельтер, А.В. Капишников, А.В. Никоноров Выявление патологических изменений в легких на основе совместного анализа радиологических отчетов и томографических изображений // КО. 2021. №2. URL: https://cyberleninka.ru/article/n/vyyavlenie-patologicheskih-izmeneniy-v-legkih-na-osnove-sovmestnogo-analiza-radiologicheskih-otchetov-i-tomograficheskih (дата обращения: 18.07.2021).
6. А. С. Грицай, Т. О. Левицька Інтелектуальна система виявлення аномалій в рентгенівських знімках із застосуванням методів deep learning // Вестник Херсонского национального технического университета. 2019. №3 (70). URL: https://cyberleninka.ru/article/n/intelektualna-sistema-viyavlennya-anomaliy-v-rentgenivskih-znimkah-iz-zastosuvannyam-metodiv-deep-learning (дата обращения: 18.07.2021).
7. Горелов, И. А. Применение технологий компьютерного зрения при поиске патологий на рентгенограммах органов грудной клетки / И. А. Горелов, В. А. Немтинов // Wschodnioeuropejskie Czasopismo Naukowe. – 2016. – Т. 7. – № 2. – С. 6-13. URL: https://www.elibrary.ru/item.asp?id=28183686 (дата обращения: 18.07.2021).
8. Кузнецов, Н. А. Применение нейронных сетей для диагностики заболеваний / Н. А. Кузнецов // Инженерные и информационные технологии, экономика и менеджмент в промышленности : Сборник научных статей по итогам второй международной научной конференции, Волгоград, 24–25 декабря 2020 года. – Волгоград: Общество с ограниченной ответственностью "КОНВЕРТ", 2020. – С. 240-242. URL: https://www.elibrary.ru/item.asp?id=44673027 (дата обращения: 18.07.2021).
9. Мелдо, А. А. Алгоритмы диагностики XXL века. Искусственный интеллект в распознавании рака легкого / А. А. Мелдо, Л. В. Уткин, В. М. Моисеенко // Практическая онкология. – 2018. – Т. 19. – № 3. – С. 292-298. – DOI 10.31917/1903292. URL: https://www.elibrary.ru/item.asp?id=36458480 (дата обращения: 18.07.2021).
10. Анализ рентгеновских изображений для выявления патологий с использованием нейронных сетей / Р. Ш. Минязев, А. А. Румянцев, С. А. Дыганов, А. А. Баев // Известия Российской академии наук. Серия физическая. – 2018. – Т. 82. – № 12. – С. 1685-1688. – DOI 10.1134/S036767651812013X. URL: https://www.elibrary.ru/item.asp?id=36427649 (дата обращения: 18.07.2021).
11. Толкачев, А. Ю. Об опыте применения технологий искусственного интеллекта для автоматического распознавания рентгеновских изображений органов грудной полости / А. Ю. Толкачев, Р. Ф. Кулеев // Цифровое здравоохранение : Труды XX Международного конгресса «Информационные технологии в медицине», Москва, 10–11 октября 2019 года. – Москва: Общество с ограниченной ответственностью "Консэф", 2019. – С. 18-22. URL: https://www.elibrary.ru/item.asp?id=41662952 (дата обращения: 18.07.2021).
12. Верзунов, С. Н. Сравнение глубоких нейронных сетей на основе различных предварительно обученных CNN для диагностики COVID-19 по рентгеновским снимкам / С. Н. Верзунов, Х. А. Раимжанов // Проблемы автоматики и управления. – 2021. – № 1(40). – С. 12-25. URL: https://www.elibrary.ru/item.asp?id=45678650 (дата обращения: 18.07.2021).
13. Зубаиров, В. А. Использование Transfer Learning в распознавании COVID-19 на рентгеновских снимках / В. А. Зубаиров, Д. В. Захарова, П. С. Смирнова // Тенденции развития науки и образования. – 2021. – № 73-1. – С. 48-44. – DOI 10.18411/lj-05-2021-10. URL: https://www.elibrary.ru/item.asp?id=46197888& (дата обращения: 18.07.2021).
14. Максимова, Е. И. Алгоритм обнаружения образований в легких человека на снимках компьютерного томографа с использованием искусственной нейронной сети / Е. И. Максимова, П. А. Хаустов // Фундаментальные исследования. – 2016. – № 4-2. – С. 290-294. URL: https://www.elibrary.ru/item.asp?id=25953356 (дата обращения: 18.07.2021).
15. Гаврилов, П. В. Возможности автоматических систем в интерпретации рентгенограмм легких у пациентов с подозрением на округлое образование / П. В. Гаврилов, У. А. Смольникова // Лучевая диагностика и терапия. – 2020. – № 1(11). – С. 46-51. – DOI 10.22328/2079-

5343-2020-11-1-46-51. URL: https://www.elibrary.ru/item.asp?id=42619697 (дата обращения: 18.07.2021).
16. Лисовская, М. Г. Разработка алгоритма распознавания патологий на цифровых рентгенограммах / М. Г. Лисовская // Научные исследования и перспективные проекты 2017 : Сборник трудов 2-й научно-практической конференции аспирантов, преподавателей, ученых, Уфа, 26–29 апреля 2017 года. – Уфа: Общество с ограниченной ответственностью "Клауд Кэпитал", 2017. – С. 17-21. URL: https://www.elibrary.ru/item.asp?id=29279403 (дата обращения: 18.07.2021).
17. Использование искусственного интеллекта в клинической практике / Д. Н. Борисов, И. И. Кушнирчук, В. В. Севрюков, Е. И. Коваленко // Клиническая патофизиология. – 2019. – Т. 25. – № 2. – С. 26-31. URL: https://www.elibrary.ru/item.asp?id=41538467 (дата обращения: 18.07.2021).
18. Старожилова, О. В. Распознавание неоднородностей на цифровых изображениях с использованием нейронной сети / О. В. Старожилова, К. А. Захаров // Международный студенческий научный вестник. – 2018. – № 1. – С. 76. URL: https://www.elibrary.ru/item.asp?id=32517669 (дата обращения: 18.07.2021).
19. Арбузова, А. А. Решение задачи распознавания медицинских изображений с помощью нейронных сетей / А. А. Арбузова // Проблемы информатики в образовании, управлении, экономике и технике : Сборник статей XX Международной научно-технической конференции, посвященной 75-летию Победы в Великой Отечественной войне, Пенза, 11–12 декабря 2020 года. – Пенза: Автономная некоммерческая научно-образовательная организация «Приволжский Дом знаний», 2020. – С. 61-64. URL: https://www.elibrary.ru/item.asp?id=44805451 (дата обращения: 18.07.2021).
20. Думаев, Р. И. Автоматическое обнаружение COVID-19 по рентгеновским снимкам / Р. И. Думаев, С. А. Молодяков // Современные технологии в теории и практике программирования : Сборник материалов научно-практической конференции, Санкт-Петербург, 22 апреля 2021 года. – Санкт-Петербург: Федеральное государственное автономное образовательное учреждение высшего образования "Санкт-Петербургский политехнический университет Петра Великого", 2021. – С. 22-24. URL: https://www.elibrary.ru/item.asp?id=45781311 (дата обращения: 18.07.2021).

СЕКЦИЯ 5.4
ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И ЗАЩИТА ИНФОРМАЦИИ

УДК 004.056.5

Д. С. АЛЕКСЕЕВА
ads.stat@mail.ru
Науч. руководов. – д-р техн. наук, доц. В. В. АНТОНОВ

Уфимский государственный авиационный технический университет

ПРОЦЕСС ПОСТРОЕНИЯ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В АНАЛИТИЧЕСКОМ ЦЕНТРЕ

***Аннотация*.** В статье рассмотрен процесс построения информационной безопасности в аналитическом центре.
***Ключевые слова*:** автоматизация; торговый агент.

Аналитический центр – это организация, которая осуществляет исследовательскую, прогнозную и консультационную деятельность в области политического производства.

Построение системы информационной безопасности сторонней организацией, в центре начинается с анализа предприятия.

Анализ предприятия включает в себя:

- Посещение организации:
- Идентификация активов, представляющих ценность;
- Анализ информационных ресурсов, которые уязвимы с точки зрения информационной безопасности;
- Анализ источников угроз;
- Анализ угроз;
- Оценка возможного ущерба;
- Выбор средств защиты информации;
- Принятие организационных мер:
- Разработка политики безопасности;

– Разработка стандарта ЗИ[1];

– Разработка инструкций, направленных на поддержание системы ИБ[2];

– Обязательное информирование сотрудников;

– Постоянный мониторинг системы ИБ и ее совершенствование в результате изменений в работе организации или изменений в информационных технологиях.

1. Идентификация активов, представляющих ценность

Первым этапом при посещении организации, на базе которой будет разворачиваться система информационной безопасности, является идентификацию активов, представляющих ценность. [1]

Данный этап заключается в обследовании физической составляющей будущей системы, включая расположение машин.

Активы, представляющие ценность — это любой физический или нематериальный объект, играющий важную финансовую роль для собственника.

Так в аналитическом центре активами, представляющими ценность могут являться:

– Серверное оборудование;

– Персональные вычислительные машины сотрудников;

– Общие вычислительные машины организации;

– Демонстрационное оборудование;

– Устройства вывода информации (принтеры, МФУ[3]).

Кроме технической составляющий важным активом для аналитического центра является обрабатываемая информация, которая в конечном итоге подлежит защите.

Это подводит к следующему этапу разработки системы информационной безопасности.

[1] ЗИ – Защита информации
[2] ИБ – Информационная безопасность
[3] МФУ – многофункциональное устройство

2. Анализ информационных ресурсов, которые уязвимы с точки зрения информационной безопасности

Информация, в соответствии с Федеральным законом №149 «Об информации, информатизации и защите информации», делится на общедоступную и информацию ограниченного доступа [2].

Информацию ограниченного доступа делится на государственную тайну и конфиденциальную информацию.

В аналитических центрах фигурируют оба вида ограниченной информации. Многое зависит от статуса организации.

Если организация не работает со сведениями защищаемых государством (государственная тайна), то информация является конфиденциальной.

Перечень сведений, относящихся к конфиденциальной информации, определен в Указе Президента РФ от 6 марта 1997 г. N 188 «Об утверждении перечня сведений конфиденциального характера»:

– Сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях.

– Сведения, составляющие тайну следствия и судопроизводства, а также сведения о защищаемых лицах и мерах государственной защиты, осуществляемой в соответствии с Федеральным законом от 20 августа 2004 г. N 119-ФЗ "О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства" и другими нормативными правовыми актами Российской Федерации.

– Служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (служебная тайна).

– Сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и фе-

деральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и так далее).

– Сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (коммерческая тайна).

– Сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них.

Информация формирует информационные ресурсы, которые используются внутри аналитического центра.

Информационный ресурс — это индивидуальные и коллективные экспертные знания, отдельные документы, отдельные массивы документов, а также документы и их массивы, составляющие базы и банки данных, базы знаний, библиотеки, архивы, фонды, информационные системы и другие системы в определенной предметной тематической области, которые удовлетворяют функциональным потребностям и запросам потребителей информации.

Уязвимость информационных ресурсов может заключаться в их утрате, случайном уничтожении, передаче третьим лицам.

3. Анализ источников угроз

Под источниками угроз информационной безопасности понимаются как исходные основания (причины) опасного воздействия на жизненно важные интересы личности, общества и государства в информационной сфере.

В аналитическом центре источником угрозы информационной безопасности могут выступать как технические составляющие, в том числе съемные носители, так и сами сотрудники центра.

К технической составляющей источников угроз можно отнести:

– Незащищенные каналы связи;

– Использование незарегистрированных съемных носителей;

– Незащищенные вычислительные машины;

Из сотрудников центра источниками угроз могут являться:

– Сотрудники, непосредственно работающие с информацией;

– Системные администраторы.

Сотрудники, непосредственно работающие с информацией, делятся на аналитиков и операторов.

Операторы занимаются сбором информации, аналитики – анализом полученных данных.

4. Анализ угроз

Анализ угроз информационной безопасности позволяет выделить составляющие современных компьютерных угроз – их источники и движущие силы, способы и последствия реализации.

Также анализ необходим для определения потенциальной величины ущерба, а также выработки мер противодействия.

Существует несколько методов анализа:

– Экспертная оценка;

– Статистический анализ;

– Факторный анализ.

Экспертная оценка основана на субъективном мнении эксперта в области информационной безопасности.

Название статистического анализа говорит само за себя. Данный метод основан на накопление данных об инцидентах, источниках угроз, их типе.

Факторный анализ основан на вероятностном анализе, который позволяет выявить угрозы, которые могут привести к реальным последствиям.

В случае с аналитическим центром фактором может послужить наличие привлекательной для киберпреступников информации.

5. Оценка возможного ущерба

Результатом нарушения системы информационной безопасности аналитического центра может быть, как утечка, так и искажение информации, в том числе ее полное уничтожение.

При оценке возможного ущерба выделяют две категории: материальный и нематериальный [3].

К материальному ущербу относятся вышеперечисленные факты, к нематериальному – уничтожение репутации и/или имиджа центра.

Степени ущерба представлена в таблице 1.

Таблица 1

Степени ущерба и их описание

Степень ущерба	Описание ущерба
Ничтожный	Ущербом (угрозой) можно пренебречь
Незначительный	Ущерб легко устраним, затраты на ликвидацию последствий реализации угрозы невелики. Финансовые операции не ведутся некоторое время. Положение на рынке и количество клиентов меняются незначительно.
Умеренный	Ликвидация последствий реализации угрозы не связана с крупными затратами и не затрагивает критически важные задачи. Положение на рынке ухудшается. Потеря части клиентов
Серьезный	Затрудняется выполнение критически важных задач. Утрата на длительный период (например, до года) положения на рынке. Ликвидация последствий со значительными финансовыми инвестициями
Критический	Невозможность решения критически важных задач. Организация прекращает существование

6. Выбор средств защиты информации

После того как проведен анализ угроз и ущерба специалист по информационной безопасности приступает к выбору средств защиты информации.

Средства защиты информации (СЗИ) - это совокупность инженерно-технических, электрических, электронных, оптических и других устройств и приспособлений, приборов и технических систем, а также иных вещных элементов, используемых для решения различных задач по защите информации, в том числе предупреждения утечки и обеспечения безопасности защищаемой информации. [4]

Средства защиты информации подбираются под каждую организацию индивидуально исходя из информации полученной на предыдущих этапах (п. 1 – 5). При выборе средства обязательно производится его оценка.

Так для аналитического центра в качестве средств защиты информации могут быть выбраны:

– Межсетевой экран - программный или программно-аппаратный элемент компьютерной сети, осуществляющий контроль и фильтрацию проходящего через него сетевого трафика в соответствии с заданными правилами (разрабатываются экспертами);

– Защита от вредоносного ПО – использования антивирусного программного обеспечения, а также применение техники безопасности использования сети Интернет;

– Контроль USB – портов – позволяет администратору вести журнал действий пользователя с внешними накопителями. Для реализации контроля используется специализированное ПО, в котором имеется белый список устройств, разрешенных к подключению;

– Резервное копирование – реализуется с использованием как систем управления базами данных, так и специализированного ПО. Резервная копия позволяет с меньшими потерями восстановить данные в случае их утраты;

– Защита сервера – может быть реализована с помощью пары криптографических ключей (SSH – ключи4). Система будет использовать закрытый и открытый ключ. Открытый ключ передается с любого SSH сервера, а закрытый ключ хранится в тайне. При таком подходе открытый ключ помещается в специальной директории сервера, этим действием пользователь осуществляется вызов на который должен ответить держатель закрытого ключа;

– Защита корпоративной сети – реализуется с помощью устройств UTM. Устройства UTM (Универсальный шлюз безопасности; Unified Threat Management) часто упаковываются как устройства сетевой безопасности, которые могут помочь защитить сети от комбинированных угроз безопасности, включая вредоносные программы и атаки, которые одновременно направлены на отдельные части сети;

– Электронные замки;

4 SSH (Secure Shell) – сетевой протокол, используемый для безопасного обмена информацией между двумя компьютерами по зашифрованному каналу

– Сейфы;

– Шредеры;

– Видеокамеры;

– Датчики движения.

Также важным моментом при построении системы ИБ и выборе СЗИ является возможность регулярное обновление ПО, это помогает управлять уязвимостями системы.

7. Принятие организационных мер

Одной из организационных мер разработки системы информационной безопасности является разработка политики безопасности.

Политика безопасности (ПБ) [5] это особый документ, содержащий руководящие принципы, правила, процедуру и практические приемы в области безопасности, которые регулируют управление, защиту и распределение ценной информации.

ПБ должна быть реалистичной и выполнимой, а также не приводить к существенному снижению общей производительности центра.

ПБ должна отвечать на типичные вопросы осуществления ИБ, в т.ч:

—кто имеет право доступа к объектам, поддерживаемым сервисом?

—при каких условиях можно читать и модифицировать данные?

—как организован удаленный доступ к сервису?

—кто имеет право модернизировать сервис?

Также в аналитическом центре, как и в любой другой организации, должен быть разработан стандарт предприятия.

Стандарт устанавливает общие требования к обеспечению безопасности данных, обрабатываемых в аналитическом центре и распространяется на все подразделения организации.

Стандарт входит в состав нормативных документов системы управления аналитического центра и, как правило, содержит в себе ссылки на определенные нормативно – правовые акты.

В рамках разработки и принятия организационных мер также разрабатывается инструкция, направленная на поддержание ИБ.

В инструкции должна быть зафиксирована ответственность сотрудников за нарушение требований ИБ, разглашение и нарушение конфиденциальной информации.

Заключительном этапом внедрения системы информационной безопасности является обязательное информирование сотрудников под роспись.

Построение системы информационной безопасности в аналитическом центре, или в любой другой организации, достаточно трудоемкий и длительный процесс.

Система ИБ позволяет обезопасить данные, аналитические анализы и отчеты сотрудников от утечки, повреждения и прочего нежелательного вмешательства.

Построение системы информационной безопасности включает в себя:

—Анализ предприятия;

—Выбор средств защиты информации;

—Информирование сотрудников;

—Постоянный мониторинг системы ИБ и ее совершенствование в результате изменений в работе организации или изменений в информационных технологиях.

СПИСОК ЛИТЕРАТУРЫ

1. Анализ угроз информационной безопасности URL: https://arinteg.ru/articles/analiz-ugroz-informatsionnoy-bezopasnosti-27291.html
2. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 N 149-ФЗ.
3. ОЦЕНКА УЩЕРБА ОТ НАРУШЕНИЯ ИБ. URL: https://www.audit-ib.ru/complete-protection/protection-methods/damage-assessment/
4. Средства защиты информации. URL: https://it-security.admin-smolensk.ru/zinfo/szi/#:~:text=Средства%20защиты%20информации%20—%20это,и%20обеспечения%20безопасности%20защищаемой%20информации
5. Построения системы информационной безопасности URL: https://intuit.ru/studies/courses/13845/1242/lecture/27501?page=2

УДК 004.056

К. М. АМИРОВ
karamirov@gmail.com

Уфимский государственный авиационный технический университет

ВНЕДРЕНИЕ КРИПТОШЛЮЗОВ В РАБОТУ ЧАСТНЫХ МЕДИЦИНСКИХ УЧРЕЖДЕНИЙ

Аннотация. В данной статье описывается методология внедрения защищенных информационных систем в работу медицинских учреждений. Описаны требования к программно-аппаратному комплексу, подлежащему внедрению. Описана методология внедрения защищенной сети в работу частного медицинского учреждения. Проведен анализ негативных и позитивных последствий после внедрения криптошлюза в работу учреждения. Приведены примеры внедрения защищенных частных сетей в работу других предприятий.
Ключевые слова: информационная безопасность; информационные системы; здравоохранение; защита персональных данных; внедрение защищенных сетей; виртуальные частные сети.

Введение

Ставший за последние годы наиболее актуальным, Федеральный закон «О персональных данных» от 27 июля 2006 г. (№152-ФЗ), определяет персональные данные как ««любую информацию, относящуюся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных)». К персональным данным относятся фамилия, имя, отчество субъекта персональных данных, год, месяц, дата и место его рождения, адрес, семейное, социальное, имущественное положение и т.д.

С точки зрения информационной безопасности в медицине сведения о состоянии здоровья относятся к специальным категориям персональных данных, а действующее законодательство обязывает лечебно-профилактические учреждения обеспечить защиту этой информации.

Федеральный закон №152-ФЗ «О защите персональных данных» является основным регулирующим документом в обеспечении защиты информации в медицине. Согласно ему, лечебные учреждения являются операторами персональных данных, следовательно, обеспечение безопасности этих данных – документов, инициированных, например, ФСБ и ФСТЭК России. Согласно пред-

писанным в них способам и порядку обеспечивается безопасность персональных данных, в том числе и в здравоохранении.

Техническое обеспечение реализации концепции информационной защиты включает в себя: юридически обеспеченное электронное документоведение, отсутствие дубликата зафиксированных данных на бумаге, заверка электронных документов цифровой подписью, обеспечение безопасности информационных баз данных.

На рынке информационных систем уже представлены комплекты оборудования, разработанные в соответствии с требованиями Министерства здравоохранения, представляющие собой набор сервера-терминала и аппаратного клиента с включенными модулями защищенного ввода и определения абонента.

На данный момент, отечественный рынок криптошлюзов может предложить следующие решения, который подходят под описанные выше задачи:

1) Программно-аппаратный комплекс «Атликс-VPN». Отличительной особенностью является способ ввода ключевой информации, необходимой для реализации его функций. Для этого используется «Российская интеллектуальная карта» — микропроцессорная карта, разработанная «НТЦ Атлас», ЗАО «Программные системы и технологии», ОАО «Ангстрэм». Карта выполнена на основе отечественного микропроцессора производства ОАО «Ангстрэм».

2) Аппаратно-программный комплекс шифрования «Континент» — криптографический шлюз производства российской компании «Код Безопасности». Аппаратно-программный комплекс шифрования обеспечивает межсетевое экранирование и криптографическую защиту открытых каналов связи в соответствии с ГОСТ 28147-89. Поддерживает централизованное управление и мониторинг с помощью продукта «Центр управления сетью «Континент»;

3) Программно-аппаратный комплекс «Фильтр пакетов сетевого уровня — Internet Protocol» производства российской компании АМИКОН при участии «ИнфоКрипт». Программно-аппаратный комплекс представляет собой межсетевой экран и средство построения виртуальных частных сетей.

4) Программно-аппаратный комплекс ViPNet Coordinator HW разработан российской компанией «ИнфоТеКС» и представляет собой сертифицированный криптошлюз и межсетевой экран. Для построения VPN используется собственный протокол ViPNet VPN, который обеспечивает беспрепятственное защищенное взаимодействие независимо от типа канала связи, автоматический роуминг между каналами связи. Поддержка взаимодействия с клиентскими компонентами (ПО ViPNet Client) на различных операционных системах (Windows, Linux, macOS, iOS, Android).

Включенный аппаратный клиент обеспечивает безопасный доступ к образу всей базы данных.

Аутентификация абонента производится с помощью ввода личного ключа и секретного кода. Загрузка системы производится исключительно после проверки соответствия введенных паролей доступа.

Терминал производит разграничение доступа отдельных абонентов, обеспечивая аппаратную защиту сведений в медицинской сфере.

Администратор обеспечивает опознавание персональных кодов доступа. Это позволяет терминальному ресурсу установить связь с сервером и «опознать» абонента.

Начать работу с удаленным сервером через тонкий терминал абонент может после ввода персонального ключа и кода доступа. Таким образом, система идентифицирует клиента и гарантирует защиту информационной базы.

Внедрение технологии «опознавания» абонента предполагает наличие руководящего звена (администратора), наделенного полномочиями свободного доступа к размещенным сведениям, а также установки ограничений для других абонентов системы.

Заверить электронный документ подписью позволяет разработанная программа, обеспечивающая ее проверку и оформление. Работает программа в онлайн-режиме. Завершенное программное обеспечение аппаратного клиента на

базе отдельной операционной системе запускается только в ограниченном режиме «для чтения».

Программа независимых гарантий предусматривает образование системы персонифицированного учета оказания медицинских услуг. Подобная система способна обеспечить регистрацию: оказанных услуг, медперсонала, закупок медикаментов. Таким образом, будет облегчено управление учреждением здравоохранения. В ходе всего вышесказанного, оптимальным выбором является программно-аппаратный комплекс «ViPNet Coordinator HW».

Информационные системы, современных частных медицинских учреждений, объединяют высокотехнологичную медицинскую технику, рабочие места врачей и единый архив историй заболеваний пациентов.

Так как в информационной системе медицинских учреждений обрабатываются персональные данные пациентов, то необходимо выполнять требования ФЗ-152 «О персональных данных» и подзаконных актов, связанных с этим законом. Одним из требований по защите персональных данных является организация защищенных каналов связи с помощью средств криптографической защиты информации. В соответствии с этим требованием необходимо спроектировать систему защиты персональных данных в целом и средства криптографической защиты информации в частности.

Основные требования, которым должны соответствовать средства криптографической защиты информации, для внедрения в медицинских учреждениях:

1) задержки в канале (это самый важный критерий, потому что медицинский персонал с помощью клиентского приложения на рабочем месте подключается к серверной части в Центре управления сетью, и задержки в канале сильно влияют на производительность системы и скорость работы с пациентом);

2) наличие сертификата ФСБ России на криптосредства (требование нормативных документов, касающихся защиты персональных данных (Приказ ФСБ №378 от 10 июля 2014 г. «Об утверждении состава и содержания организацион-

ных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»));

3) масштабируемость решения (предполагается расширение системы на дополнительные объекты);

4) отказоустойчивость;

5) достаточная производительность (необходимо обеспечить хороший канал связи до Центра управления сетью);

6) мониторинг (так как инфраструктура может быть распределена по всему городу, необходимо обеспечить постоянный мониторинг оборудования и отслеживать нагрузки на сеть);

7) простота обслуживания (администратор сети должен решить проблему на месте по инструкции).

К внедрению предполагается сеть, с одним координатором (криптошлюзом), и закрепленными за ним VPN-клиентами.

Внедрение криптошлюза состоит из следующих этапов:

1) Преднастройка (выпуск и установка наборов ключей на программно-аппаратный комплекс, настройка сетевых интерфейсов, настройка snmp-агента, заведение программно-аппаратного комплекса в Администрирующем программном обеспечении);

2) Установка криптошлюза в медицинское учреждение (настройка альтернативного канала для того, чтобы не прерывать работу учреждения);

3) Установка клиентского программного обеспечения в медицинское учреждение;

4) Подключение криптошлюза и клиентского программного обеспечения к системе мониторинга.

СПИСОК ЛИТЕРАТУРЫ

1. Иорпшатт С., Новак Д. Обнаружение вторжений в сеть. Москва: «ЛОРИ», 2018. 384 с.
2. Рябко С.Д., Смыслов В.А. Безопасность IP: таинство творения. // ИнфомКурьер-Связь, 2007. №12. С.20-23.
3. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. Москва.: «Питер», 2016. 992 с.
4. Беленькая М.Н., Малиновский С.Т., Яковенко Н.В. Администрирование в информационных системах. Москва: «Горячая линия-Телеком», 2017. 400 с.
5. Шаньгин В., Защита компьютерной информации. Эффективные методы и средства. Москва: «ДМК Пресс», 2016. 544 с.
6. Безкоровайный М.М., Костогрызов А.И., Львов И.М. Инструментально-моделирующий комплекс для оценки качества функционирования информационных систем. Москва: «СИНТЕГ», 2015. 113 с.
7. Виноградов К. А., Никитина М. И. Формирование информационной системы регионального здравоохранения // Врач и информационные технологии, 2004. №2. С. 15-18.
8. Калиниченко В. И. Необходимость создания интегрированной системы управления медицинской помощью // Врач и информационные технологии. - №2, 2014. №4. С. 25-28.
9. Эльянов М. М. Медицинские информационные технологии // Третья медицина, 2005. №5 - С.32
10. Чугунова К. Ю. Информационное оружие как угроза национальной безопасности Российской Федерации // Актуальные проблемы российского права, 2017. №7. С.59-64.
11. Столлингс В. Network Security Essentials. Applications and Standards Москва: «Вильямс», 2016. С. 432.
12. Захватов М. Построение виртуальных частных сетей (VPN) на базе технологии MPLS. Москва: «Риверсайд Тауерз», 2016. 435 с.
13. Murdoch St. J, Danezis G. Low-cost traffic analysis of Tor. USA, Oakland, 2017. P. 183-195.
14. Ruiz-Martinez A. A survey on solutions and main free tools for privacy enhancing Web communications. // Journal of Network and Computer Applications. 2019. №35. P.1473-1492.
15. Александр Р. Виртуальные частные сети VPN. Москва: «Телеком», 2019. 320 с.

УДК 004.056

Е. А. АТАРСКАЯ
arskaya25@mail.ru
Науч. руководитель – канд. техн. наук, доц. А. М. ВУЛЬФИН

Уфимский государственный авиационный технический университет

СИСТЕМА ОБНАРУЖЕНИЯ АНОМАЛИЙ ТЕХНОЛОГИЧЕСКИХ ВРЕМЕННЫХ РЯДОВ ПАРАМЕТРОВ ПРОМЫШЛЕННОГО ПРОЕКТА

Аннотация. Целью работы является повышение защищенности АСУ ТП за счет совершенствования алгоритмов обнаружения аномалий наблюдаемых параметрах объектов АСУ ТП на основе интеллектуального анализа технологических временных рядов. В статье разрабатывается система обнаружения аномалий в технологических временных рядах в наблюдаемых параметрах, характеризующих состояния объектов АСУ ТП.
***Ключевые слова*:** система обнаружения аномалий; АСУ ТП; технологические временные ряды; интеллектуальный анализ данных.

Актуальность работы обусловлена широким использованием сетевых телекоммуникаций в АСУ ТП и высоким уровнем опасности угроз подмены, искажения или потери накапливаемых данных о ходе ТП в результате воздействия злоумышленника на сетевую инфраструктуру объекта. Применение методов обнаружения аномалий технологических временных рядов накапливаемых параметров состояния сложных технических объектов с использованием технологий интеллектуального анализа данных и методов машинного обучения позволяет выявлять сложные атаки злоумышленника на элементы промышленных систем.

Объект исследования – обеспечение информационной безопасности данных, являющихся результатами измерений параметров технологических объектов, от угрозы несанкционированной модификации информации.

Предмет исследования – алгоритмы выявления аномалий в наблюдаемых параметрах объектов АСУ ТП промышленного предприятия на основе технологий обнаружения аномалий в многомерных технологических временных рядах.

Цель работы: повышение защищенности АСУ ТП за счет совершенствования алгоритмов обнаружения аномалий наблюдаемых параметрах объектов

АСУ ТП на основе интеллектуального анализа технологических временных рядов.

Задачи:

– анализ систем мониторинга технологического процесса в задаче обнаружения аномалий в накапливаемых данных о ходе ТП;

– разработка структурной схемы мониторинга и обнаружения аномалий в наблюдаемых параметрах состояния объектов АСУ ТП.

Основным инструментом реализации предиктивного обслуживания является задача поиска аномалий (см. рисунок 1) во временных рядах, так как при возникновении аномалии в данных велика вероятность того, что через некоторое время возникнет сбой или отказ. Аномалия – это некоторое отклонение показателей программной системы, такое как выявление деградации скорости выполнения запроса одного вида или снижение среднего числа обслуживаемых обращений при постоянном уровне клиентских сессий [1].

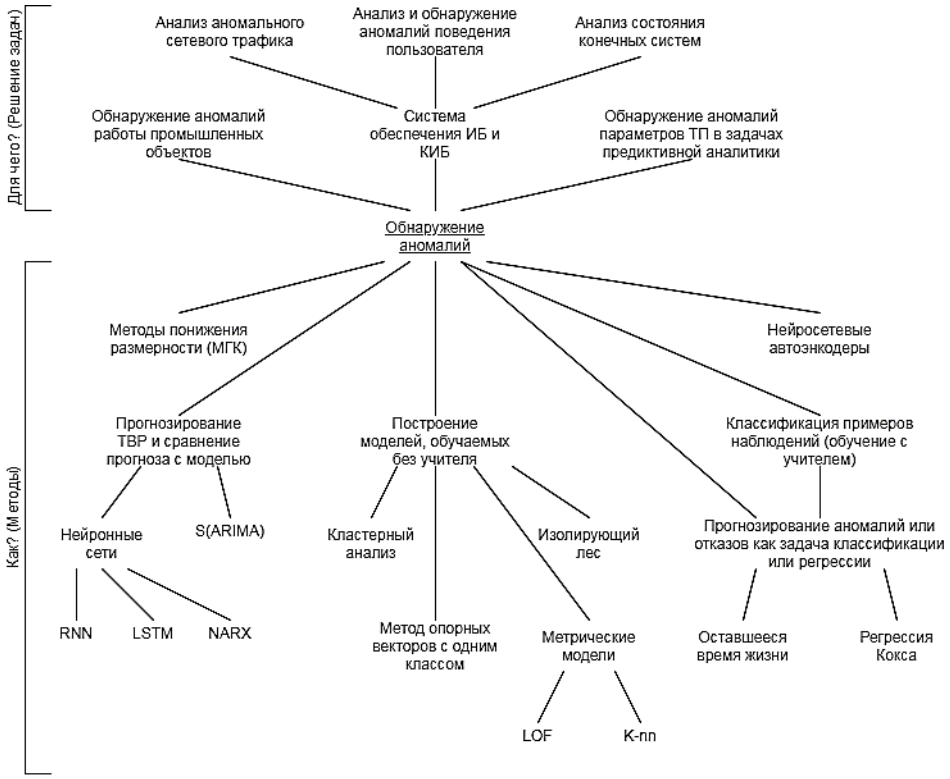


Рис. 1. Методы обнаружения аномалий и задачи, решаемых с помощью них

Структурная схема системы обнаружения аномалий технологического процесса, основанная на применении методов анализа собираемых данных телеметрии, и позволяющая выявить действия злоумышленника, получившего доступ в промышленную сеть управления технологическим процессом, представлена на рисунке 2.

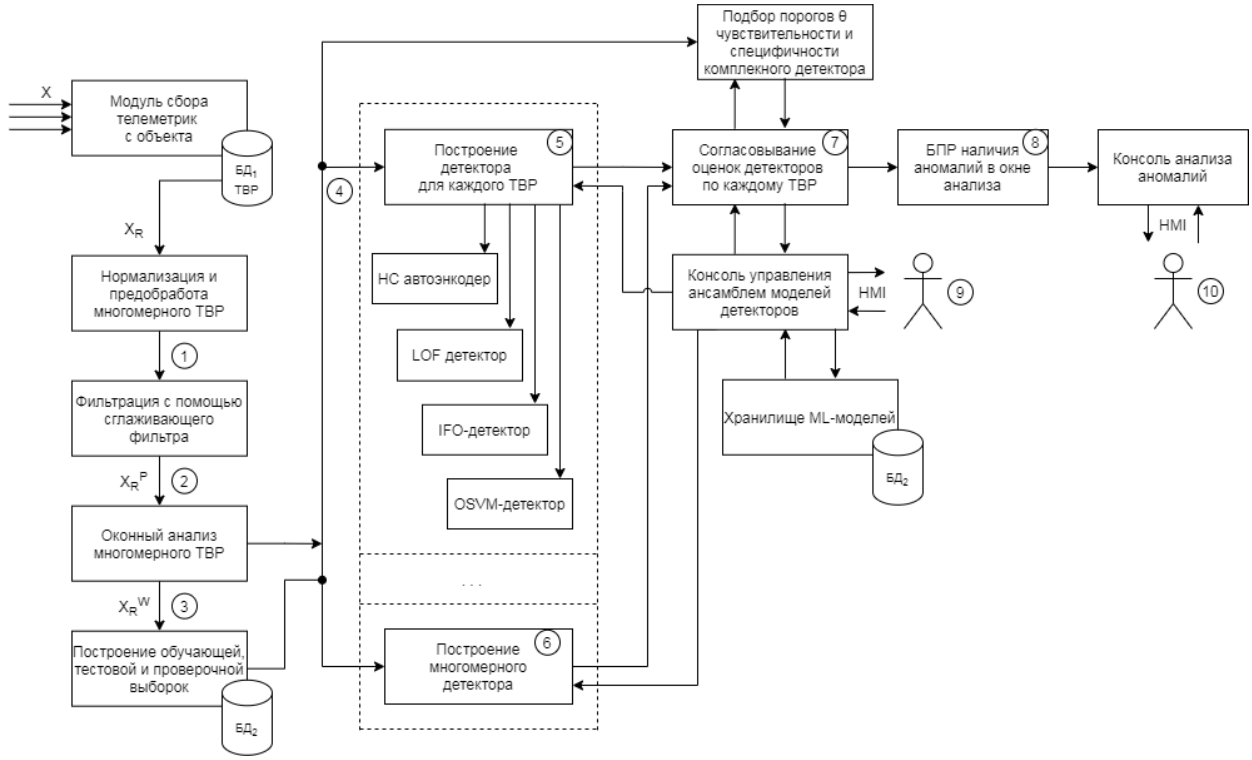


Рис. 2. Структурная схема системы обнаружения аномалий

где:

1) Нормализация каждого из рядов многомерного ТВР X_R.

2) Сглаженные многомерные ТВР X_R^P.

3) Скользящее окно длины W с шагом S формирует набор отсчетов для анализа по каждому из рядов ТВР X_R^W (см. рисунок 3).

4) Подготовленные данные для построения, тестирования и использования ансамбля детекторов.

5) Автоэнкодер на основе нейронной сети LSTM. Детектор выбросов с автоподстройкой порога (LOF детектор). Детектор аномалий на основе модели изолирующего леса (IFO). Детектор аномалий на основе машины опорных векторов (One class SVM).

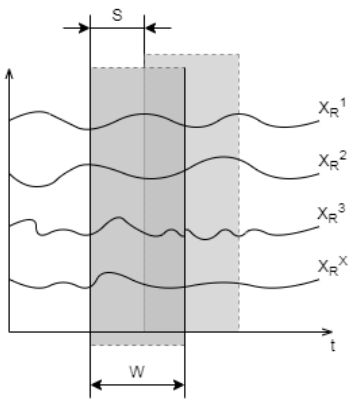


Рис. 3. Скользящее окно длины W с шагом S

6) Многомерный детектор HC LSTM (см. рисунок 4).

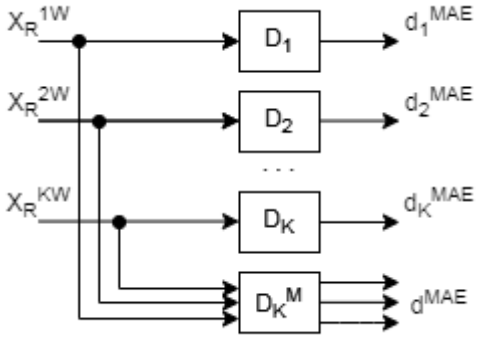
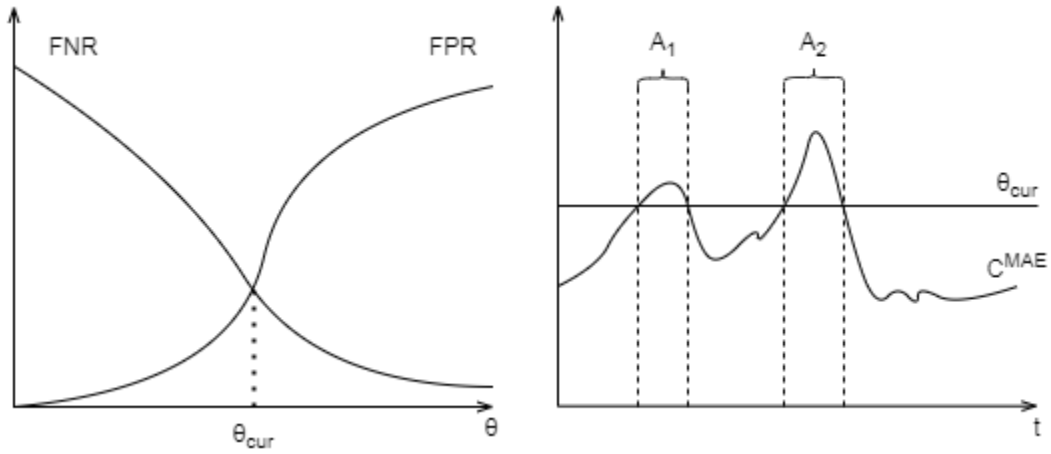


Рис. 4. Многомерный детектор HC LSTM



а *б*

Рис. 5. Подбор порога чувствительности и специфичности комплексного детектора

7) Суммирование оценок детекторов в каждом окне W одномерных ТВР.

8) Блок принятия решений о наличии аномалий в окне анализа W одномерных ТВР.

9) Специалист по интеллектуальному анализу данных.

10) Оператор системы обнаружения аномалий.

Признаки представляют собой данные измерений, собранные системой SCADA со встроенных датчиков. В крупномасштабных АСУ ТП обычно много датчиков. Во-первых, для создания производительной модели системы обнаружения вторжений необходимо правильно выбрать признаки; во-вторых, из-за большого количества измеренных данных алгоритм модели должен иметь возможность быстрого прогнозирования, чтобы его можно было использовать в приложениях реального времени. Цель выбора признаков – найти наиболее эффективные признаки, что позволит обучить более точные модели и сократить время вычислений. Методы выбора признаков можно разделить на методы фильтрации, оболочки, встроенные и гибридные методы. В методе фильтрации широко используются критерии корреляции в задачах машинного обучения. Корреляция – это мера линейной связи между двумя или более параметрами. Для построения модели будут выбраны наиболее коррелированные признаки с целью.

Чтобы выбрать признаки с высокой корреляцией с целью, нам нужно установить пороговое значение для выбора функций с более высокой корреляцией. Предположим, что выбранные признаки коррелированы друг с другом. В этом случае мы можем отбросить тот, у которого наименьшая корреляция к цели. Кроме того, можно объединить признаки, которые вместе показывают высокую корреляцию. Для этого вычисляется корреляция двух признаков, а наиболее коррелированные признаки назначаются для удаления [2].

На этапе предварительной обработки входные данные должны масштабироваться. Это может привести к устойчивому процессу обучения. Нормализация количественных признаков подразумевает приведение к нулевому среднему и единичному стандартному отклонению.

В задаче обнаружения аномалий во временных рядах аномалии представляют собой отдельные отрезки временного ряда, которые являются аномалиями в определенном контексте, но не иначе. К примеру, температура 0°C может быть нормальной в течение зимы, но такое же значение в течение лета в этой климатической зоне было бы аномалией.

С помощью метода скользящего окна из временных рядов набора данных формируются обучающие и тестовые выборки. Мотивация метода скользящих окон заключается в том, что аномалия во временном ряду может быть вызвана наличием одной или нескольких аномальных последовательностей [3].

Для создания детектора аномалий в АСУ ТП используются данные о нормальной деятельности для построения прогнозной модели нормального класса, а также класса аномалий. Затем любые непредвиденные данные сравниваются с созданной моделью для определения ее класса. Обучающая выборка содержит только данные о нормальном поведении системы, тестовая – содержит данные и нормального класса, и класса аномалий (одиночные атаки и их комбинации).

В данном исследовании применяется несколько алгоритмов для обучения модели машинного обучения для обнаружения аномалий с помощью промышленных систем контроля. В данном исследовании выбраны следующие алгоритмы обучения: автоэнкодер на основе нейронной сети LSTM для одномерного ТВР, детектор выбросов с автоподстойкой порога (LOF-детектор), детектор аномалий на основе изолирующего леса (IFO-детектор), детектор аномалий на основе машины опорных векторов (One-class SVM).

Оценка методов обнаружения аномалий в данных временных рядов производится с помощью TaPR – точности и отзыва временных рядов. Цель состоит в том, чтобы определить область действия атак.

Разнообразие обнаруженных аномалий более важно при использовании двух стратегий оценки в показателях TaPR. Две стратегии: оценка обнаружения, которая называется TaR (то есть, сколько аномалий обнаружено), и оценка

части, которая называется TaP (то есть, насколько точно обнаруживается каждая аномалия). Кроме того, показатели TaPR дают более низкие оценки тем экземплярам, которые отмечены как нормальные, хотя на них влияет их прецедентная аномалия, поскольку они, вероятно, являются аномальными [4].

Автоэнкодеры – это нейронные сети, обученные без учителя, целью которых является реконструкция входных данных. Они состоят из двух частей: кодера и декодера. Кодер – это функция f, которая отображает входные данные $x \in \mathbb{R}^{d_x}$ на скрытый код/представление $z \in \mathbb{R}^{d_z}$. Он имеет вид

$$z = f(x) = s_f\ (W_x + b_z) \tag{1}$$

где s_f обозначает функцию активации (часто нелинейную), $W \in \mathbb{R}^{d_z * d_x}$ – матрицу весов, $b_z \in \mathbb{R}^{d_z}$ – вектор смещения.

Декодер – это функция g, осуществляющая обратное отображение из скрытого кода во входное пространство (реконструкция).

$$\hat{x} = g(z) = g(f(x)) = s_g\ (W'_z + b_x) \tag{2}$$

где s_g – функция активации декодера, $W' \in \mathbb{R}^{d_z * d_x}$ – весовая матрица, $b_x \in \mathbb{R}^{d_x}$ – вектор смещения. Иногда весовая матрица декодера является транспонированной весовой матрицы кодера, т.е. $W' = W^t$. В этом случае автоэнкодер имеет связанные веса.

Процедура обучения автоэнкодеров состоит в нахождении набора параметров: $\theta = (W, b_z, b_x)$, которая минимизируют функцию потерь, $L(x, g(f(x)))$, которая измеряет качество реконструкций таким образом, чтобы выходная реконструкция $\hat{x}$ была как можно ближе к исходному входу x. Типичный выбор для функции потерь – это средняя квадратичная ошибка.

$$L\left(x, g\left(f(x)\right)\right) = \|x - \hat{x}\|_2^2 \tag{3}$$

Этот подход имеет ряд преимуществ перед другими методологиями, основанными на моделях контролируемого обучения, которые пытаются классифицировать аномалию в рамках набора заранее определенных аномалий. Во-первых, в ряде приложений, представляющих интерес таких как обнаружение

сбоев, выявление мошенничества или кибербезопасность, могут появляться новые аномалии (например, могут появиться новые атаки или новые виды мошенничества). Узнав, что является нормальным, модель готова даже обнаруживать данные с (аномальными) паттернами, которые никогда не наблюдались во время обучения [5].

Схема применяемого многомерного автоэнкодера на основе LSTM для анализа данных:

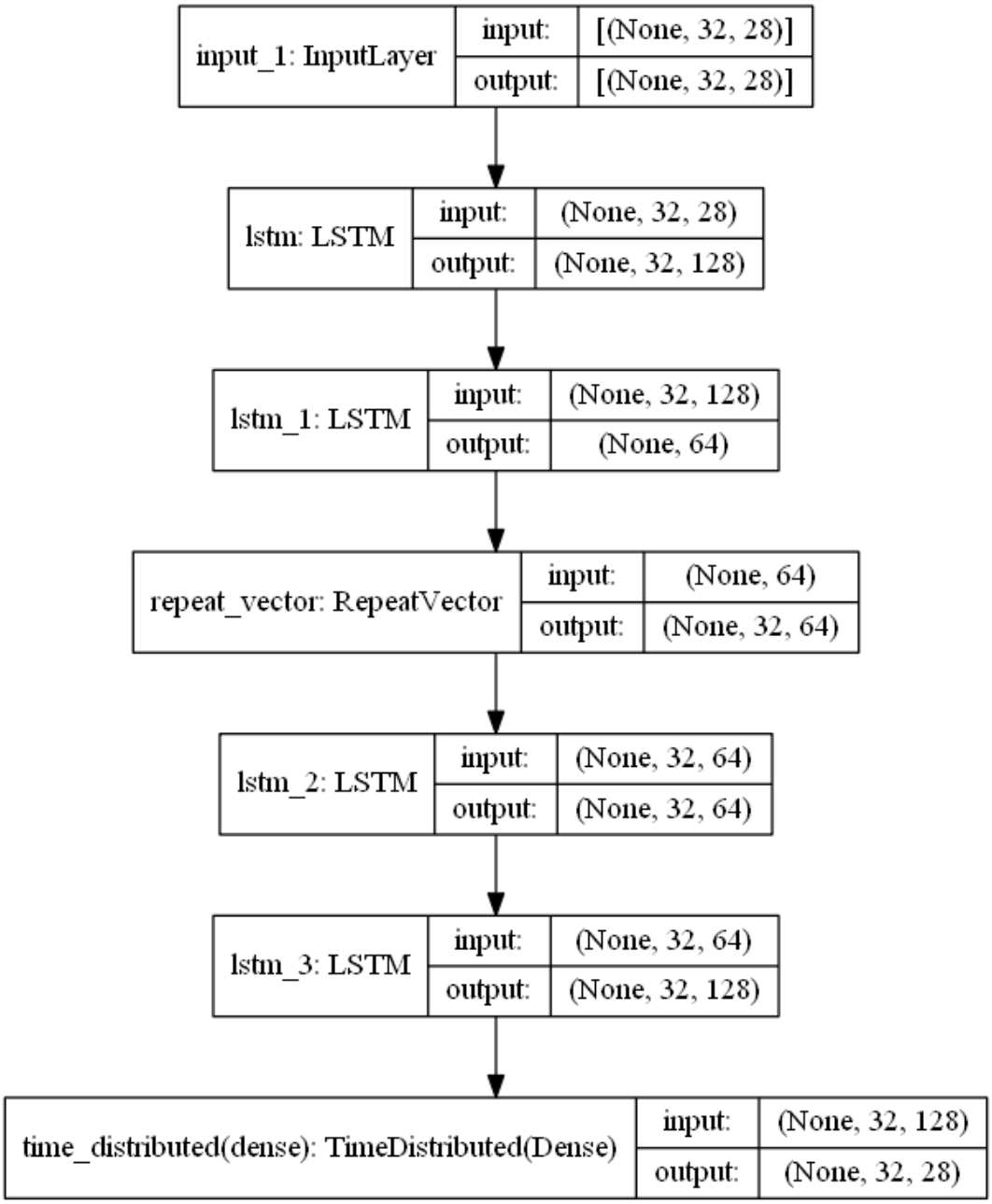


Рис. 6. Схема применяемого многомерного автоэнкодера на основе LSTM

Итоговая модель ансамбля детекторов представлена на рисунке 7.

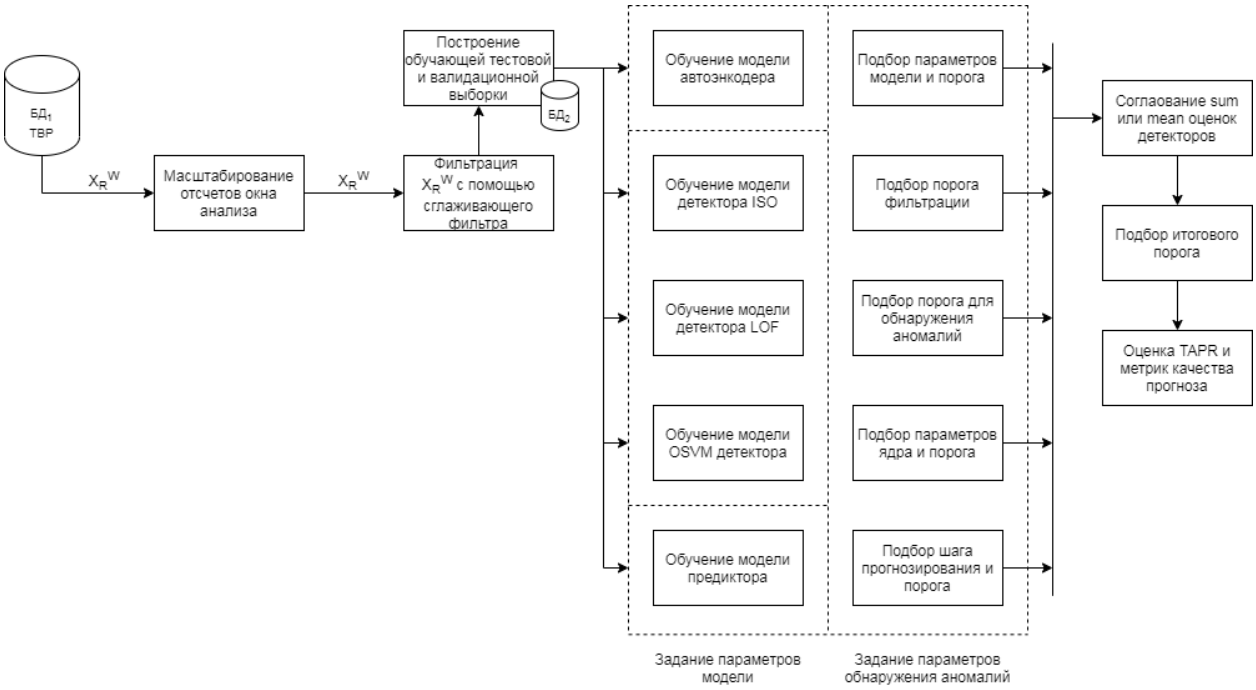


Рис. 7. Модель обнаружения аномалий на основе ансамбля детекторов

СПИСОК ЛИТЕРАТУРЫ

1. Ищем аномалии и предсказываем сбои с помощью нейросетей [Электронный ресурс]. – Режим доступа: https://habr.com/ru/company/krista/blog/478392/
2. Sohrab Mokhtari, Alireza Abbaspour, Kang K. Yen, Arman Sargolzaei A Machine Learning Approach for Anomaly Detection in Industrial Control Systems Based on Measurement Data / Electronics. – 2021. – Т. 10. – №. 407.
3. Соболев К.В. Автоматический поиск аномалий во временных рядах Магистерская диссертация / Соболев Константин Викторович – Москва, 2018.
4. Xingchao Bian Detecting Anomalies in Time-Series Data using Unsupervised Learning and Analysis on Infrequent Signatures / j.inst.Korean.electr.electron.eng. – 2020. . – Т. 24. – №. 4. – С. 1011-1016.
5. João Pereira Unsupervised Anomaly Detection in Time Series Data using Deep Learning / – 2018.

УДК 004.056.5

А. С. АХМЕРОВ, И. Н. РЕЗЯПОВ.
akhmerov.almaz.00@gmail.com rezyapov101100@gmail.ru
Науч. руководв. – доц. В. Е. КЛАДОВ

Уфимский государственный авиационный технический университет

СРАВНИТЕЛЬНЫЙ АНАЛИЗ АЛГОРИТМОВ АСИММЕТРИЧНОГО ШИФРОВАНИЯ RSA И ECC

Аннотация. Задачи данной статьи – провести сравнительный анализ алгоритма асимметричного шифрования RSA и криптографии, основанной на эллиптических кривых. Проанализировать достоинства и недостатки обоих алгоритмов.
Ключевые слова: асимметричное шифрование; RSA; ECC; эллиптическая кривая; криптография; информационная безопасность.

В настоящее время мы живем в цифровом мире, где большая часть наших сообщений или информации обменивается между общающимися пользователями или системами немедленно через цифровые устройства и цифровую сеть. Однако Интернет, будучи открытой архитектурой, имеет некоторые недостатки, благодаря которым перехватчики выполняют кибератаки на передаваемое сообщение. Используя криптографические методы, мы можем обуздать подобные атаки.

Криптография бывает двух видов – симметричная (с закрытым ключом) и асимметричная (с открытым ключом). Несмотря на высокую скорость симметричных криптосистем, они имеют проблемы с распределением ключей и их управлением, в то время как асимметричная криптография обеспечивает распределение ключей.

Одним из самых популярных алгоритмов асимметричного шифрования является алгоритм RSA, придуманный в 1977 году Роном Ривестом, Ади Шамиром и Леонардом Эйдлманом. Данный алгоритм широко используется в наше время как для шифрования данных, так и для электронных подписей. Но он имеет некоторые недостатки, такие как необходимость большой длины ключа для повышения крипостойкости. Соответственно, это повышает и время вычисления. Такую проблему решает криптография на основе эллиптических кри-

вых (ECC – Elliptic Curve Cryptography). Уменьшение длины ключей добивается за счет замены вычисления чисел (как в алгоритме RSA) на вычисления в группах, связанных с эллиптической кривой.

Безопасность зависит от конкретного алгоритма и длины ключа. В приведенной ниже таблице представлено четкое сравнение алгоритмов RSA и ECC, которое показывает, как увеличивается длина ключа по мере увеличения уровня безопасности.

Таблица 1

Длины ключей RSA и ECC

Уровень безопасности (бит)	RSA	ECC
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	512

Как видно из таблицы 1 ключи ECC гораздо короче ключей RSA для одинакового уровня криптостойкости, что позволяет производить необходимые вычисления значительно быстрее.

Рассмотрим, как работают сами алгоритмы RSA и ECC (в виде протокола ECIES).

1. Алгоритм RSA

RSA считается первой реальной и практичной криптосистемой с асимметричным ключом. Его безопасность заключается в проблеме целочисленной факторизации. Процесс дешифрования RSA не так эффективен, как процесс шифрования.

Сам алгоритм состоит из нескольких шагов:

i. Выбрать различные простые числа p и q;

ii. Вычислить n = pq;

iii. Вычислить $\Phi(n) = (p-1)(q-1)$;

iv. Выбрать число e ($1 < e < \Phi(n)$) такое, что НОД($\Phi(n), e$) = 1

v. Вычислить $d \equiv e^{-1}(mod\ \Phi(n))$

vi. Закрытый ключ = {e, n}

vii. Открытый ключ = {d, n}

Для передачи сообщения m от Алисы Бобу, ей потребуется вычислить $C \equiv m^e\ mod\ n$ и передать C Бобу.

Для расшифрования Боб использует открытый ключ d для вычисления D такого, что $D \equiv\ C^d\ mod\ n\ \equiv\ [(m)^e]^d\ mod\ n\ \equiv\ m$

2. Эллиптическая криптография

Вычисления в эллиптической криптографии выполняются над группой точек эллиптической кривой. Эллиптической кривой называют совокупность точек, удовлетворяющих уравнению:

$$y^2 = x^3 + ax + b\ mod\ q$$

Мы можем определить группу для эллиптических кривых. А именно:

– элементы группы являются точками эллиптической кривой;

– единичный элемент — это бесконечно удаленная точка 0;

– обратная величина точки P — это точка, симметричная относительно оси x;

– сложение задается следующим правилом: сумма трех ненулевых точек P, Q, R, лежащих на одной прямой, будет равна P + Q + R = 0 (рис. 1) [3]

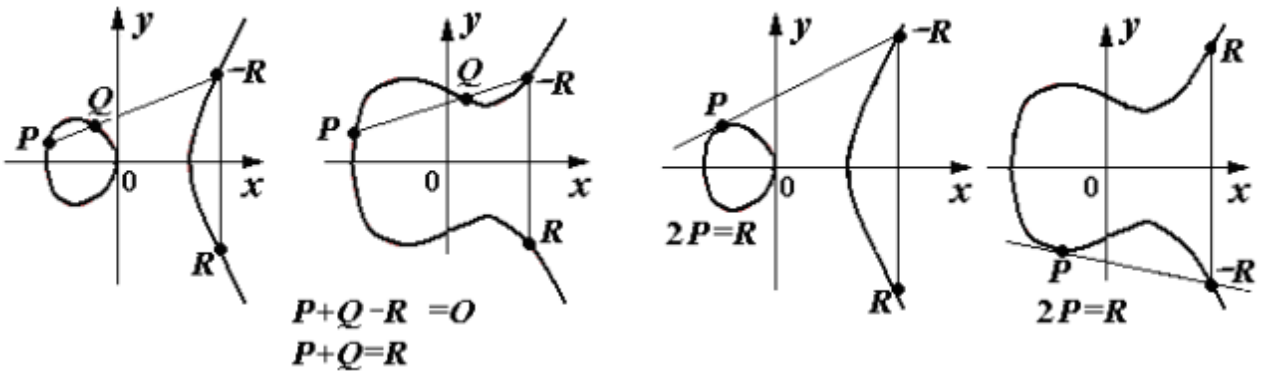


Рис. 1. Сложение и удвоение точек на эллиптической кривой

Алгоритм, основанный на эллиптических кривых (протокол ECIES)

Для передачи информации от Алисы Бобу, им необходимо будет знать следующую информацию:

– KDF (key derivation function) – функция формирования ключа, позволяющая формировать один или несколько ключей на основе секретного значения;

– MAC (message authentication code) – имитовставка, обеспечивающая целостность данных;

– SYM – алгоритм симметричного шифрования;

– $E(\mathbb{F}_p)$ – эллиптическая кривая;

– G – точка на эллиптической кривой (генератор);

– K_B – открытый ключ Боба; $K_B = k_BG$, где k_B – это закрытый ключ Боба.

Чтобы зашифровать сообщение m Алиса производит следующие шаги:

i. Выбрать случайное число k и вычислить R = kG

ii. Вычислить $Z = kK_B$

iii. Создать ключи k_1 и k_2 так, чтобы $(k_1, k_2) = KDF(Z_x, R)$, где Z_x – абсцисса точки Z

iv. Зашифровать сообщение m: $C = SYM(k_1, m)$

v. Сгенерировать имитовставку $t = MAC(k_2, C)$

vi. Отправить Бобу (R, C, t).

Чтобы расшифровать полученное сообщение Бобу потребуется сделать следующее:

i. Проверить принадлежность R эллиптической кривой. Отвергнуть сообщение, если R не принадлежит;

ii. Вычислить $Z = k_BR = k_BkG = kK_B$;

iii. Создать ключи k_1 и k_2 так, чтобы $(k_1, k_2) = KDF(Z_x, R)$, где Z_x – абсцисса точки Z;

iv. Сгенерировать имитовставку t` = MAC(k2, C);

v. Проверить равенство t и t`. Если не равны, сообщение отвергнуть;

vi. Расшифровать сообщение, вычислив $M = SYM^{-1}(k_1, C)$. [4]

3. Сравнение скорости работы алгоритмов

Таблица 2

Время зашифровывания и расшифровывания RSA и ECC

Уровень безопасности (бит)	Зашифровывание		Расшифровывание		Общее время	
	ECC	RSA	ECC	RSA	ECC	RSA
80	0,4885	0,0307	1,32	0,75	1,81	0,78
112	2,2030	0,0299	1,58	2,70	3,78	2,73
128	3,8763	0,0305	1,76	6,94	5,64	6,97
144	4,7266	0,0489	2,00	13,64	6,72	13,69

Как видно из таблицы 2, приведенной выше, шифрование производится быстрее алгоритмом RSA, однако алгоритм, основанный на эллиптических кривых, выигрывает со значительным отрывом в расшифровывании сообщений. Общее время для обоих алгоритмов для низких уровней практически равно, но чем больше уровень безопасности, тем больше разница во времени между двумя алгоритмами в пользу ECC. [1]

Итак, алгоритмы на основе эллиптических кривых являются хорошей альтернативой алгоритму RSA. Криптосистемы на эллиптических кривых имеют надежность, сравнимую с RSA, но с ключами меньшей длины, что делает их идеальным выбором для применения в системах, где малые вычислительные мощности и недостаток памяти предотвращают эффективное применение алгоритма RSA. Алгоритмы, основанные на эллиптических кривых к тому же и значительно быстрее алгоритма RSA, особенно для больших уровней безопасности, что обуславливается применением арифметики на эллиптических кривых, вместо арифметики с действительными числами. [4]

СПИСОК ЛИТЕРАТУРЫ

1. Dindayal Mahto, Dilip Kumar Yadav, 2017 “RSA and ECC: A Comparative Analysis”
2. «RSA vs ECC – Which is Better Algorithm for Security?» [Электронный ресурс] URL: https://www.ssl2buy.com/wiki/rsa-vs-ecc-which-is-better-algorithm-for-security
3. «Доступно о криптографии на эллиптических кривых» [Электронный ресурс] URL: https://habr.com/ru/post/335906/
4. Nelson Josias G. Saho, Eugène C. Ezin, 2020, “Comparative Study on the Performance of Elliptic Curve Cryptography Algorithms with Cryptography through RSA Algorithm”.

УДК 004.056

М. А. БАКУЛИН
misha.bakulin.2013@mail.ru

Уфимский государственный авиационный технический университет

АНАЛИЗ И ПОВЫШЕНИЕ УРОВНЯ ЗАЩИЩЕННОСТИ ЗНАЧИМОГО ОБЪЕКТА КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

Аннотация. Описывается и практически реализовывается порядок анализа и повышения защищенности значимого объекта критической информационной инфраструктуры с учетом выполнения требований нормативно-правовых актов.
***Ключевые слова*:** критическая информационная инфраструктура; объект КИИ; риск нарушения ИБ; категорирование; СЗИ; нечеткая когнитивная карта.

С развитием информационных технологий и распространением сети Интернет практически все сферы деятельности человека были в той или иной степени автоматизированы, а информация стала одним из самых ценных ресурсов любой организации. Общество стало информационным. Потребность людей и организаций в информационных системах стала не простым желанием, а настоящей необходимостью. Без ИС, ИТС и АСУ сегодня невозможна деятельность практически любой организации, а дестабилизирующие воздействия на данные объекты ставят под угрозу жизнь общества. Именно поэтому появилось понятие КИИ, разработана нормативно-правовая база в данной области, а в Уголовный кодекс РФ была добавлена статья 274.1 [1], которая предполагает различные наказания за неправомерные воздействия на КИИ, вплоть до лишения свободы сроком до 10 лет.

Выделено 14 отраслей [2], в которых функционируют объекты КИИ. В связи с чем, количество организаций и компаний, которым необходимо выполнять требования НПА в области обеспечения безопасности КИИ достаточно велико, а СЗИ таких организаций, зачастую не удовлетворяют требованиям. Каждой организации необходимо определить является ли она субъектом КИИ. Если организация относится к категории гос. органов, гос. учреждений, юридических лиц или индивидуальных предпринимателей, и при этом осуществляет свою деятельность, которая относится к одной или нескольким из 14 областей, кото-

рые перечислены в ФЗ № 187 [2], то такая организация является субъектом КИИ и ей необходимо выполнять требования, которые предписаны НПА в области обеспечения безопасности КИИ. Таким образом, вопрос обеспечения безопасности КИИ относится к достаточно большому числу организаций, а модернизация их СЗИ на сегодняшний день является одной из самых актуальных тем в области ИБ, т. к. исходная СЗИ достаточно редко удовлетворяет требованиям, а уровень риска нарушения ИБ у таких субъектов находится на весьма высоком уровне и его необходимо снижать.

Объектом исследования является ГБУЗ РБ Стоматологическая поликлиника города Салават. Организационная структура данного объекта представлена на рисунке 1.

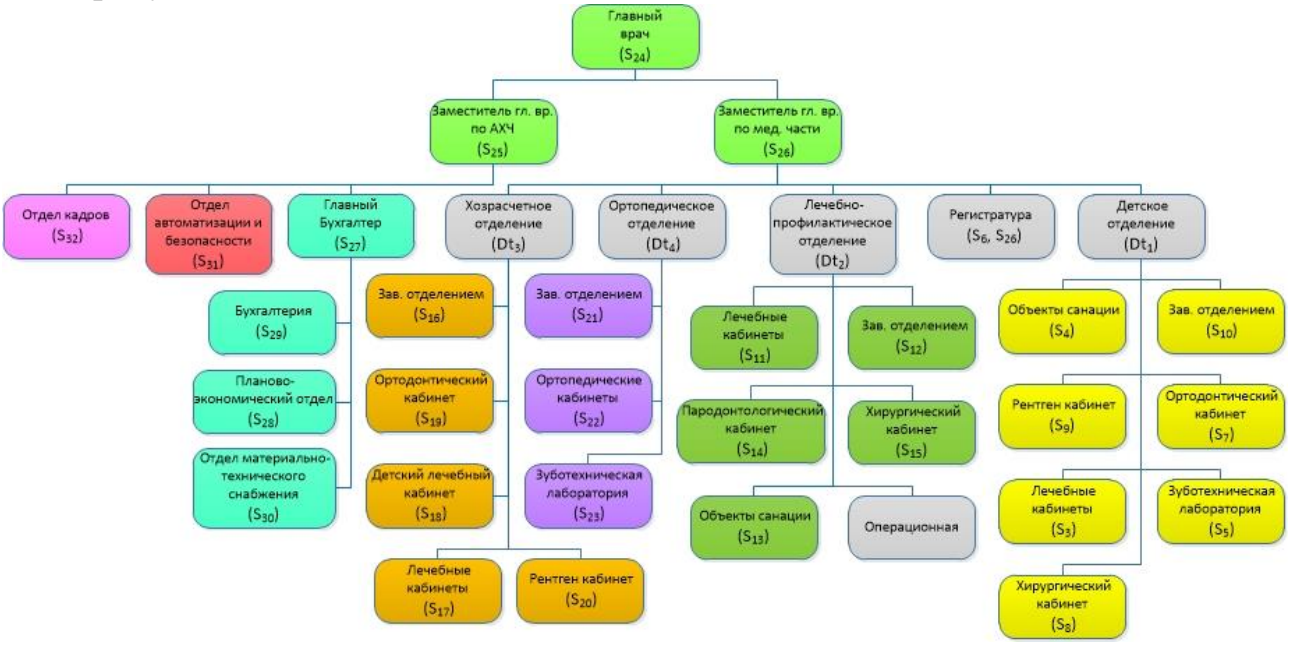


Рис. 1. Организационная структура

Данная стоматология имеет два отдельных здания:

– головное здание. В этом здании находится руководство, а именно главный врач (S_{24}) и его заместитель по АХЧ (S_{25}) и заместитель по мед. части (S_{26}), стоматологические отделения ($Dt_{2\text{-}4}$), отдел кадров (S_{32}), отдел автоматизации и безопасности (S_{31}), материально-финансовый отдел ($S_{27\text{-}30}$), регистратура (S_{33}) и серверный сегмент (S_{34});

– детское стоматологическое отделение. В данном здании находится непосредственно само детское отделение (D_1), регистратура (S_6) и серверный

сегмент (S_{35}). Данное отделение имеет связь с головным зданием через сеть Интернет.

Помимо ЛВС самой стоматологической поликлиники следует выделить также РИАМС «ПроМед» и Call-центр. Все электронные-медицинские карты пациентов хранятся в центре обработки данных РИАМС «ПроМед», а сотрудники поликлиники имеют к нему доступ через веб-браузер. Данный центр также автоматизирует запись на прием к врачу. Общедоступный сервер эл. почты как в детском отделении (D_3), так и в головном здании (C_3), не выделен в демилитаризованную зону, соответственно, необходима также реорганизация сети. Топология ЛВС представлена на рисунке 2.

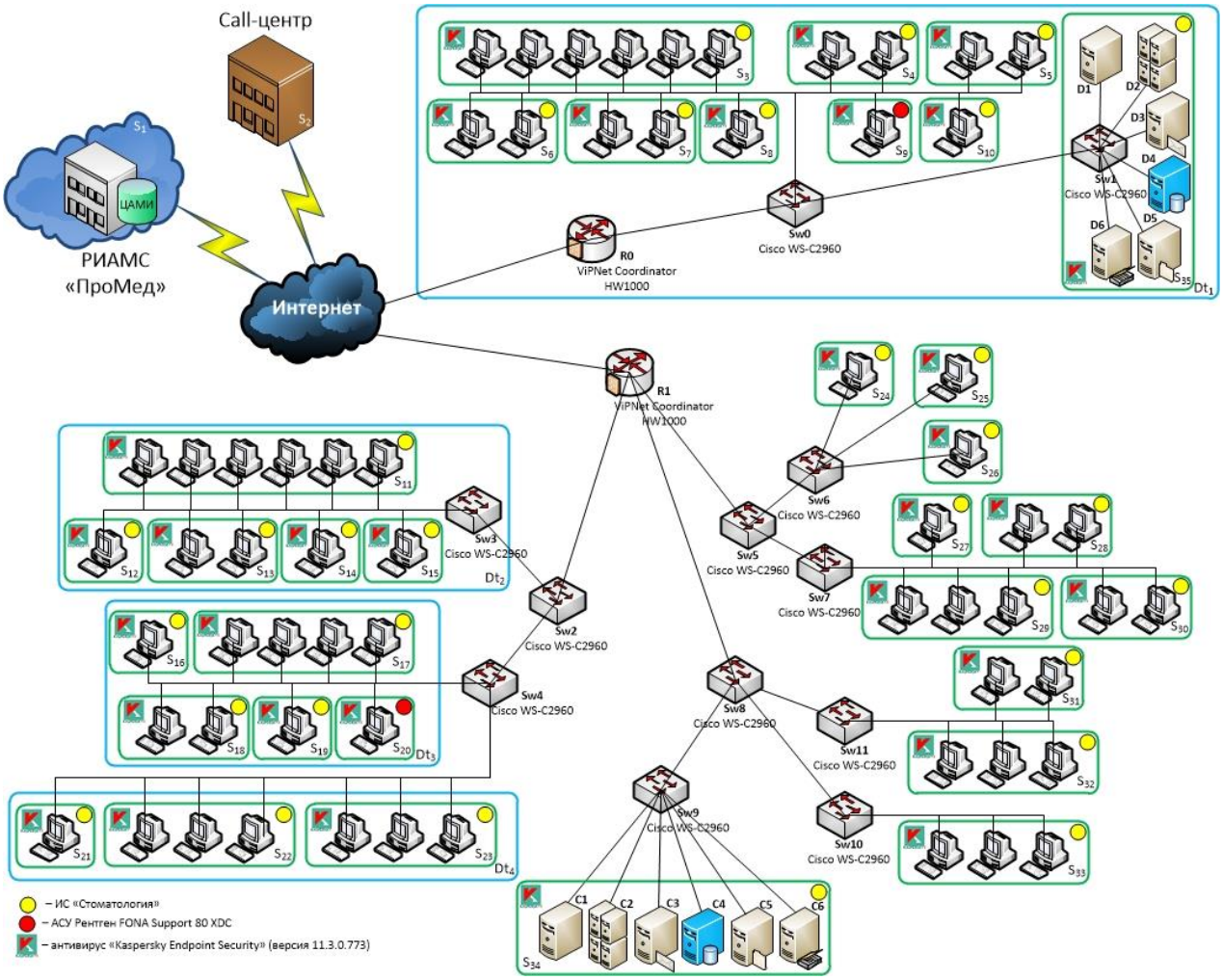


Рис. 2. Топология ЛВС

На объекте защиты функционируют следующие СрЗИ:

– антивирус. На всех АРМ и серверах установлен антивирус «Kaspersky Endpoint Security для Windows (версия 11.3.0.773)». Данный антивирус имеет 2

класс защиты АРМ и 2 класс защиты серверов. Имеет действующий сертификат до 22.01.2024;

– МЭ. В качестве МЭ используется ПАК ViPNet Coordinator HW1000, который также выполняет функции маршрутизации. У данного СрЗИ вышел срок действия сертификата 26.05.2020. Соответственно его можно использовать пока предоставляется техническая поддержка, но данная поддержка также закончилась 26.05.2020. Таким образом, данное СрЗИ необходимо заменить.

В качестве коммуникационного оборудования используются следующие устройства:

– маршрутизатор. Функции маршрутизатора выполняет ПАК ViPNet Coordinator HW1000;

– коммутатор. Используются коммутаторы второго уровня (L2) Cisco WS-C2960+24PC-L, которые имеют по 24 порта Ethernet 100 Мбит/с.

Далее необходимо проанализировать протекающие бизнес-процессы. Под бизнес-процессом понимают несколько взаимосвязанных операций и процедур, которые в совокупности реализуют некоторую цель, осуществляемой обычно в рамках организационной структуры, которая определяет отношения между участниками. В данной стоматологической поликлинике функционируют бизнес-процессы, представленные в таблице 1.

Таблица 1

Перечень бизнес-процессов

Бизнес-процесс	Обозначение связи
1	2
запись на прием в регистратуре (офлайн) и электронная запись (онлайн)	1
уведомление пациентов о записи на прием	2
направление на рентген ротовой полости	3
оказание лечебных стоматологических услуг	4
оказание услуг санации полости рта	5
оказание услуг ортодонта	6
оказание услуг стоматологического хирурга	7
снятие рентгеновского снимка	8
изготовление зубных имплантов, протезов и эстетических конструкций	9
оказание услуг по лечению и профилактике околозубных тканей	10
установка протезов и эстетических конструкций	11
фиксация термометрии сотрудников и пациентов с целью профилактики COVID-19	12

Окончание табл. 1

1	2
назначение заработных плат сотрудникам	13
формирование документов на поставку нового оборудования, медикаментов и предметов мебели	14
составление расписания работы сотрудников, а также прием и увольнение сотрудников	15
оформление документов на повышение квалификации сотрудников	16
направление пациента на операцию	17
оплата платных стоматологических услуг	18
разработка политики управления стоматологией, плановых и отчетных форм	19
оформление отчетов о движении денежных средств	20
ведение списка сотрудников	21
руководство над отделениями и контроль выполнения планов	22
обеспечение работы оборудования и вычислительной техники	23
списание стоматологического оборудования, техники и мебели	24

Графическая модель бизнес-процессов представлена на рисунке 3.

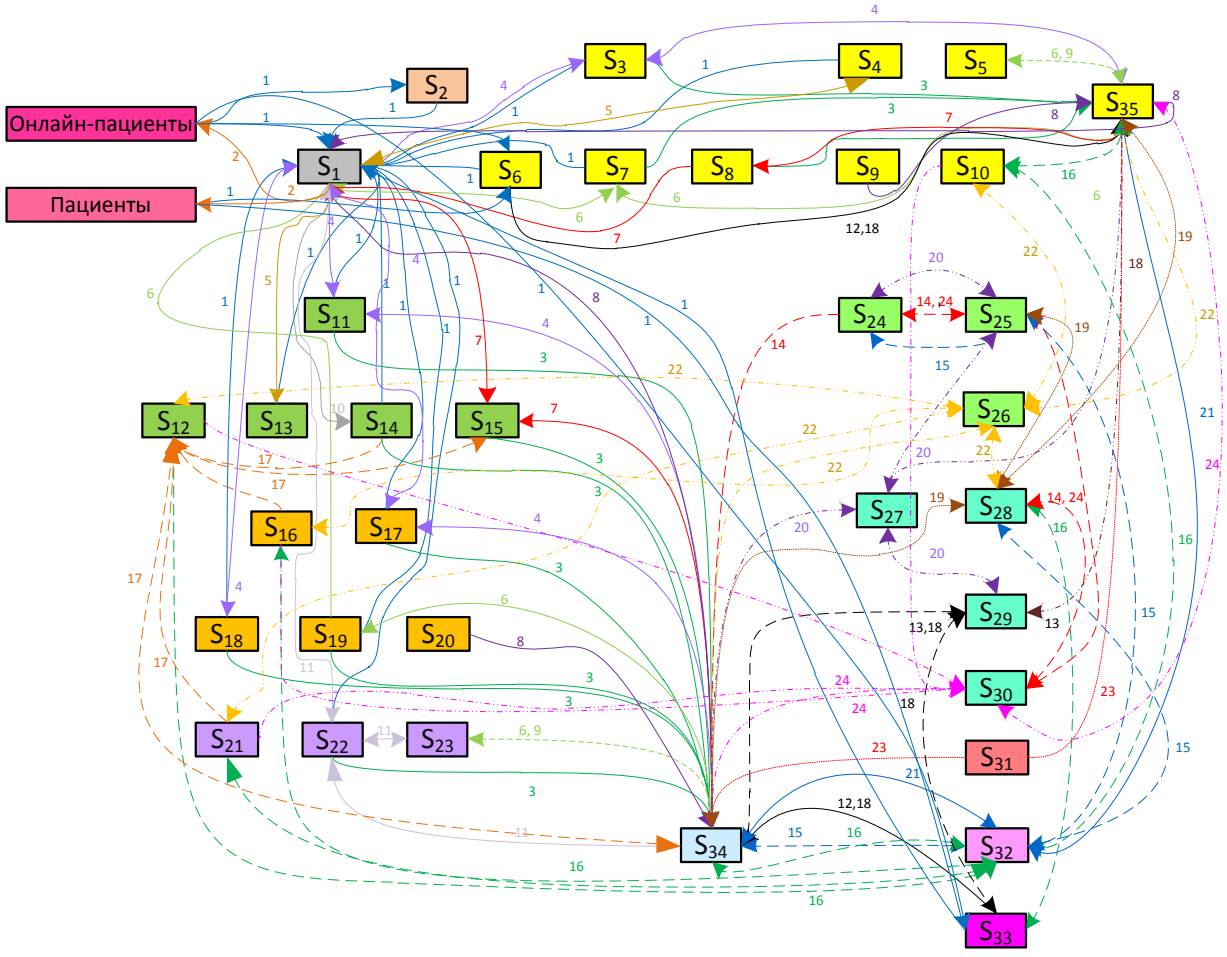


Рис. 3. Модель бизнес-процессов

Для того, чтобы построить эффективную СЗИ и выполнить требования НПА, необходимо произвести категорирование имеющихся объектов КИИ в

соответствии с ПП №127 [3]. Только после того, как будет установлена категория значимости, можно составлять меры обеспечения безопасности для полученной категории и определять и внедрять СрЗИ, реализующие данные меры.

Прежде чем приступать к категорированию, необходимо первым делом сформировать перечень объектов КИИ. Любой протекающий информационный бизнес-процесс, не может протекать без соответствующей техники, линий связи и т. д. Таким образом, в соответствии с ПП №127 [3] для формирования такого перечня необходимо сначала определить все протекающие бизнес-процессы и выделить среди них критические. Все бизнес-процессы были определены ранее, а критические процессы и объекты КИИ, которые обеспечивают выполнение данных процессов, представлены в таблице 2.

Таблица 2

Критические бизнес-процессы

№ п/п	Объект КИИ	Тип объекта	Обеспечиваемый критический процесс
1.	Рентген FONA Support 80 XDC	АСУ	3, 8
2.	ИС «Стоматология»	ИС	3, 4, 6, 7, 8, 11, 13, 17, 18, 23
3.	ЛВС организации	ИТС	1, 3, 4, 5, 6, 7, 8, 10, 11, 13, 17, 18, 23

Таким образом, выделено три объекта КИИ. Для каждого значимого объекта (ЗО) также необходимо определить одну из трех возможных категорий значимости. По результатам оценки, все три объекта КИИ являются значимыми и имеют 3 категорию значимости.

Чтобы СЗИ удовлетворяла требованиям НПА необходимо первым делом составить базовый набор мер обеспечения безопасности, которые были определены в соответствии с приказом ФСТЭК № 239 [4] для соответствующей категории значимости.

После определения базового набора мер нужно адаптировать его. При определении адаптированного набора мер учитывается специфика рассматриваемой организации. На объекте защиты не используются следующие технологии и средства:

− система обеспечения единого времени. Следовательно, мера АУД.3 является избыточной;

− беспроводные соединения. Беспроводные точки доступа не используются, соответственно, мера ЗИС.32 является избыточной;

− мобильные устройства. Мобильные устройства для выхода в сеть также не используются, соответственно, мера ЗИС.38 является избыточной;

− виртуальные машины. В данной стоматологии виртуальные машины не используются, следовательно, мера ЗИС.39 является избыточной.

Таким образом, согласно мерам обеспечения безопасности ЗО, нужно внедрить (заменить) следующие средства защиты информации (СрЗИ):

– МЭ – заменить по причине отсутствия у имеющихся МЭ действующего сертификата;

– СЗИ от НСД – внедрить по причине отсутствия;

– СКЗИ – заменить по причине отсутствия у имеющихся СКЗИ действующего сертификата;

– СДЗ – внедрить по причине отсутствия;

– сканер безопасности сети – внедрить по причине отсутствия.

В результате выбора рационального набора СрЗИ и коммуникационного оборудования были выбраны средства, представленные в таблице 3.

Таблица 3

Внедряемые СрЗИ

Компонент		Стоимость за шт. (руб.)	Количество	Итоговая стоимость (руб.)
Тип	Название			
1	2	3	4	5
МЭ	Cisco Firepower 2110	264000	2	528000
СЗИ от НСД	Secret Net Studio (версия 8.6) компонент «Клиент»	5750	72	414000
	Secret Net Studio (версия 8.6) компонент « Сервер безопасности»	15500	2	31000
	Secret Net Studio (версия 8.6) компонент «Центр управления»	9400	1	9400
СДЗ	Программно-аппаратный комплекс «Соболь». Версия 4»	10868	75	815100
Сканер безопасности	RedCheck	–	75	115000

Окончание табл. 3

1	2	3	4	5
СКЗИ	«КриптоПро CSP» версия 5.0 КС3 (исполнение 3-Base)	2700	63	170100
Маршрутизатор	Cisco 1100-4P	52700	1	52700
Итого				2135300

Итоговая стоимость модернизации СЗИ составила 2135300 руб.

Требуется также реорганизация ЛВС по причине присутствия в сети общедоступного сервера эл. почты, который не выделен в демилитаризованную зону. Соответственно, необходимо на коммуникационном оборудовании произвести настройку такой зоны в детском отделении и головном здании, а почтовый сервер как в детском отделении (D_3), так и в головном здании (C_3) выделить в демилитаризованную зону. Схема ЛВС после реорганизации с учетом модернизации СЗИ представлена на рисунке 4.

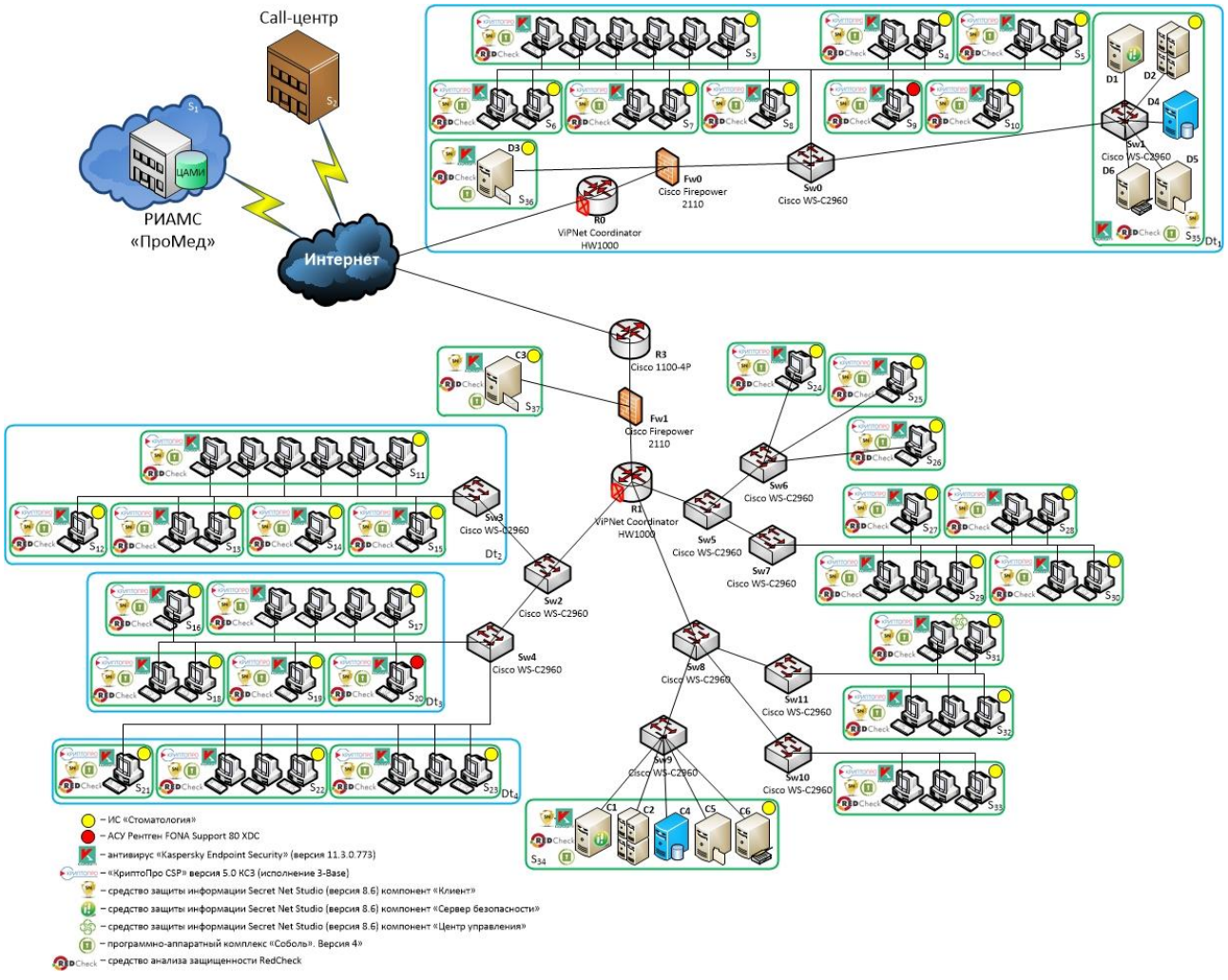


Рис. 4. ЛВС после реорганизации с учетом модернизации СЗИ

Чтобы оценить исходный уровень защищенности и эффективность модернизированной СЗИ необходимо построить нечеткую когнитивную карту (НКК) и рассчитать риск нарушения ИБ до модернизации СЗИ, после модернизации СЗИ и после реорганизации сети с учетом модернизации СЗИ.

Построенная НКК до модернизации СЗИ представлена на рисунке 5.

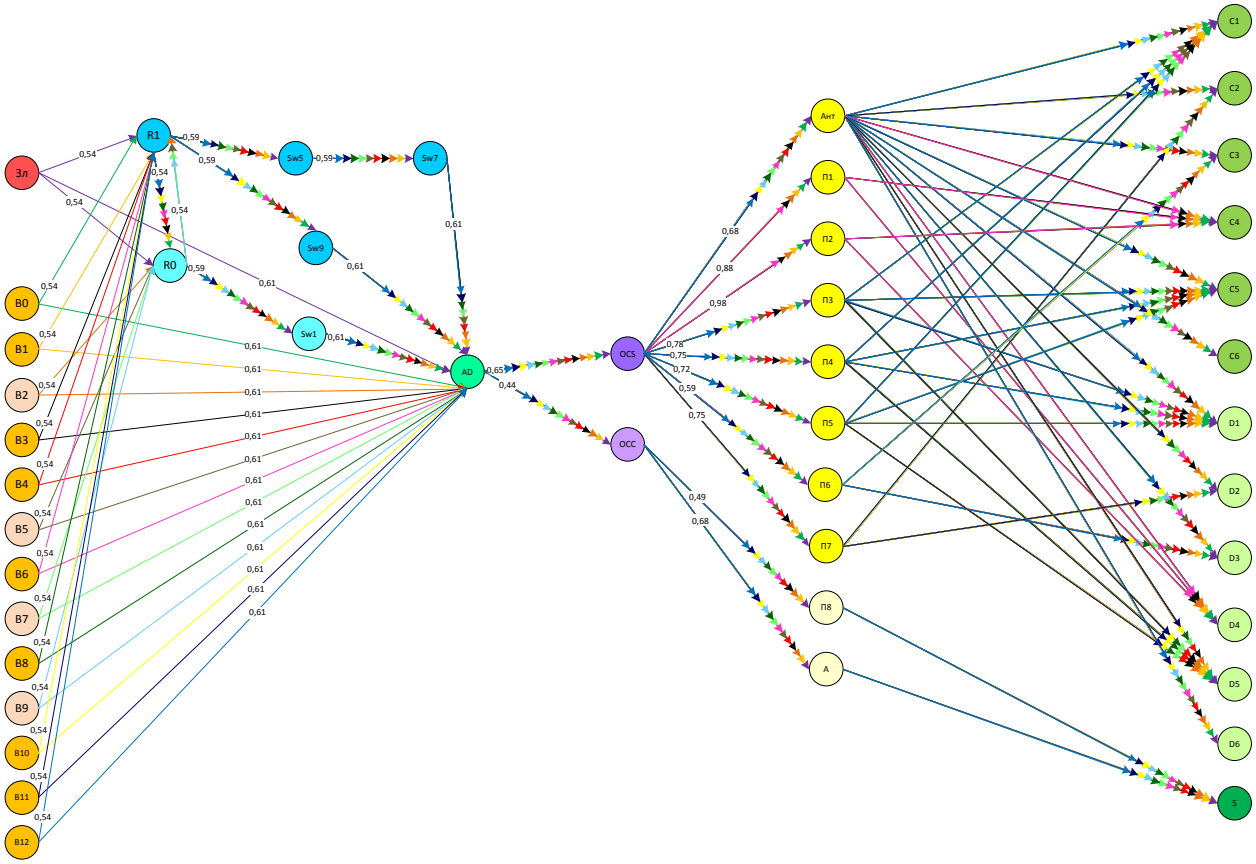


Рис. 5. НКК до модернизации СЗИ

Результаты произведенных вычислений результирующего уровня угроз для каждого объекта атаки и уровня риска как для каждого объекта атаки, так и для всей системы представлены в таблице 4.

Таблица 4

Результирующие уровни угроз, уровни риска

Объекты атаки		Результирующий уровень угроз	Уровень риска
Сегмент	Ценность		
1	2	3	4
$S_{27\text{-}30}$	0,2	0,128499163	0,0257
D_1	0,06	0,177827441	0,0107
D_2	0,05	0,130356485	0,0065
D_3	0,055	0,539781199	0,0297
D_4	0,085	0,098760615	0,0084
D_5	0,055	0,247249999	0,0136

Окончание табл. 4

1	2	3	4
D_6	0,045	0,160500355	0,0072
C1	0,085	0,214809606	0,0183
C2	0,056	0,246252081	0,0138
C3	0,07	0,539781199	0,0378
C4	0,094	0,129612877	0,0122
C5	0,085	0,441611512	0,0375
C6	0,06	0,189883483	0,0114
Итог			0,2327

Таким образом, риск нарушения ИБ до модернизации СЗИ и до реорганизации сети составил 23,27%. Значение риска достаточно высокое, что подтверждает необходимость модернизации СЗИ и реорганизация сети.

НКК после модернизации СЗИ представлена на рисунке 6.

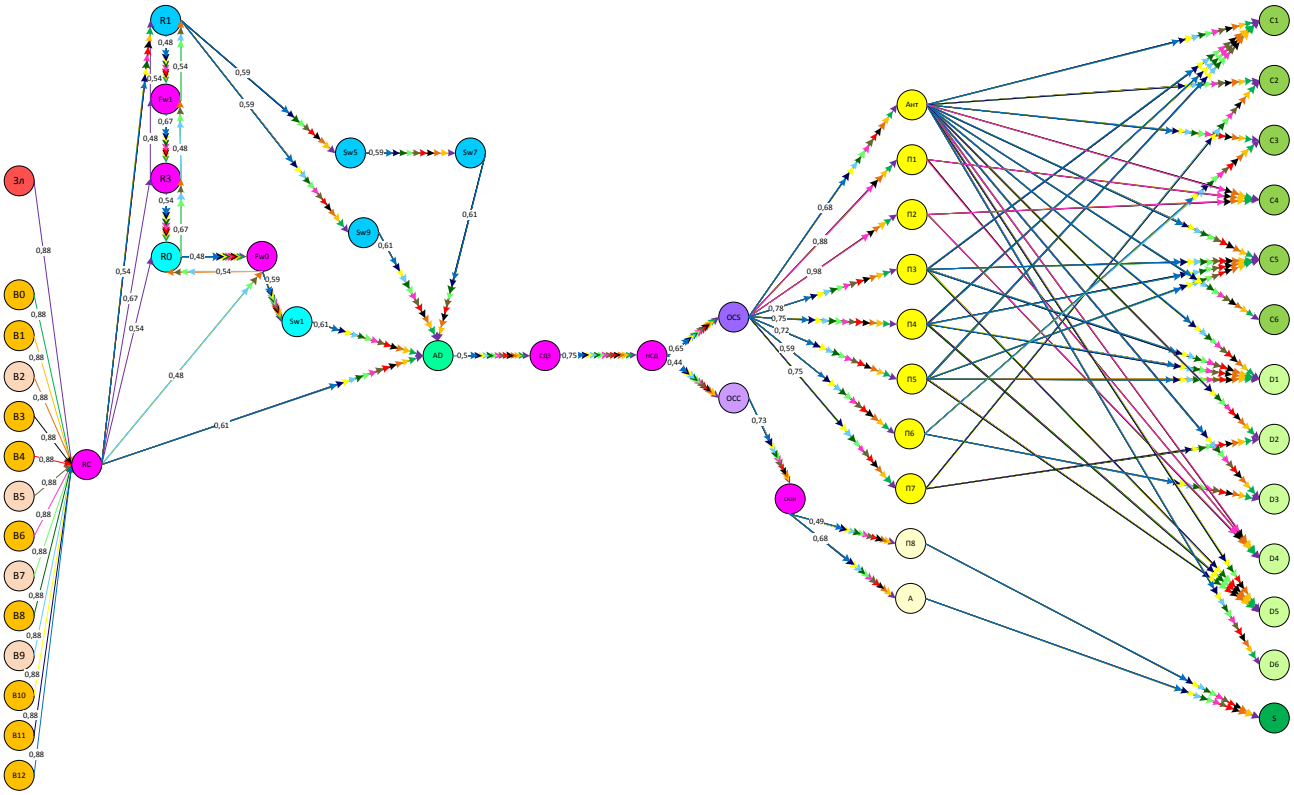


Рис. 6. НКК после модернизации СЗИ

Результаты произведенных вычислений представлены в таблице 5.

Таблица 5

Результирующие уровни угроз, уровни риска

Объекты атаки		Результирующий уровень угроз	Уровень риска
Сегмент	Ценность		
1	2	3	4
$S_{27\text{-}30}$	0,2	0,029741208	0,0059

Окончание табл. 5

1	2	3	4
D_1	0,06	0,020303372	0,0012
D_2	0,05	0,013102464	0,0007
D_3	0,055	0,222267113	0,0122
D_4	0,085	0,010528792	0,0009
D_5	0,055	0,068343794	0,0038
D_6	0,045	0,017939322	0,0008
C_1	0,085	0,061040188	0,0052
C_2	0,056	0,07238358	0,0041
C_3	0,07	0,222267113	0,0156
C_4	0,094	0,035484634	0,0033
C_5	0,085	0,160735162	0,0137
C_6	0,06	0,05340709	0,0032
Итог			0,0705

Таким образом, риск нарушения ИБ после модернизации СЗИ без реорганизации сети составил 7,05%. За счет модернизации СЗИ удалось снизить риск нарушения ИБ на 16,22% или в 3,3 раза. Это говорит об эффективности внедренных СрЗИ.

Далее необходимо построить НКК после реорганизации сети с учетом модернизации СЗИ. Результаты построения представлены на рисунке 7.

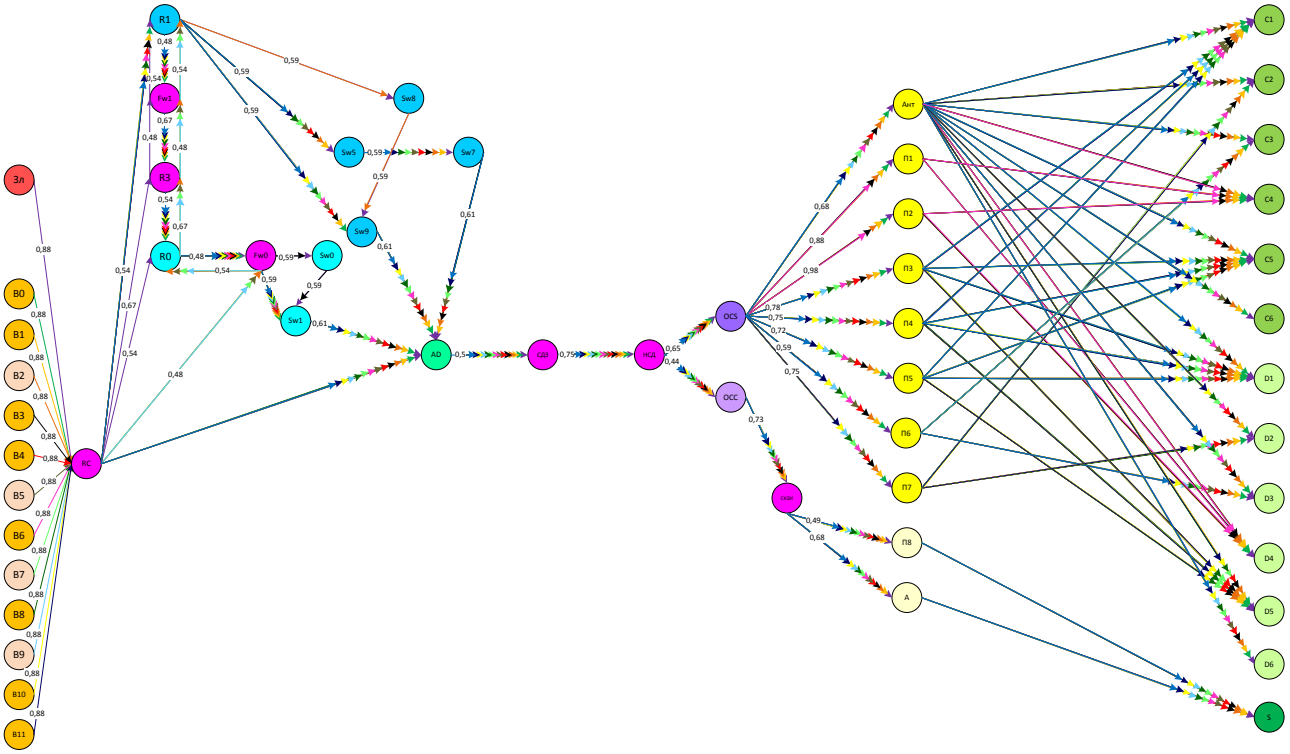


Рис. 7. НКК после реорганизации сети с учетом модернизации СЗИ

Результаты аналогичных вычислений представлены в таблице 6.

Таблица 6

Результирующие уровни угроз, уровни риска

Объекты атаки		Результирующий уровень угроз	Уровень риска
Сегмент	Ценность		
$S_{27\text{-}30}$	0,2	0,020357899	0,0041
D_1	0,06	0,016239231	0,0010
D_2	0,05	0,010063567	0,0005
D_3	0,055	0,194503484	0,0107
D_4	0,085	0,007459359	0,0006
D_5	0,055	0,057873049	0,0032
D6	0,045	0,01428174	0,0006
C1	0,085	0,051911416	0,0044
C2	0,056	0,061582603	0,0034
C3	0,07	0,194503484	0,0136
C4	0,094	0,029496123	0,0028
C5	0,085	0,139144235	0,0118
C6	0,06	0,04539445	0,0027
Итог			0,0595

Таким образом, в результате реорганизации сети удалось снизить риск еще на 1,1% или в 1,18 раза. Исходный риск нарушения ИБ составлял 23,27%. В результате модернизации СЗИ и реорганизации сети его удалось снизить до 5,95%, т. е. на 17,32% или в 3,91 раза, что говорит об эффективности произведенных действий.

Таким образом, цель работы выполнена в полном объеме: требования НПА в области обеспечения безопасности ЗО КИИ субъектом КИИ выполнены, разработанная модель модернизации СЗИ и реорганизации сети эффективна, что доказано результатами вычислений рисков нарушения ИБ.

СПИСОК ЛИТЕРАТУРЫ

1. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 05.04.2021, с изм. от 08.04.2021);
2. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»;
3. Постановление Правительства РФ от 08.02.2018 № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений»;
4. Приказ ФСТЭК от 25.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации

УДК 004.056

А. Р. БИКТАШЕВА, Т. Ф. МАЛИКОВ, Р. Т. КУДРЯВЦЕВА
bikalba@mail.ru, malikovtf1@gmail.com, cudrt@mail.ru
Науч. руководитель – канд. техн. наук, доц. Р. Т. КУДРЯВЦЕВА

Уфимский государственный авиационный технический университет

КВАНТОВАЯ КРИПТОГРАФИЯ КАК МЕТОД ЗАЩИТЫ ИНФОРМАЦИИ

Аннотация. В данной статье описан принцип работы технологии квантового распределения ключей. Рассмотрены основные протоколы квантовой криптографии. Приведены недостатки и уязвимости квантовых коммуникаций.
Ключевые слова: квантовая криптография; информационная безопасность; квантовые алгоритмы; протокол; квантовое распределение ключей; фотон.

Введение

В современном информационном обществе существует большое и постоянно нарастающее количество информационных ресурсов, требующих надежных методов защиты от несанкционированного доступа. Актуальной и востребованной стала проблема применения квантовых технологий в области обеспечения системы информационной безопасности и защиты конфиденциальной информации, передаваемой по открытым каналам связи [1].

Квантовые вычисления как средство защиты информации

Угроза квантовых вычислений породила новые подходы к защите информации. Первый подход - постквантовая криптография - предлагает использовать алгоритмы шифрования, базирующиеся на математических задачах, которые сложны как для классических вычислений, так и для квантовых. Второй подход - квантовая криптография - для обеспечения секретности информации использует основные законы квантовой механики. В квантовой криптографии можно выделить следующие основные направления: технологии квантовой передачи данных; технологии квантового распределения ключей; квантовое шифрование; технологии квантовой цифровой подписи, технологии квантового хеширования.

Математически было доказано, что квантовые каналы передачи данных являются самыми безопасными, что позволяет получить новый уровень защиты информации. Носителем информации, которая зашифрована с использованием законов квантовой механики, в данном случае будет квантовый объект, например, фотон. Согласно фундаментальным законам квантовой физики измерение квантового объекта или любое другое воздействие на него приводит к изменению его состояния. Из этого следует, что попытка перехватить сообщение или прослушивание канала приведет к изменению состояния фотона, что сразу же станет известно получателю.

Квантовые каналы передачи данных являются основой для реализации алгоритмов квантового распределения ключей -главного направления развития квантовой криптографии.

Технология квантового распределения ключей (далее - КРК) позволяет распределять ключи между удаленными пользователями по открытым каналам связи, основываясь на законах квантовой физики. Технология КРК строится на невозможности копирования неизвестного квантового состояния; невозможности прослушать сигнал; невозможности абсолютно надежно различить два неортогональных квантовых состояния [3].

Все протоколы КРК работают по следующему принципу: Алиса (отправитель) задает квантовые состояния фотонов и передает по квантовым каналам передачи данных. Боб (получатель) получает фотоны и регистрирует их состояния. Если Алиса и Боб заранее не договорились, какой вид поляризации фотонов будет выбран, тогда Боб разрушит полученный сигнал. Имело ли место прослушивание при передаче ключа Алиса и Боб смогут определить, сравнивая переданные и полученные данные. Метод сравнения определяется каждым протоколом КРК.

Главным требованием к абсолютно стойким шифрам заключается в том, что ключ для него должен быть равен по длине или превосходить длину кодируемого сообщения [2]. Однако учеными было доказано, что в квантовой крип-

тографии ключ может быть короче самого сообщения. Была реализована абсолютно стойкая система квантового шифрования, которая позволяет передавать шесть бит информации в каждом фотоне, при этом длина ключа меньше чем длина сообщения. Это позволяет передавать новый ключ внутри основного сообщения.

Основные протоколы квантовой криптографии

Протоколы квантового распределения ключа описывают механизм работы квантовой связи. Первым из них был протокол BB84, который и сегодня активно используется во многих коммерческих системах. Работает он так.

Для передачи информации используются поляризованные фотоны. Алиса поляризует фотоны в двух разных базисах — под углом 0 и 90 градусов, либо 45 и 135 градусов, причем базисы она выбирает каждый раз случайным образом. Затем Боб получает фотоны и измеряет их состояния, тоже выбирая базисы случайно. После этого Алиса по открытому каналу сообщает Бобу набор использованных базисов, Боб отбрасывает несовпавшие базисы и говорит Алисе, какие данные не прошли. При этом сами результаты измерений по открытому каналу не передаются. Несмотря на это, у Алисы и Боба оказывается ключ — одинаковая последовательность нулей и единиц. Если Ева захочет перехватить данные, она должна будет измерять поляризацию фотонов. Она не знает базиса, поэтому, если не угадает правильно, не получит верных данных. Кроме того, само измерение изменит поляризацию, и ошибки обнаружат и Алиса, и Боб.

В случае протокола BB84 допустимый уровень ошибок, вызванных разными причинами, — 11 процентов, если он выше, то считается, что канал прослушивается. Этот протокол в модернизированном виде может обеспечивать скорость передачи 2,38 мегабит в секунду на дистанции 25 километров, и 52 килобита в секунду — на дистанции 70 километров [4].

Аналогом протокола BB84, в котором для передачи данных используется не поляризация, а фаза фотонов, является протокол B92, предложенный Бенне-

том в 1992 году. Одно из его преимуществ — увеличенная скорость генерации квантовых битов по сравнению с BB84.

Более современные протоколы DPS и COW позволяют обеспечить большую дальность передачи — до 250 и даже 300 километров. Однако для этих двух протоколов еще нет строгого доказательства защищенности.

В протоколе E91 используется явление квантовой запутанности. Суть его в том, что Алиса и Боб получают квантово запутанные пары фотонов и при измерении получают связанные значения. Однако этот протокол пока считается экзотикой, так как создание запутанных пар фотонов — сложная и ресурсоемкая задача.

Недостатки и уязвимости квантовых коммуникаций

Кодировать данные в квантовых состояниях достаточно сложно, поскольку для этого необходимо уметь генерировать и детектировать одиночные фотоны, что само по себе непростая технологическая задача. Кроме того, квантовые состояния уязвимы и могут разрушаться под действием тепловых шумов и других помех. Наконец, реальные квантовые устройства, в отличие от идеальных, могут быть уязвимы для некоторых типов атак.

Рассмотрим недостатки квантовой криптографии поподробнее.

1. Ограничения скорости и дальности передачи данных. Квантовая связь сегодня возможна только на ограниченных расстояниях. Лучшие лабораторные образцы квантовых систем едва преодолели порог дальности 400 километров, при этом они обеспечивают крайне низкую по современным стандартам скорость — около 1 бита в секунду. Поэтому существующие квантовые сети в основном обеспечивают защищенную связь на расстояниях в десятки километров. Их используют, например, для передачи данных между офисами банков в пределах крупного города.

Решением проблемы может быть создание квантовых сетей из «отрезков», связанных между собой специальными «доверенными» узлами, способными принимать, читать и передавать дальше квантовые данные.

Второй вариант — использование космических технологий: потери фотонов в атмосфере и космосе относительно невелики по сравнению с поглощением в оптоволокне, поэтому спутник-ретранслятор может обеспечить квантовую связь на дистанции в тысячи километров.

2. Детекторы и источники одиночных фотонов. Развитие квантовой связи сдерживает отсутствие дешевых и эффективных источников и приемников одиночных фотонов. При их создании разработчикам приходится искать компромисс между быстродействием устройств, равномерностью свойств излучения и «чистотой» квантовых состояний.

Например, лучшие детекторы фотонов, обладающие низким уровнем темновых отсчетов (срабатываний в отсутствие фотонов) и высокой скоростью счета (до 1 гигагерца) основаны на сверхпроводниковых технологиях и требуют криогенных температур — до 2 кельвин (-271 градус Цельсия), что неудобно при эксплуатации вне лабораторий и сильно увеличивает стоимость устройств [5].

3. Квантовый взлом. Теоретически квантовые устройства должны обеспечивать абсолютную защиту для передаваемых данных. Однако реальные системы имеют уязвимости.

Например, был продемонстрирован «взлом» коммерческой системы квантовой связи фирмы ID Quantique с помощью ослепления детектора фотонов сильными лазерными импульсами. Уязвимость была ликвидирована, но эксперимент показал, что квантовая криптография может быть взломана. На сегодняшний день известны методы атак на фотодетекторы, модуляторы, источники фотонов и другие компоненты квантовых устройств.

Заключение

В связи с интенсивным развитием инновационных технологий особое значение приобретают исследования квантовых технологий. Проведение экспериментов и исследований по обеспечению информационной безопасности представляет большой научный интерес по поиску решения основных задач и проблем, стоящих перед квантовыми криптографическими системами: задача

детектирования единичных фотонов с высокой вероятностью в заданном квантовом состоянии при низком уровне ложных срабатываний, отсутствие управляемых источников одиночных фотонов, проблема увеличения дальности передачи и малая скорость генерации квантового ключа.

СПИСОК ЛИТЕРАТУРЫ

1. Емельянов В.И. Квантовая физика: биты и кубиты. Учебное пособие. / В.И. Емельянов, Ю.В. Владимирова – М.: Физический факультет МГУ, 2012. С. 52-53.
2. Квантовая криптография / шифрование [Электронный ресурс] URL: https://www.tadviser.ru/index.php/Статья:Квантовая_криптография_(шифрование), 2021.
3. Шемякина М.А. Анализ использования квантовых технологий в криптографии // Международный журнал гуманитарных и естественных наук. 2019. №5-4.
4. Molotkov S.N. On the secrecy of a simple and effective implementation of bb84 quantum cryptography protocol. //Laser Physics Letters.2019. 203–213.
5. Pljonkin A., Petrov D., Sabantina L., Dakhkilgova K. Nonclassical Attack on a Quantum Key Distribution System. Entropy. 2021. 23.

УДК 004.056.53

Г. Д. ВАЛИАХМЕТОВ, Т. А. БИКБУЛАТОВ
germanvaliah@gmail.com
Науч. руководов. – канд. техн. наук, доц. Т. А. ИВАНОВА

Уфимский государственный авиационный технический университет

УГРОЗЫ И РИСКИ ДЛЯ КАНАЛОВ СВЯЗИ РАСПРЕДЕЛЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

Аннотация. В статье рассмотрены проблемы, связанные с информационной безопасностью, которые возникают из-за потери доступа к защищенному ресурсу. Проанализированы технические аспекты, а также ответственность должностных лиц при возникших условий работы системы.
***Ключевые слова*:** защищенный канал связи; информационная безопасность; ФСТЭК; модель угроз; КИИ; ГИС.

Человечество переживает одну промышленную революцию за другой. Первая и вторая промышленная революции подарили человечеству мануфактуры и фабрики. Благодаря ним возросло производство и труд человека обрел специализации. Третья промышленная революция объявила переход к цифровым технологиям и повсеместной автоматизации труда. Четвертая промышленная революция начала трансформировать не только производство, но и услуги, и сервис для обычных людей. Началась эпоха цифровизации, когда все больше и больше услуг предоставляемых людям стали оказываться в цифровом виде. Как ни странно, это затронуло не только частный бизнес, но и государственный сектор. В России государство оказывает огромный комплекс услуг своим гражданам, в том числе и медицинские. Медицинские услуги оказываются в каждом регионе, везде, где люди в них нуждаются. Каждый регион должен обеспечивать цифровые возможности в оказании таких услуг. В отличие от многих других, медицинские услуги влияют на здоровье и жизни граждан. Возникает вопрос в создании цифрового контура и агрегировании данных пациентов безопасным образом, не влияя на непрерывность таких услуг, ведь это может сказаться на здоровье и жизни людей.

В возникшей ситуации была создана региональная система, включающая в себя карты всех пациентов региона. Данная система позволяет врачам оценивать историю болезни каждого пациента от начала и до конца, в независимости от того, является ли этот пациент прикрепленным к данной больнице или приехал за медицинской помощью из другого района. Пациент в свою очередь, не волнуется на счет сохранности своей медицинской карты или забыть очередную выписку от другого специалиста. Чтобы каждый врач каждой больницы региона мог получить данные о пациенте другой больницы, требуется наличие централизованного сервера базы данных, включающего карточки всех пациентов. В этом заключается главная проблема системы с точки зрения информационной безопасности. Каждый пациент — это обладатель персональных данных, которые необходимо обрабатывать. Как обеспечить целостность, конфиденциальность и доступность передаваемых персональных данных пациентов от больницы до сервера и обратно?

Технически, решение данной задачи не кажется сложным. Напрашивается внедрение шифрования передаваемых данных, но как это обеспечить? Согласно приказу ФСТЭК от 21 декабря 2017 г. №235 «Об утверждении требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры российской федерации и обеспечению их функционирования», для обеспечения безопасности значимых объектов критической информационной инфраструктуры должны применяться сертифицированные на соответствие требованиям по безопасности средства защиты информации или средства, прошедшие оценку соответствия в форме испытаний или приемки в соответствии с Федеральным законом от 27 декабря 2002 г. N 184-ФЗ "О техническом регулировании", а всем привычный “https” использует зарубежный алгоритм шифрования данных. Для реализации подобной системы на рынке присутствуют программные и программно-аппаратные продукты.

Согласно приказу ФСТЭК от 25 декабря 2017 г. №239 «Об утверждении требований по обеспечению безопасности значимых объектов критической ин-

формационной инфраструктуры российской федерации», для обеспечения безопасности значимых объектов, являющихся информационными системами персональных данных, настоящие Требования применяются с учетом Требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» (Собрание законодательства Российской Федерации, 2012, № 45, ст. 6257). Для обеспечения безопасности значимых объектов, являющихся государственными информационными системами, настоящие Требования 3 применяются с учетом Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» (зарегистрирован Минюстом России 31 мая 2013 г., регистрационный № 28608) (с изменениями, внесенными приказом ФСТЭК России от 15 февраля 2017 г. № 27 «О внесении изменений в Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденные приказом ФСТЭК России от 11 февраля 2013 г. № 17»)

Архитектура системы состоит из центрального узла - серверной составляющей и удаленного узла, находящегося в МО. В каждом МО может использоваться от нескольких единиц, до несколько десятков, а то и сотен узлов, с которых необходим доступ в систему. Доступ в систему осуществляется через web-приложение. Для каждого пользователя необходима авторизация в системе на уровне приложения.

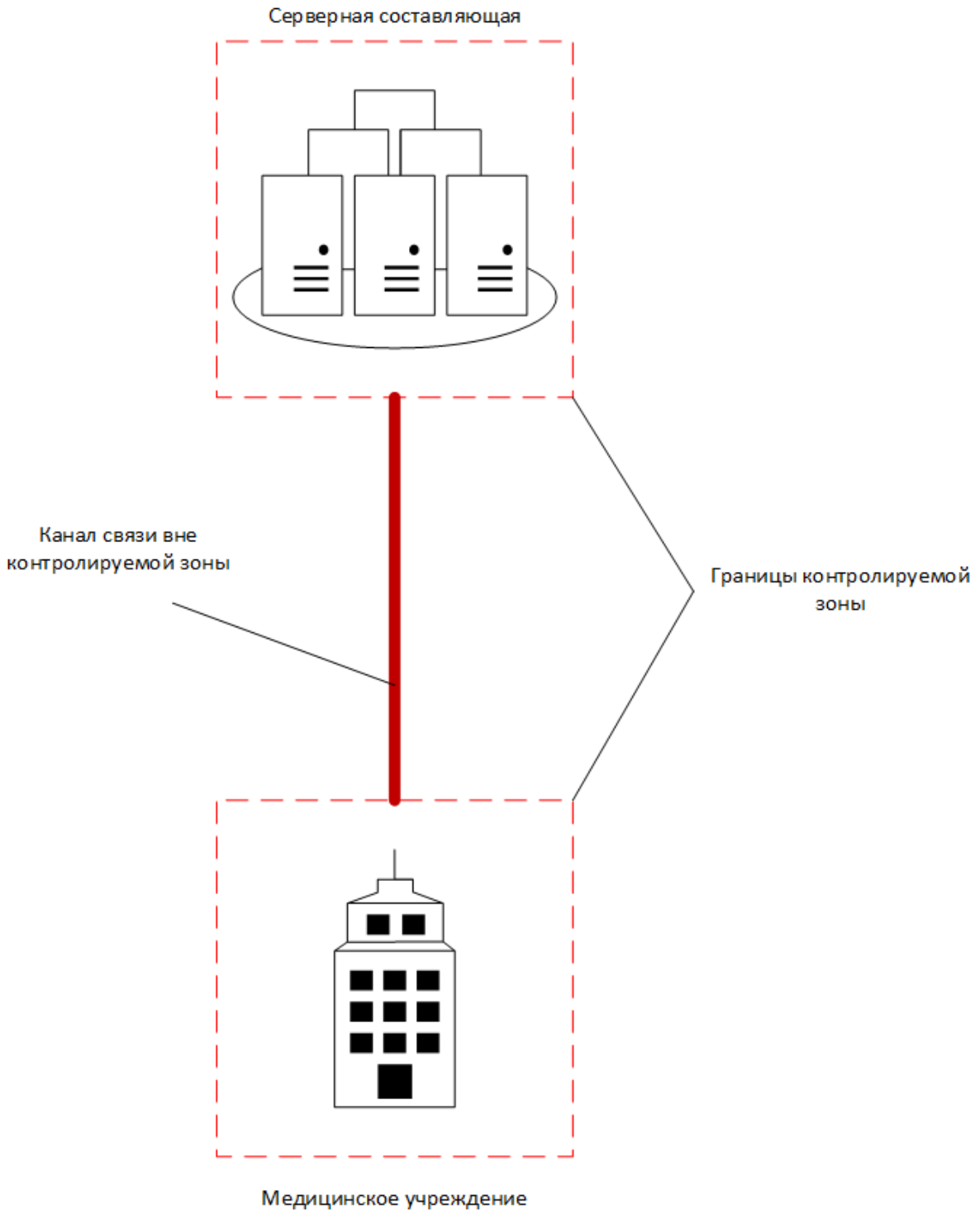


Рис. 1. Обобщенная архитектура распределенной системы

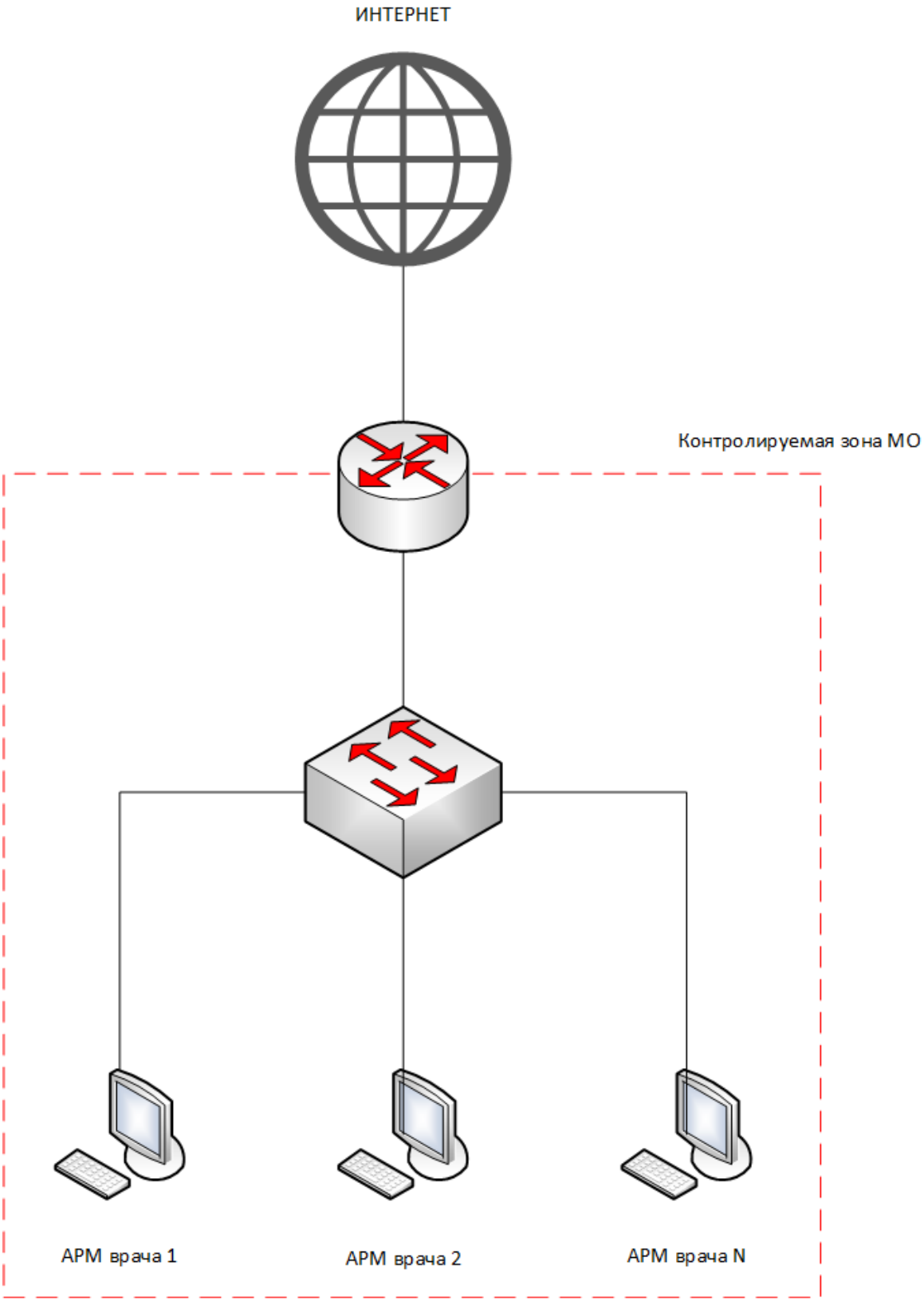


Рис. 2. Обобщенная схема медицинской организации (МО)

Исходя из законодательств, обеспечение безопасности для значимого объекта соответствующей категории значимости, касательно передачи

персональных данных в неконтролируемой зоне, необходимо обеспечить следующие меры:

– Приказ ФСТЭК от 25 декабря 2017 г. №239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»

– ИАФ.7 Защита аутентификационной информации при передаче,

– УПД.13 Реализация защищенного удаленного доступа,

– УПД.14 Контроль доступа из внешних информационных, (автоматизированных) систем,

– ЗИС.19 Защита информации при ее передаче по каналам связи,

– ЗИС.20 Обеспечение доверенных канала, маршрута,

– ЗИС.26 Подтверждение происхождения источника информации,

– ЗИС.27 Обеспечение подлинности сетевых соединений,

– ЗИС.33 Исключение доступа через общие ресурсы,

– ЗИС.38 Защита информации при использовании мобильных устройств,

– Приказ ФСТЭК от 11 февраля 2013 г. №17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»

– УПД.3 Управление (фильтрация, маршрутизация, контроль соединений однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами,

– УПД.13 Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети,

– ЗИС.3 Обеспечение защиты информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи,

– ЗИС.4 Обеспечение доверенных канала, маршрута между администратором, пользователем и средствами защиты информации (функциями безопасности средств защиты информации),

– ЗИС.10 Подтверждение происхождения источника информации, получаемой в процессе определения сетевых адресов по сетевым именам или определения сетевых имен по сетевым адресам,

– ЗИС.11 Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов,

– Приказ ФСТЭК от 18 февраля 2013 г. №21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»

– УПД.3 Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами,

– УПД.13 Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети,

– ЗИС.3 Обеспечение защиты персональных данных от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи,

– ЗИС.11 Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов.

Угрозы, возникающие при использовании незащищенного соединения согласно БДУ ФСТЭК [1]:

– Угроза «кражи» учетной записи доступа сетевым сервисам

– Угроза неправомерных действий в каналах связи

– Угроза определения типов объектов защиты

– Угроза «кражи» учетной записи доступа к сетевым сервисам

– Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети

– Угроза обнаружения открытых портов и идентификации привязанных к ним сетевых служб

– Угроза определения топологии вычислительной сети

– Угроза передачи данных по скрытым каналам

– Угроза получения предварительной информации об объекте защиты

– Угроза перехвата одноразовых паролей в режиме реального времени

Перечень основных тактик и соответствующих им типовых техник приведено в приложение 11 Модели угроз [2], описание сценариев их реализации представлено в таблице 1

Таблица 1

Описание сценариев реализации угроз

Идентификатор УБИ	Наименование УБИ	Описание	Сценарий реализации угрозы	Актуальность
168	Угроза «кражи» учетной записи доступа сетевым сервисам	Угроза заключается в возможности неправомерного ознакомления нарушителем с защищаемой информацией пользователя путем получения информации идентификации/аутентификации, соответствующей учетной записи доступа пользователя к сетевым сервисам, с которой связан неактивный/несуществующий адрес электронной почты.	T1.12-> T2.11-> T4.1 T1.11-> T10.1	Актуальная

Продолжение табл. 1

28	Угроза использования альтернативных путей доступа к ресурсам	Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к защищаемой информации в обход штатных механизмов с помощью нестандартных интерфейсов (в том числе доступа через командную строку в обход графического интерфейса).	T6.4-> T3.3 T2.3-> T3.1	Актуальная
69	Угроза неправомерных действий в каналах связи	Угроза заключается в возможности внесения нарушителем изменений в работу сетевых протоколов путем добавления или удаления данных из информационного потока с целью оказания влияния на работу дискредитируемой системы или получения доступа к конфиденциальной информации, передаваемой по каналу связи.	T8.5-> T7.21-> T10.1 T8.5-> T7.21-> T10.10	Актуальная
103	Угроза определения типов объектов защиты	Угроза заключается в возможности проведения нарушителем анализа выходных данных дискредитируемой системы с помощью метода, позволяющего определить точные значения параметров и свойств, однозначно присущих дискредитируемой системе. Использование данного метода не наносит прямого вреда дискредитируемой системе. Однако сведения, собранные таким образом, позволяют нарушителю выявить слабые места дискредитируемой системы, которые могут быть использованы в дальнейшем при реализации других угроз.	T8.8-> T9.10-> T10.10	Актуальная

Продолжение табл. 1

116	Угроза перехвата данных, передаваемых по вычислительной сети	Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к сетевому трафику дискредитируемой вычислительной сети в пассивном или активном режиме для сбора и анализа сведений, которые могут быть использованы в дальнейшем для реализации других угроз, оставаясь при реализации данной угрозы невидимым получателем перехватываемых данных.	T1.4-> T2.13-> T10.1	Актуальная
168	Угроза «кражи» учетной записи доступа к сетевым сервисам	Угроза заключается в возможности неправомерного ознакомления нарушителем с защищаемой информацией пользователя путем получения информации идентификации/аутентификации, соответствующей учетной записи доступа пользователя к сетевым сервисам (социальной сети, облачным сервисам и др.), с которой связан неактивный/несуществующий адрес электронной почты.	T1.12-> T2.11-> T4.1 T1.11-> T10.1	Актуальная
73	Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети	Угроза заключается в возможности изменения вредоносными программами алгоритма работы программного обеспечения сетевого оборудования и (или) параметров его настройки путем эксплуатации уязвимостей программного и (или) микропрограммного обеспечения указанного оборудования.	T1.9-> T2.10-> T4.1-> T9.1 T6.1-> T4.1-> T9.1	Актуальная

Продолжение табл. 1

98	Угроза обнаружения открытых портов и идентификации привязанных к ним сетевых служб	Угроза заключается в возможности определения нарушителем состояния сетевых портов дискредитируемой системы для получения сведений о возможности установления соединения с дискредитируемой системой по данным портам, конфигурации самой системы и установленных средств защиты информации, а также других сведений, позволяющих нарушителю определить по каким портам деструктивные программные воздействия могут быть осуществлены напрямую, а по каким – только с использованием специальных техник обхода межсетевых экранов.	T4.3-> T10.7 T4.3-> T10.2	Актуальная
104	Угроза определения топологии вычислительной сети	Угроза заключается в возможности определения нарушителем состояния сетевых узлов дискредитируемой системы для получения сведений о топологии дискредитируемой вычислительной сети, которые могут быть использованы в дальнейшем при попытках реализации других угроз.	T1.2	Актуальная
111	Угроза передачи данных по скрытым каналам	Угроза заключается в возможности осуществления нарушителем неправомерного вывода защищаемой информации из системы, а также передаче управляющих команд путем ее нестандартного размещения в легитимно передаваемых по сети открытых данных путем ее маскирования под служебные протоколы, сокрытия в потоке других данных, использования скрытых пикселей и т.п.	T6.1-> T10.1-> T9.7	Актуальная

Окончание табл. 1

181	Угроза перехвата одноразовых паролей в режиме реального времени	Угроза заключается в возможности получения нарушителем управления критическими операциями пользователя путем перехвата одноразовых паролей, высылаемых системой автоматически, и использования их для осуществления неправомерных действий до того, как истечет их срок действия.	Т10.11	Актуальная

Как правило, в процессе эксплуатации могут возникать те или иные трудности и непреодолимые обстоятельства, которые могут помешать использовать отечественный стандарт шифрования в канале связи от МО до сервера.

Вывод: В современном мире, в эпоху развития цифровизации, обмен и передача персональных данных стали неотъемлемой частью повседневной жизни. В связи с этим, государство озаботилось их защитой и издало ряд законов и назначало исполнительные органы для контроля и реализации защиты персональных данных. В данной статье были проанализированы требования исполнительного органа государственной власти, а также угрозы и риски при передаче данных за пределами контролируемой зоны.

СПИСОК ЛИТЕРАТУРЫ

1. Банк данных угроз безопасности информации ФСТЭК https://bdu.fstec.ru/threat [электронный ресурс]
2. Методический документ. Утвержден ФСТЭК России 5 февраля 2021 г. «Методика оценки угроз безопасности информации»
3. Приказ ФСТЭК от 21 декабря 2017 г. №235 «Об утверждении требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры российской федерации и обеспечению их функционирования»
4. Приказ ФСТЭК от 25 декабря 2017 г. №239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры российской федерации»
5. Постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»

6. Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» (зарегистрирован Минюстом России 31 мая 2013 г., регистрационный № 28608) (с изменениями, внесенными приказом ФСТЭК России от 15 февраля 2017 г. № 27 «О внесении изменений в Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденные приказом ФСТЭК России от 11 февраля 2013 г. № 17»
7. Приказ ФСТЭК от 18 февраля 2013 г. №21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»

УДК 004.056.5

А. Э. ГАБИТОВ
askargabitov@yandex.ru
Науч. руководв. – канд. техн. наук, доц. А. Ю.СЕНЦОВА

Уфимский государственный авиационный технический университет

СРАВНИТЕЛЬНЫЙ АНАЛИЗ СЕТЕВЫХ СКАНЕРОВ БЕЗОПАСНОСТИ

Аннотация. В данной статье проводится сравнительный анализ сетевых сканеров безопасности с точки зрения их использования в настоящее время. В ходе работы был произведен анализ понятия сканер безопасности, а также произведен сравнительный анализ сканеров безопасности по параметрам: количество найденных уязвимостей и качество поиска уязвимостей, удобство использования ПО и пользовательский интерфейс.
***Ключевые слова*:** сканер безопасности; уязвимость.

Для полноценного изучения изнутри, выявления потенциальных уязвимых областей решено использовать специальные системы. При этом стоит понимать, что аналитическая работа всегда подразумевает большую вероятность выявления человеческой ошибки. То есть, даже самые автоматизированные программы не будут давать стопроцентный результат, так как всегда необходимо учитывать вероятность ошибки. Для безопасного, в минимальной вероятностью ошибки осуществления контроля за аудитом безопасности рекомендовано использовать процедуру сканера безопасности. Сканер безопасности – сложное программное обеспечение, которое выполняет функции контроллера получения диагностической работы сетевых компьютеров, изучение данной работы всех подключенных к локальной сети машин, а также служат для проведения сканирования всего ПО, приложений, сетей на выявление потенциально опасных файлов, угроз и прочих компонентов, создающие уязвимости или усложнения в работах системы. В статье проводится изучение, анализ и оценивание эффективности нескольких сетевых сканеров безопасности.

Естественно, что для объективной оценки решено использовать несколько ключевых критериев. Первый компонент, позволяющих осуществить оценочную работу – это эффективность работы программы, количество найденных уязвимых элементов, опасных файлов, а также выявление угроз, которые могут

серьезно повлиять на работоспособность системы в целом. Второй компонент, интерфейс, удобство использования, интуитивность и скорость проведения операций. Для сравнения были выбраны пять различных сетевых сканеров безопасности: XSpider 7.7 Demo (XS), LanSpy 2.0 (LS), Shadow Security Scanner 7.303 Trial (SSS), GFI LANguard Network Security Scanner 9.5 Trial (GL), Nessus Security Scanner 4.2.2 (NSS). Чтобы получить максимальный результат, который будет понятным для большинства людей, решено использовать операционную систему Windows XP, как одну из самых распространенных и известных продуктов на рынке программного обеспечения от корпорации Microsoft. Перед началом нашего практического эксперимента все используемые сканеры безопасности были перестроены на максимальную производительность, соответственно все настройки были переведены на максимум.

Для получения первичных результатов решено использовать «голую» операционную систему. Это максимально упрощенное ПО без дополнений, обновлений или заранее установленных вспомогательных программы корпорации Microsoft. Чтобы получить результат, отражающий реальную эффективность каждого рассматриваемого сканера безопасности, решено использовать программы с заранее установленными последними доступными на тот момент обновлениями, соответственно после этого осуществляется повторное сканирование системы на обнаружение ошибок и уязвимостей.

После проведения первого этапа работы, проводится систематический анализ результатов, группирование данных, а также создание таблицы, в которой будут присутствовать объективные данные об эффективности сканеров безопасности. Более подробно изучить результаты можно в Таблице 1.

Таблица 1

№ п/п	Описание (Баллы)	NSS	LS	SSS	GL	XS
1	Найденные порты	48	11	10	13	48
2	Уязвимости	9	12	14	12	9
	Итого:	57	23	24	25	57

Для грамотного осмысления полученных результатов решено ввести систему оценочных баллов. Оценивались следующие проверки: – идентификация

TCP- и UDP-портов; – дополнительно найденная информация об операционной системе (версия, сетевой адрес, пользователи, ресурсы и т.д.); – обнаружение и качество уязвимостей. Идентификация TCP- и UDP-портов оценивалась следующим образом: за каждый найденный открытый порт начислялось по одному баллу. Каждый процесс работы сканеров получал собственное количество баллов, естественно, что при некорректной работе баллы отнимались. Оценки выставлялись по следующим правилам: за каждую найденную уязвимость добавлялось определенное количество баллов в зависимости от степени опасности данной уязвимости. За серьезную (критическую) уязвимость начисляется 3 балла, за среднюю уязвимость – 2 балла, за слабую – 1 балл.

В итоге можно заметить, что наиболее удобен в использовании сетевой сканер безопасности от отечественного производителя XSpider. Он полностью русифицирован, имеется возможность редактировать профили, создавать свои, сохранять и загружать настройки, генерировать отчеты. При этом в программе хороший, удобный интерфейс, расположение всех управляющих элементов. В общем, по удобству и возможностям данный сканер занимает достойное первое место. По проведенным сканированиям и проведенному исследованию можно подвести итог. Наилучший результат показал сетевой сканер безопасности от компании Tenable – Nessus Security Scanner. Он заработал самый большой балл в итоге сравнения на обоих этапах, обнаружив самое большое количество уязвимостей. В рамках проделанной работы не проводилась проверка на правильность определенных уязвимостей, поэтому данный критерий не учитывался при сравнении. Одним из больших плюсов этого приложения является то, что он распространяется бесплатно, имеет достаточно большую базу уязвимостей, определяет их критичность и имеет достаточно высокую скорость сканирования. Конечно, такое качество как скорость работы для сканеров безопасности является одним из последних критериев, которые следует учитывать. Достаточно хорошие результаты также показал отечественный продукт от компании Positive Technologies XSpider. К сожалению, исследовалась только Demo-версия данного продукта, скачанного с официального сайта разработчика. Поэтому неизвестно как давно обновлялись базы данной версии программы. Тем не менее,

на обоих этапах анализа данный сканер показал достойный результат, обнаружив открытые порты и определив наличие уязвимостей системы. Одним из больших плюсов данного сканера является то, что даже в неполной версии имеется возможность определения уязвимостей и степени их критичности. Также в полной версии имеется возможность генерации отчетов и дополнительные функции, не реализованные в Demo-версии.

Что же касается остальных участников, то их можно использовать только в качестве сканеров портов, да программ для сбора открытой информации удаленного узла. Тем не менее, они показали неплохие результаты. Так, например, LanSpy практически во всех случаях предоставляла наибольшую информацию об операционной системе, хотя и не имеет возможности определять уязвимости. Плюс к этому имеет достаточно высокую скорость работы. Shadow Security Scanner также не остается без внимания. На первом этапе это единственный сканер, который смог определить все открытые порты. Собрал дополнительную информацию, но, к сожалению, не указал уязвимости системы, а соответственно и степень их критичности, так как разработчики убрали эту возможность с Trial-версии данного приложения, что очень разочаровало. И, кончено же, данный продукт не проявил себя в полной красе. Хотя стоит заметить, что даже урезанная версия программы работала уж очень долго (практически 12 часов). Подобные замечания о недостаточной информативности предоставляемых данных можно высказать и в отношении сетевого сканера безопасности GFI LANguard Network Security Scanner, так как на анализ была взята так же Trial-версия продукта. Но в отличие от Shadow Security Scanner работает намного быстрее.

СПИСОК ЛИТЕРАТУРЫ

1. ЗАЩИТА ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СЕТЯХ: учебное пособие / Н. И. Синадский, Д. А. Хорьков. — Екатеринбург : УрГУ, 2008. 225 с.
2. Бегаев А.Н., Бегаев С.Н., Федотов В.А. Тестирование на проникновение. – СПб: Университет ИТМО, 2018. – 45 с
3. Бегаев А.Н., Кашин С.В., Маркевич Н.А., Марченко А.А., Выявление уязвимостей и недекларированных возможностей в программном обеспечении – СПб: Университет ИТМО, 2020. – 38 с.

УДК 004.056.52

А. Х. ГАЛЛЯМОВ
Науч. руководв. – канд. техн. наук Т. А. ИВАНОВА

Уфимский государственный авиационный технический университет

ИНТЕРНЕТ ВЕЩЕЙ. КАК ЭТО РАБОТАЕТ НА ТРАСПОРТЕ. ЗАЩИТА ПРОТОКОЛА

Аннотация. Анализ стандарта IEEE 1609.02, которая описывает защиту информации в транспортных сетях, работающих по технологии Wi-Fi. Обзор арифметики криптографии на эллиптических кривых и алгоритм ECDSA, используемый для создания электронной подписи в стандарте IEEE 1609.2. В конце была проверена корректность алгоритма ECDSA.
Ключевые слова: информационная безопасность; беспроводные технологии; криптография.

Интеллектуальные транспортные системы (англ.: Intelligent Transport Systems, ITS) активно развиваются. Их функционирование невозможно без создания телекоммуникационных систем, позволяющих транспортным средствам обмениваться информацией со внешними устройствами (англ. Vehicle-to-Everything, V2X). Транспортные средства накапливают информацию посредством различных сенсоров, радаров, лидаров и камер. Для обеспечения автономного вождения и передвижения машин в плотном строю (так называемый platooning) необходимо обеспечивать обмен этой информацией между различными транспортными средствами. Обмен информацией может также осуществляться с элементами дорожной инфраструктуры, что позволяет обеспечивать большую безопасность движения посредством передачи объектами инфраструктуры предупреждающих сообщений. Кроме того, существует большое число других приложений, которые обеспечивают удобство вождения и безопасность, а также уменьшают число пробок и предоставляют различные развлекательные сервисы. Разнообразные приложения порождают различные требования на задержки, надежность и скорость беспроводной передачи данных. Однако кроме требований на производительность сети во многих случаях важно, чтобы передаваемые данные были защищены. В данной статье я хотел бы представить краткий обзор основных механизмов стандарта IEEE 1609.2, в ко-

тором описаны методы защиты информации в транспортных сетях, построенных с использованием технологии Wi-Fi.

DSRC телекоммуникации

На данный момент одним из самых распространенных способов коммуникации в V2X является выделенная связь на короткие расстояния (DSRC), для обеспечения которой используется набор стандартов беспроводной связи в транспортной среде: стандарты IEEE 1609 и IEEE 802.11p. Комитетом IEEE был выпущен специальный гайд, в котором они детально описаны. Заинтересовавшиеся могут найти его по ссылке https://ieeexplore.ieee.org/document/8686445

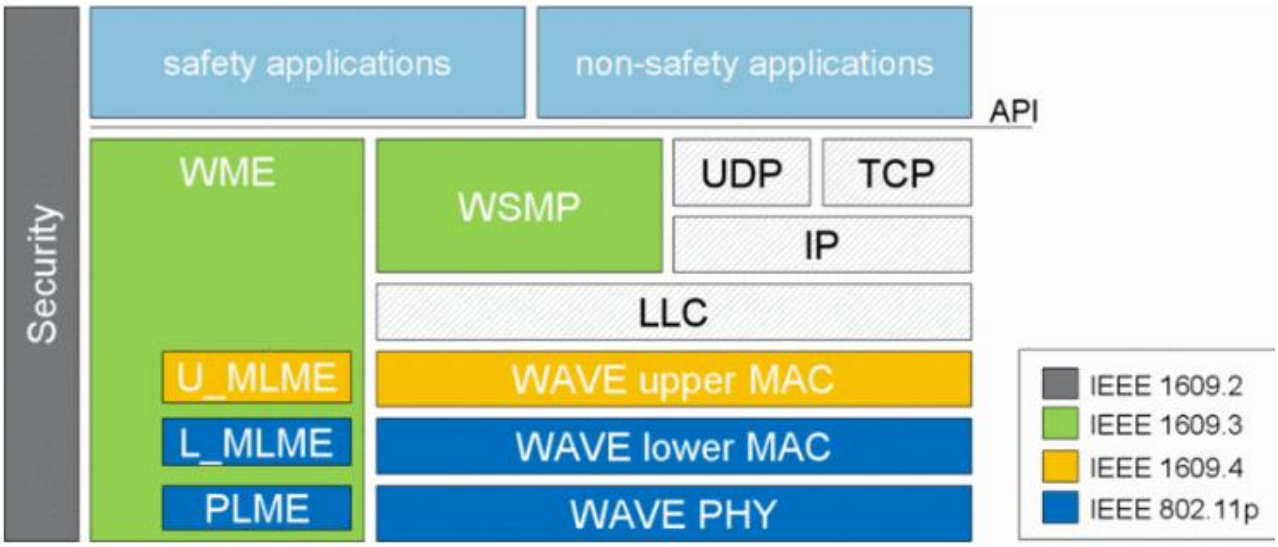


Рис. 1. Набор стандартов для DSRC

Стандарт IEEE 802.11p описывает работу физического и основной части MAC уровня модели OSI в диапазоне частот 5,9 ГГц (и 60 ГГц опционально). Как видно, этот диапазон частот отличается от частот, на которых работает "классический Wi-Fi": 2,4 ГГц и 5 ГГц. "Классические" частоты являются нелицензируемыми, и это приводит к их зашумленности передачами устройств, работающих по другим стандартам, что крайне нежелательно для транспортных сетей, которые сделаны в частности для поддержки приложений, обеспечивающих безопасность дорожного движения. В свою очередь, диапазон частот в 5,9 ГГц является бесплатным и лицензированным в том плане, что в этом диапазоне могут работать только устройства, использующие определенный набор

стандартов. Стандарт IEEE 1609.4 описывает многоканальные методы доступа к среде, которые позволяют поочередно передавать сразу в двух каналах, например, канале для передачи данных и канале для контрольных сообщений. IEEE 1609.3 описывает WSMP (Wave Short Message Protocol), который является альтернативой протоколам TCP/UDP и IP на транспортном и сетевом уровне соответственно. Также стандарт IEEE 1609.3 выполняет некоторые другие функции, например, выбор канала для передачи данных. Стандарт IEEE 1609.2 описывает методы обеспечения безопасной передачи данных и именно ему я хотел бы уделить внимание в данной статье.

Основные положения IEEE 1609.2

Стандарт IEEE 1609.2 основывается на асимметричной криптографии и в частности описывает методы шифрования сообщений и методы создания цифровой подписи. Единицей данных для этого стандарта является так называемый SPDU (Secured Protocol Data Unit), который состоит из защищаемых данных и специальных полей для обеспечения защиты информации. IEEE 1609.2 защищает только данные, являющиеся полезной нагрузкой для протокола транспортного уровня. То есть заголовки транспортного, сетевого, LLC, MAC, а тем более физического уровней стандарт IEEE 1609.2 не защищает. Пример пакета, который иллюстрирует местоположение защищаемых данных, представлен на рисунке ниже. Базовая структура SPDU стандарта IEEE 1609.2 представлена здесь под буквой D:

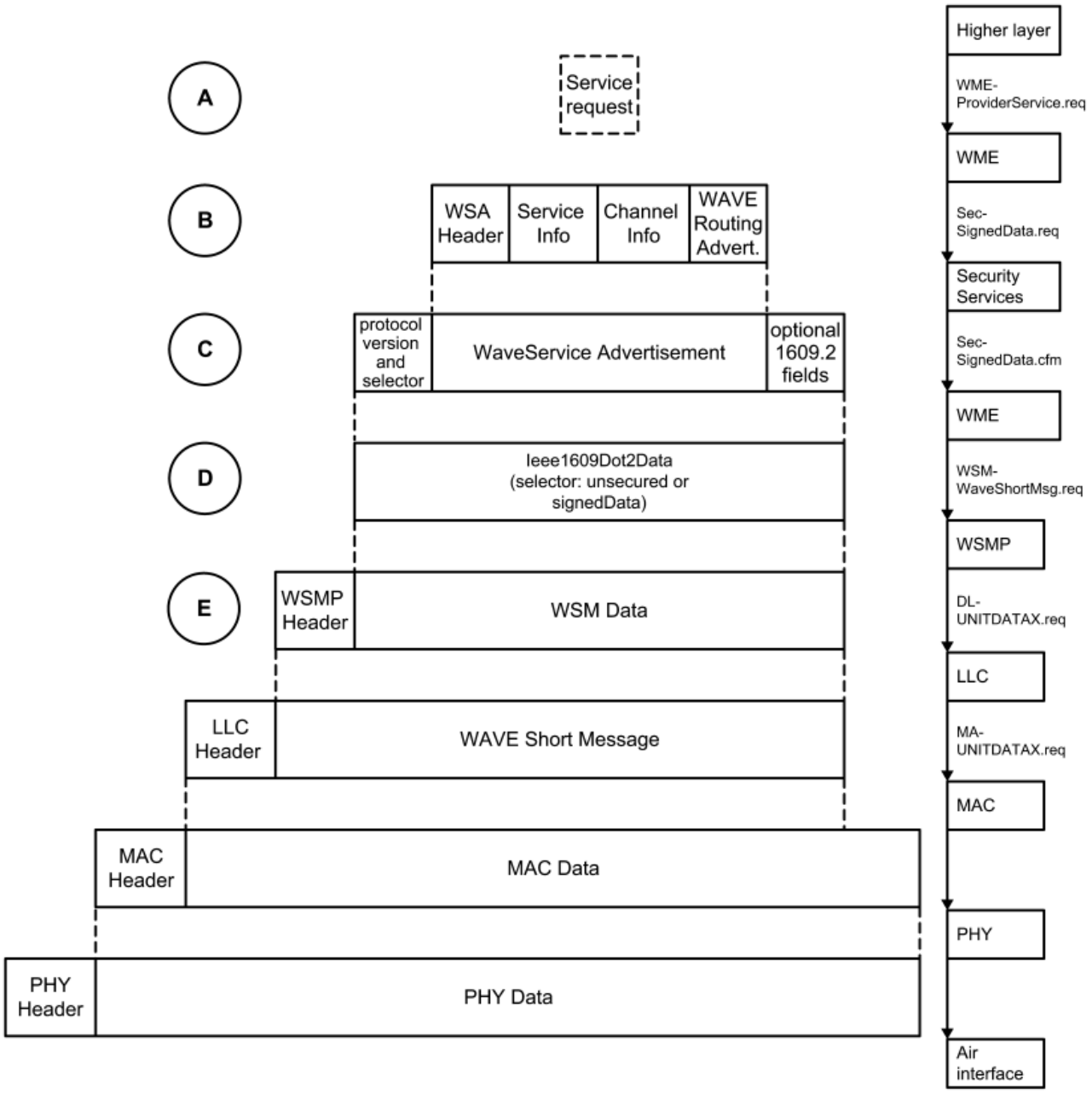


Рис. 2. Местоположение данных, защищаемых стандартом IEEE 1609.2

Так как трафик в транспортных сетях по большей части является широковещательным, описывать методы шифрования я не буду, так как при шифровании у принимающего устройства есть секретный ключ, известный только ему, а у передающих открытый - расшифровать сообщений может только принимающее устройство, то есть передача должна быть не широковещательной, а по конкретному адресу. Поэтому я сосредоточусь на описании инфраструктуры для криптографии с открытым ключом (англ.: PKI, Public Key Infrastructure) применительно к транспортным сетям и на алгоритме создания и проверки

цифровой подписи. Цифровая подпись используется для проверки того, что отправитель сообщения действительно является тем устройством, за которое себя выдает, и для проверки того, что данные не были изменены сторонним устройством. Для создания цифровой подписи устройство использует свой секретный ключ и добавляет значение цифровой подписи в специальные поля SPDU. Проверить сообщение на подлинность может любое устройство, которое знает открытый ключ, соответствующий секретному ключу передающего устройства. Так как для проверки цифровой подписи необходимо знать только открытый ключ, то добавлять цифровую подпись можно даже к широковещательным сообщениям, например, к базовым сообщениям приложений безопасности (англ.: Basic Safety Messages, BSM) и к beacon-ам (специальные кадры технологии Wi-Fi, применяемые для обмена служебной информацией). О том, как устройства узнают открытый ключ, соответствующий секретному ключу, я расскажу в следующей главе.

Инфраструктура открытых ключей в сетях V2X

Сразу оговорюсь, что далее я буду говорить только о транспортных средствах, поддерживающих процедуру создания и проверки электронной подписи по стандарту IEEE 1609.2, так как на данный момент этот стандарт поддерживают не все транспортные средства. Сперва я хотел бы отметить, что у каждого транспортного средства имеется 2 типа секретных ключей: долгосрочный и краткосрочный. При этом краткосрочных ключей может быть несколько. Долгосрочный секретный ключ выдается при производстве транспортного средства по договоренности производителя и властей того региона, где ключ выдавался. Выдается он вместе с соответствующим открытым ключом, некоторой технической и идентификационной информацией о транспортном средстве и сертификатом открытого ключа (сертификат содержит открытый ключ и некоторую информацию о владельце соответствующего секретного ключа). Долгосрочный секретный ключ известен только устройству, которому он выдан, и хранится в так называемом аппаратном защитном модуле транспортного средства, из ко-

торого секретный ключ не так-то просто достать. Открытый ключ, его сертификат и некоторая идентификационная информация устройства хранятся в сертификационном центре (англ.: Certification Authority, CA), из которого другие устройства могут получить информацию о сертификате и открытом ключе зарегистрированного устройства. Стоит отметить, что во время производства нового транспортного средства оно получает также 2 открытых ключа сертификационного центра: один для проверки электронной подписи сообщений, переданных от CA, а второй на случай, если злоумышленнику удастся узнать первый секретный ключ CA. Если злоумышленнику удастся узнать этот ключ, то CA сможет сменить секретный и открытый ключ, разослав новый открытый ключ всем устройствам и подписав сообщение вторым секретным ключом. Стоит отметить, что время жизни долгосрочного секретного ключа должно быть равно времени жизни транспортного средства или по крайней мере составлять большую часть его жизни.

Теперь я хотел бы пояснить, зачем нужны краткосрочные закрытые ключи. Как я уже говорил, долгосрочный ключ рассчитан на длительное использование, поэтому хотелось бы использовать его нечасто, чтобы у злоумышленника было меньше шансов взломать этот ключ. Для этого используются секретные краткосрочные ключи. Транспортное средство генерирует несколько пар краткосрочных секретных и открытых ключей и отправляет CA сообщение с сертификатами открытых ключей. Сообщение подписывается долгосрочным закрытым ключом. После того как CA получил сертификаты краткосрочных открытых ключей от транспортного средства, он сохраняет их у себя в памяти, и далее эти сертификаты могут получить другие устройства. После отправки сертификатов краткосрочных открытых ключей CA наше устройство начинает подписывать сообщения краткосрочными секретными ключами. Периодически оно меняет свои секретные и соответствующие им открытые ключи. При этом уже использованные закрытые и соответствующие им открытые ключи стираются из памяти и больше не используются. Поэтому устройству периодически

нужно генерировать новые пары открытых и закрытых ключей и рассылать соответствующие сертификаты открытых ключей на CA.

Я довольно много говорил об обмене информацией между CA и нашим устройством, но не сказал, как он осуществляется. Для пояснения я приведу следующую картинку:

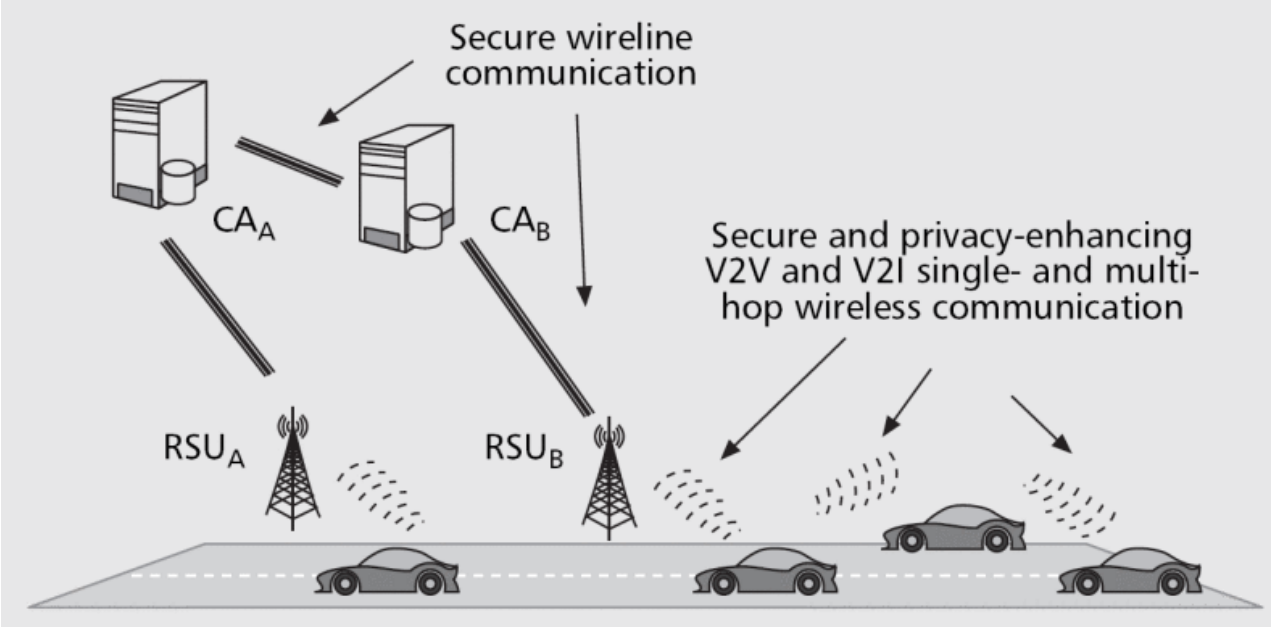


Рис. 3. Обмен информацией между сертификационным центром и транспортным средством

Транспортные средства обмениваются информацией с CA посредством придорожной инфраструктуры (англ.: Road-Side Unit, RSU). Ранее я писал, что стандарт IEEE 1609.2 защищает только полезную нагрузку транспортного уровня, но не заголовки транспортного уровня и нижележащих уровней модели OSI, что позволяет RSU и другим устройствам, выполняющим роль маршрутизатора, передавать сообщения от транспортного средства к CA и обратно, даже не имея возможности узнать содержимое сообщения (если оно зашифровано, например). То есть обмен информацией между автомобилями и CA осуществляется через RSU.

Теперь я хотел бы описать обмен информацией между транспортными средствами. При отправке радиомодулем автомобиля широковещательного сообщения сущность, отвечающая за безопасность передачи данных, должна

прицепить к сообщению электронную подпись и сертификат открытого ключа для проверки этой электронной подписи. При приеме сообщения другое транспортное средство должно сперва проверить, что полученный сертификат зарегистрирован и отмечен как действительный в CA, а затем использовать открытый ключ из сертификата для проверки электронной подписи. Для проверки действительности сертификата при первом его получении нужно направлять запрос в CA. Дальнейшая проверка действительности сертификата может осуществляться посредством его временного сохранения в буфере транспортного средства (то есть устройство на время запоминает, что сертификат действительный).

Стоит отдельно отметить, что CA может не только регистрировать сертификаты, но и отзывать их по истечении срока жизни или по каким-то иным причинам. Так что если злоумышленник захочет сбить систему дорожной безопасности транспортного средства с толку, но сертификат открытого ключа злоумышленника не будет зарегистрирован в CA, то у него ничего не выйдет. Больше информации об инфраструктуре открытых ключей в транспортных сетях можно узнать, например, из статьи №1 или статьи №2, на которых основывается мой рассказ про инфраструктуру открытых ключей в V2X.

Параметры алгоритма создания электронной подписи и операции на эллиптических кривых

Для создания и проверки электронной подписи в стандарте IEEE 1609.2 используется алгоритм цифровой подписи на основе эллиптических кривых (англ.: Elliptic Curve Digital Signature Algorithm, ECDSA). Алгоритм ECDSA позволяет создать электронную подпись сообщения с помощью закрытого ключа, а затем проверить ее с помощью открытого. То есть отправитель должен знать секретный ключ, а все принимающие устройства должны знать открытый ключ. Однако кроме знания одного из двух ключей устройства также должны знать параметры алгоритма. Первыми двумя параметрами алгоритма являются коэффициенты используемой эллиптической кривой. В алгоритме ECDSA ис-

пользуются эллиптические кривые форме Вейерштрасса, под которыми в криптографии подразумевается множество точек (x, y) следующего вида (далее под эллиптической кривой буду подразумевать именно это множество точек):

$$\{(x,y) \in \mathbb{F}_p^2 |\ y^2 = x^3 + ax + b\ (mod\ p),\ 4a^3 + 27b^2 \neq 0\} \cup \{"0"\}$$

$$\text{где}\ \ \mathbb{F}_p^2 = \{(x,y) \in \mathbb{R}^2 |\ x \in \mathbb{F}_p, y \in \mathbb{F}_p\}$$

Здесь Fp - это поле Галуа, состоящее из целых чисел от 0 до p - 1, где p - простое число, либо степень простого числа. В криптографии p выбирают либо простым числом, либо степенью двойки. Числа a и b, являющиеся параметрами эллиптической кривой, также принадлежат F_p. Дополнительное условие на эти коэффициенты делает эллиптическую кривую применимой в криптографии. Под "0" подразумевается нулевой элемент эллиптической кривой, при прибавлении которого к любому элементу получится тот же самый элемент. Геометрически нулевой элемент - это бесконечно удаленная точка расширенной действительной плоскости. Стоит отметить, что эллиптическая кривая имеет конечное число элементов и при правильном введении операции сложения и взятия обратного элемента становится абелевой группой относительно этой операции сложения. Чтобы геометрически пояснить операцию сложения и взятия обратного элемента, я вставлю сюда картинку, которая иллюстрирует вид эллиптической кривой в R^2, то есть кривой вида:

$$\{(x,y) \in \mathbb{R}^2 |\ y^2 = x^3 + ax + b\ (mod\ p),\ 4a^3 + 27b^2 > 0\}$$

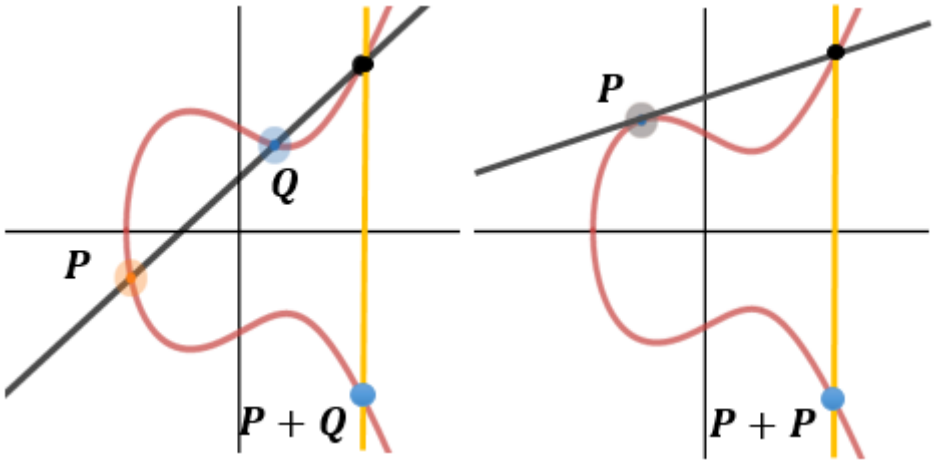


Рис. 4. Сложения на эллиптической кривой в форме Вейерштрасса

Красная кривая - это качественный вид эллиптической кривой, задаваемой уравнением выше. У такой кривой есть ось симметрии, которая в данном случае проходит через ось абсцисс. Ось симметрии позволяет ввести понятие обратного элемента: точка P эллиптической кривой называется обратной к точке M эллиптической кривой, если точка M симметрична точке P относительно оси симметрии нашей эллиптической кривой. Результат сложения симметричных точек M и P определяется следующим образом:

$$M + P = "0"$$

Стоит отметить, что на представленном выше рисунке изображена не только сама эллиптическая кривая, но и геометрический смысл операции сложения. Чтобы найти сумму двух разных точек эллиптической кривой, не симметричных относительно оси симметрии этой кривой (на рисунке точки P и Q), необходимо провести через них прямую и найти ее точку пересечения с кривой (точка пересечения существует в силу условий на параметры a и b). Тогда суммой точек эллиптической кривой называется точка, обратная к указанной выше точке пересечения. Для нахождения результата сложения некоторой точки эллиптической кривой с самой собой (на рисунке P + P) необходимо провести касательную к этой точке, найти пересечение касательной с эллиптической кривой (пересечения опять-таки существует в силу условий на a и b) и взять точку, обратную к пересечению. Для реализации алгоритма ECDSA на компьютере указанные выше операции сложения необходимо записать в аналитическом виде. Это можно сделать, используя методы аналитической геометрии. Здесь я напишу лишь конечные формулы для сложения точек в полях Галуа. Под делением в полях Галуа я подразумеваю, взятие обратного элемента: элемент x поля Галуа называется обратным к элементу y поля Галуа если:

$$x \cdot y = 1 \; mod \; p$$

Для вычисления обратного элемента обычно используется расширенный алгоритм Евклида. С учетом замечания про взятие обратного элемента формула для сложения разных точек $M(x_1, y_1)$ и $\overline{Q(x_2, y_2)}$, не симметричных относитель-

но оси симметрии эллиптической кривой, имеет следующий вид (*все!!!* операции по модулю p):

$$R = (x_3, y_3) = P + Q$$
$$x_3 = \lambda^2 - x_1 - x_2 \; mod \; p$$
$$y_3 = -y_1 + \lambda(x_1 - x_3) \; mod \; p$$
$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \; mod \; p$$

В свою очередь, формула для сложения точки с самой собой имеет вид:

$$R = (x_3, y_3) = P + P$$
$$x_3 = \lambda^2 - 2x_1 \; mod \; p$$
$$y_3 = -y_1 + \lambda(x_1 - x_3) \; mod \; p$$
$$\lambda = \frac{3x_1^2 + a}{2y_1} \; mod \; p$$

Однако a, b и p - это не единственные параметры алгоритма ECDSA. Дело в том, что алгоритм ECDSA работает не на всей эллиптической кривой, а на ее циклической подгруппе, образуемой некоторой генерирующей точкой G эллиптической кривой. Все элементы этой подгруппы получаются путем сложения точки G с самой собой некоторое число раз. Порядок этой подгруппы (то есть число элементов в ней) является пятым параметром алгоритма ECDSA. По-другому порядок подгруппы можно определить как наименьшее положительное целое число n такое, что: nG = "0". Последним параметром является так называемый кофактор подгруппы. Он определяется следующим образом:

$$h = \frac{N}{n}$$

Здесь под N подразумевается порядок всей эллиптической кривой, то есть число элементов в ней. В силу так называемой теоремы Лагранжа, n всегда является делителем числа N, так что кофактор определен корректно.

В стандарте IEEE 1609.2 возможно использование лишь определенного набора параметров, для которых нет общеизвестных методов быстрого взлома алгоритма ECDSA (о том, как его можно взломать я расскажу чуть позже). Ис-

пользуемый набор параметров для передающего устройства можно получить вместе с его открытым ключом от CA.

Алгоритм ECDSA

Теперь перейду к описанию самого алгоритма ECDSA. Этот алгоритм работает не с самим передаваемым сообщением, а с его хэшем. Хэш-функция позволяет преобразовать сообщение произвольной длины в последовательность бит фиксированной длины. При этом данное преобразование выполняется таким образом, что восстановление всех возможных исходных значений сообщения по заданному значению хэша является вычислительно сложной задачей, тогда как вычисление самой хэш-функции можно произвести быстро. Полученную после действия хэш-функции последовательность бит можно интерпретировать как десятичное число в двоичной форме записи. Именно это число используется алгоритмом ECDSA. Если это число получается большим, чем n, то хэш сообщения необходимо урезать. Стандарт IEEE 1609.2 определяет всего 2 допустимые хэш-функции: SHA-256 и SHA-384.

Описание процедуры генерации открытого и закрытого ключей. Закрытый ключ d является случайно выбранным элементом поля Галуа, лежащим в интервале [1, n - 1]. Открытый ключ вычисляется из закрытого по следующей формуле (здесь и далее набор параметров алгоритма (p, a, b, G, n, h)):

$$Q = dG$$

Для вычисления значения открытого ключа по закрытому ключу и генерирующей точке существуют эффективные алгоритмы, позволяющие вычислить открытый ключ быстро. А вот обратная задача, то есть вычисление закрытого ключа по известной генерирующей точке и открытому ключу, считается сложной. Эта задача называется задачей дискретного логарифмирования, и именно на сложности ее решения базируется криптографическая стойкость алгоритма ECDSA. Для того чтобы эта задача была по-настоящему сложной и не решалась за приемлемое время на обычных компьютерах, необходимо выбирать большие значения p и n. Например, для одного из специфицируемых стан-

дартом IEEE 1609.2 набора параметров алгоритма ECDSA под названием NIST P-224 параметры p и n имеют следующие значения:

$$p = 26959946667150639794667015087019630673557916260026308143510066298881$$

$$n = 26959946667150639794667015087019625940457807714424391721682722368061$$

Теперь перейду к процедуре генерации электронной подписи алгоритмом ECDSA. Выпишу ее в виде алгоритма (m - это исходное сообщение):

1) - Сперва необходимо выбрать случайное число:

$$k \in [1, n-1]$$

2) - Далее вычисляем точку и число:

$$kG = (x_1, y_1);\ r = x_1\ mod\ n$$

3) - Если r = 0, то возвращаемся к шагу №1

4) - Затем необходимо вычислить значение:

$$s = k^{-1}(Hash(m) + dr)\ mod\ n$$

5) - Если s = 0, то возвращаемся к шагу №1

6) - Возвращаем сообщение m и пару чисел (r, s)

Процедура проверки электронной подписи выглядит следующим образом:

1) - Проверяем, что:

$$r \in [1, n-1]; s \in [1, n-1]$$

2) - Вычисляем значения:

$$u_1 = s^{-1}Hash(m)\ mod\ n$$

$$u_2 = s^{-1}r\ mod\ n$$

3) - Вычисляем точку:

$$P = (x_2, y_2) = u_1G + u_2Q$$

4) - Подпись действительна тогда и только тогда когда:

$$r = x_2\ mod\ n$$

Проверка корректности алгоритма

Теперь проверим корректность этого алгоритма (нестрого). Сперва перепишем P в несколько другом виде, учитывая что Q=dG:

$$P = u_1 G + u_2 Q$$

$$P = u_1 G + u_2 dG$$

$$P = (u_1 + u_2 d)G$$

Учитывая определение u_1 и u_2, получим:

$$P = (u_1 + u_2 d)G$$

$$P = (s^{-1} Hash(m) + s^{-1} rd)G$$

$$P = s^{-1}(Hash(m) + dr)G$$

Ранее было дано следующее определение:

$$s = k^{-1}(Hash(m) + dr)\ mod\ n$$

Умножив обе части уравнения на k и поделив на s, мы получим, что:

$$k = s^{-1}(Hash(m) + dr)\ mod\ n$$

А это значит, что:

$$P = kG \Rightarrow x_2 = r$$

Из написанной выше проверки корректности следует, что посредством этого алгоритма значение r было вычислено двумя способами: на передающем устройстве с помощью закрытого ключа и на принимающем с помощью открытого. Затем 2 значения r были сопоставлены друг с другом.

Заключение

В данной статье были рассмотрены базовые принципы функционирования стандарта IEEE 1609.2, описывающего защиту информации в транспортных сетях, работающих по технологии Wi-Fi. Сперва был рассмотрен набор стандартов для беспроводной связи в транспортных сетях. Затем был сделан обзор методов распределения открытых и генерации секретных ключей в сетях V2X. Далее была описана арифметика криптографии на эллиптических кривых и алгоритм ECDSA, используемый для создания электронной подписи в стандарте IEEE 1609.2. В конце была проверена корректность алгоритма ECDSA.

СПИСОК ЛИТЕРАТУРЫ

1. Грингард, Сэмюэл Интернет вещей. Будущее уже здесь / Сэмюэл Грингард. - М.: Альпина Паблишер, 2016. - 188 с.

2. Байер, Доминик Microsoft ASP .NET. Обеспечение безопасности / Доминик Байер. - М.: Питер, Русская Редакция, 2008. - 430 с.
3. Здор, С. Е. Кодированная информация. От первых природных кодов до искусственного интеллекта / С.Е. Здор. - М.: Либроком, 2012. - 168 с.
4. IEEE 1609.2-2013 - http://www.ieee.org/findstds/standard/1609.2-2013.html
5. IEEE Internet of Things https://iot.ieee.org/

УДК 004.056.5

А. Р. ГАРАПОВ
Garapov_2015@mail.ru

Уфимский государственный авиационный технический университет

ОСОБЕННОСТИ ОРГАНИЗАЦИИ УДАЛЕННОГО МОНИТОРИНГА И ДИАГНОСТИКИ ЭНЕРГЕТИЧЕСКОГО ОБОРУДОВАНИЯ

Аннотация. В данной статье рассматривается особенности организации удаленного мониторинга и диагностики энергетического оборудования. А так же предложен пример решения защиты информации для удаленного доступа с помощью устройства типа «диод».
***Ключевые слова*:** информационная безопасность; передача данных; мониторинг; локальные сети.

ИТ-инфраструктура современного предприятия уже давно предполагает значительную распределенность в пределах локальной вычислительной сети, а также выход за контролируемый периметр, и даже может пересекать физические границы страны, в том числе находиться в другой правовой юрисдикции.

На практике такая распределенность может выглядеть как:

– использование различных сервисов государственных и регулирующих органов, новостных сервисов и сервисов аналитики, взаимодействие с контрагентами и службами технической поддержки оборудования и ПО;

– использование сторонних услуг SOC и NOC;

– использование предприятием арендуемых аппаратных мощностей (VM) по принципу IaaS;

– использование стороннего ПО на принципах SaaS;

– развитие облачных и ресурсоемких систем Data Science и Machine Learning и т.п.

Любой из приведенных выше примеров показывает использование ресурсов, находящихся далеко за пределами периметра сети отдельного предприятия. Как следствие, практически каждая локальная сеть имеет сопряжение с сетью Интернет и сетями сторонних организаций. К сожалению, очень часто такие точки взаимодействия не имеют каких-либо дополнительных средств защиты, кроме стандартных межсетевых экранов.

Удаленные сервисы на предприятиях энергетики

Требования, предъявляемые к современному предприятию, предполагают определенную степень открытости и взаимодействия. Без этого невозможно построение современного конкурентоспособного и развивающегося бизнеса. В частности, особую важность приобретает взаимодействие с поставщиками (вендорами) промышленного оборудования. Не является здесь исключением и энергетический сектор. Например, компания *GE* еще в 2018 г. Предложила[1] своим клиентам программные продукты по управлению эффективностью активов на базе разработанной облачной платформы. Решение в том числе позволяет проводить техническое обслуживание "по состоянию" и осуществлять удаленный мониторинг оборудования из глобального центра мониторинга и диагностики. Это только один из примеров наиболее тесного сопряжения сетевых ресурсов предприятия энергетики со сторонним поставщиком в целях организации мониторинга и поддержки.

Очень часто сервис, который предлагается производителем, носит удаленный характер взаимодействия. В первую очередь это связано с тем, что нередко для анализа ситуации или расследования какого-либо инцидента требуются специализированные решения вендора – его внутренние системы, профильные эксперты, сотрудники службы технической поддержки.

Другими примерами взаимодействия предприятия энергетики с внешними контрагентами в части обмена информацией могут быть:

– передача данных об ошибках в работе оборудования его производителю;

– вывод "картинки" в экспертный ситуационный центр;

– передача данных в специализированные организации, оказывающие услуги по устранению инцидентов безопасности;

– обмен данными с третьей и четвертой линиями технической поддержки производителей и поставщиков и т.п.

"Диоды" для защиты удаленного периметра

Новые технические и сервисные возможности, предполагающие расширение границ бизнеса и повышение его конкурентоспособности, одновременно расширяют контролируемый сетевой периметр и идут бок о бок с новыми вызовами в области информационной безопасности. Неконтролируемый и непрогнозируемый доступ к защищенному сегменту предприятия порождает угрозы из сопрягаемых сетей, которые могут приводить к катастрофическим последствиям. За последние несколько лет уже наблюдались примеры неконтролируемого распространения вирусов и скомпрометированного ПО из внешних сетевых сегментов, обладающих меньшим уровнем доверия. Такое распространение обычно происходит веерно и исключительно быстро.

Производители оборудования, ПО, АСУ ТП для предприятий энергетики и сами стараются предлагать самые различные инструменты для устранения этой проблемы (NGFW, специализированные маршрутизаторы промышленного трафика, средства защиты информации и т.п.).

В последнее время одним из применяемых на практике решений стало использование устройств класса "диод" (однонаправленный шлюз). На западных рынках применение таких устройств в промышленности и энергетике уже давно является стандартом и "настойчивой рекомендацией" регуляторов[2],[3],[4].

Особое внимание производителей, предприятий энергетики и представителей регуляторов к такому классу решений связано с тем, что на данный момент число доступных практических сценариев использования "диодов" значительно выросло. Важной особенностью всех этих сценариев является тот факт, что во всех случаях применения "диодов" обеспечивается гарантированная защита сетевого сегмента от какого-либо внешнего воздействия на физическом уровне. Несколько возможных сценариев их применения для предприятий энергетики в целях решения задач мониторинга представлены ниже.

Однонаправленные шлюзы могут применяться для репликации различных источников данных из технологической сети предприятия в некую сторон-

нюю сеть, в том числе в сеть производителя оборудования. Репликация исторических данных, доставка файлов могут быть использованы в сценариях предоставления отчетности, обмена сырыми данными и файлами, обеспечивающими сопровождение процессов отладки и мониторинга. Внешние пользователи и приложения, например служба технической поддержки производителя оборудования, могут обращаться к ним без какой-либо угрозы для технологической сети и оборудования критической инфраструктуры предприятия.

Еще одним сценарием применения "диодов" является передача Syslog-трафика и трафика, циркулирующего в технологическом сегменте предприятия, на специализированные серверы/системы безопасности сторонней организации или в пределах одного предприятия.

Такая передача выполняется для фиксации событий в SIEM-системах, специализированных системах обнаружения вторжений и изменения сетевой топологии, функционирующих в рамках корпоративных SOC, NOC-центров. В тех случаях, когда предприятие имеет филиальную структуру, решение с применением однонаправленных шлюзов может использоваться для сбора/передачи данных в головные SIEM-системы и центры компетенций.

Другим вариантом эффективного взаимодействия в условиях гарантированной защиты от внешнего воздействия может быть организация мониторинга данных через "диод" с автоматизированных рабочих мест в защищенном сегменте и демонстрации этих данных получателю через стандартные средства воспроизведения видеопотока. Такой сценарий позволяет обеспечить эффект присутствия внешнего специалиста или эксперта и своевременно оказать качественную поддержку сотрудникам предприятия в режиме реального времени. Рассмотрим такой кейс более подробно на примере следующей схемы передачи видеотрафика и снимков рабочего стола (онлайн) показанный на рис1.

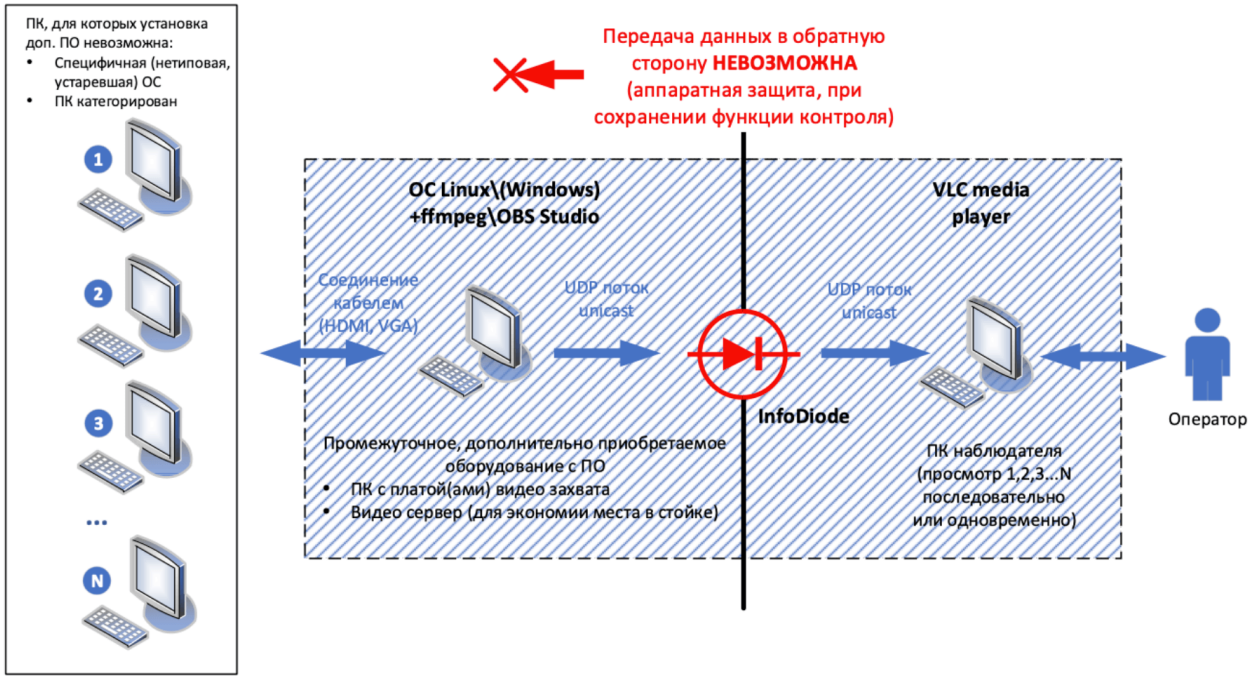


Рис. 1. Схема передачи видеотрафика и снимков рабочего стола

Мониторинг и воспроизведение видео от источника/источников в закрытом сегменте к приемнику в открытом сегменте осуществляется по протоколу UDP в режиме unicast показанный на рис1. Передача UDP-потока с одной рабочей станции на другую в изолированный сегмент сети осуществляется через "диод" и исключает возможность какого-либо воздействия на защищаемый сегмент. В качестве ПО для просмотра полученного сигнала на рабочих станциях также могут применяться общедоступные и бесплатные решения/плееры.

Следует обратить внимание на то, что описанный выше сценарий может быть реализован как с использованием аппаратно-программного решения ("диодов", включающих и программную, и аппаратную компоненты), так и аппаратного решения.

Подводя итог

Еще несколько лет назад межсетевые экраны были фактически единственной доступной технологией, способной защитить наиболее критические объекты сети и отделить их от сетей сторонних обслуживающих организаций и сети Интернет, обеспечивая при этом мониторинг и сбор информации из закрытого сегмента. Однако современные компьютерные атаки демонстрируют спо-

собность планомерно и эффективно обходить все программные средства обеспечения безопасности, в том числе межсетевые экраны. Поэтому современное предприятие в области энергетики, равно как и в других областях, безусловно, должно рассматривать весь перечень доступных средств защиты своих процессов и организации их безопасного мониторинга. Это связано не только с ростом числа атак на промышленные объекты, но и с ростом количества точек сопряжения локальных сетей с внешними, не контролируемыми сетевыми сегментами. Возможно, в данном случае не стоит дожидаться формирования более четких требований и рекомендаций по применению "диодов" со стороны регуляторов, которые, в свою очередь, могут отставать от западных практик на 2–3 года.

СПИСОК ЛИТЕРАТУРЫ

1. https://www.ge.com/news/press-releases/ge-представила-сервисные-решения-для-повышения-производительности-и-надежности (дата обращения 20.09.2021)
2. NSA and CISA Recommend Immediate Actions to Reduce Exposure Across Operational Technologies and Control Systems, https://us-cert.cisa.gov/ncas/alerts/aa20-205a (дата обращения 20.092021)
3. NIST SP800-82. Guide to Industrial Control Systems (ICS) Security https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf (дата обращения 20.092021)
4. Cybersecurity for Industrial Control Systems - Документ Национального агентства по безопасности информационных систем Франции, https://www.ssi.gouv.fr/uploads/2014/01/industrial_security_WG_Classification_Method.pdf (дата обращения 20.092021)

УДК 004.056.5

А. О. ДАВЫДОВА, Д. А. КУСЯПОВА, Я. Э. ТИТУХ
kusyapovadilara@gmail.com
Науч. руководв. – канд. техн. наук, доц. А. Ю. СЕНЦОВА

Уфимский государственный авиационный технический университет

ЦЕЛЕВОЙ ФИШИНГ: СТРУКТУРА И МЕТОДЫ БОРЬБЫ

Аннотация. Атаки, начальным этапом которых являются действия злоумышленника, использующие методы социальной инженерии, на данный момент являются одним из самых распространенных видов атак. При использовании социальной инженерии злоумышленник стремится получить конфиденциальную информацию и доступ в различные интересующие сегменты предприятия при помощи психологического воздействия и манипуляций на пользователей. Чтобы успешно провести атаку с помощью социальной инженерии, необходимо войти в доверие к «жертве», что успешно осуществляется с помощью целевого (персонализированного) фишинга. По причине относительной легкости осуществления сегодня наблюдается стремительный рост использования целевых фишинговых атак как на домашние персональные компьютеры, так и на компьютеры сотрудников крупных компаний. Целевые фишинговые атаки тщательно продумываются для воздействия на определенный тип людей, и научить пользователей их различать практически невозможно. В данной статье раскрываются понятие и методы целевого фишинга, а также решения и способы защиты от данного вида атак. Кроме того, эта обзорная статья представляет собой попытку научить пользователей распознавать целевые фишинговые электронные письма. В статье также приводятся примеры атак с использованием целевого фишинга.
Ключевые слова: фишинг; социальная инженерия; целевой фишинг; персонализированный фишинг; атака.

Введение

Одним из самых уязвимых компонентов любой системы защиты информации являются исполнители, которые используют технику защиты информации, а также сотрудники компании, которые могут, зачастую, пренебрегать правилами политики безопасности. Эксплуатируя эту уязвимость системы защиты информации и корпоративной информационной системы в целом, с помощью методов социальной инженерии, злоумышленник может получить пользовательскую информацию для дальнейших мошеннических действий. Наиболее популярный на сегодняшний день метод социальной инженерии– целевой (персонализированный) фишинг.

Самое распространенное определение фишинга – это письма на электронную почту, похожие на сообщения от существующих, легальных организа-

ций. Данные сообщения обычно несут не ознакомительный характер, а принуждают, подталкивают пользователя к какому-либо действию, например, подтверждение своей учетной записи. Такие письма рассылаются большому количеству пользователей и, обычно, не содержат в себе какой-либо детальной информации об атакуемом. Целевой фишинг является более сложной модификацией фишинговых атак и, прежде чем осуществить такую атаку, злоумышленник должен выяснить как можно больше личной информации о жертве, поэтому целевой или персонализированный фишинг требует тщательной подготовки и не малых физических и материальных затрат от злоумышленника. Но вероятность проведения успешной атаки на основе целевого фишинга в разы увеличивается, по сравнению с обычным нецелевым фишингом. Согласно отчету Verizon о кибербезопасности, злоумышленник, отправивший 10 персонализированных фишинговых писем, имеет 90-процентную вероятность того, что один человек попадется в ловушку [1].

По данным компании Group-IB, ежедневно жертвами финансового фишинга в России становятся около 1000 клиентов различных банков, что в три раза превышает ежедневное количество жертв от вредоносных программ, а около 10–15 % посетителей финансовых фишинговых сайтов вводят на них свои данные [2]. Кроме того, любая фишинговая атака может являться первым этапом жизненного цикла атаки, которая приведет к еще более серьезным последствиям, в том числе денежному ущербу и деструктивным воздействиям на информационную систему. Поэтому, темы, связанные с социальной инженерией и, особенно с персонализированным фишингом, являются особо актуальными.

Одним из последних примеров атаки с использованием целевого фишинга являются письма, которые приходили пользователям, якобы от портала «Госуслуги». Письмо было похоже на подлинное сообщение портала «Госуслуги» и содержало следующие элементы: логотипы в начале и конце письма, похожий шрифт и гиперссылки голубого цвета. В самом письме содержались сведения о том, что в отношении его получателя вынесено постановление о начислении социальных компенсаций. Для их оформления предлагалось перейти в личный

кабинет и обратиться к ведущему юристу, а для идентификации в личном кабинете необходимо указать номер СНИЛС. После перехода по ссылке в браузере открывалось окно, в котором пользователь должен был указать номер своей банковской карты, на которую должны поступить выплаты [3].

Благодаря тому, что злоумышленники обращаются к атакуемому по имени и знают точный адрес получателя, увеличивается степень доверия к вредоносному письму и вероятность того, что атака будет успешной, повышается в несколько раз.

Ситуация усугубляется тем, что на данный момент не существует средств защиты информации, которые были бы способны гарантированно детектировать и предотвращать атаки, начинающиеся с целевого фишинга, в котором злоумышленники используют человеческий фактор как уязвимость системы, и только технических (программных) средств защиты в этом случае недостаточно. Статья направлена на анализ методов целевого фишинга и существующих мер защиты от внедрения вредоносного программного обеспечения (ПО) в корпоративную среду данным путем. Также приводятся рекомендации по комплексности защиты от целевого фишинга.

1. Особенности целевого фишинга

Классический фишинг– это массовая рассылка писем с идентичным содержанием. Целевой фишинг (англ. spear-phishing), в отличие от классического, направлен на конкретную цель, а значит является намного опаснее. Качественно составленное письмо для целевого фишинга очень трудно отличить от легитимного письма.

Кроме того, целевой фишинг предполагает тщательную подготовку и большие затраты ресурсов, таких как время и денежные средства. Но вероятность проведения такой атаки во много раз успешнее, чем атака с помощью обычного фишинга, следовательно, данная атака окупит все затраты на ее проведение.

Структура целевой фишинговой атаки состоит из нескольких этапов (рисунок 1). Первым этапом, как и в любых других видах атак, является планиро-

вание. На данном этапе проводится разведка и анализ уязвимостей. Следующим этапом выступает подготовка, на котором злоумышленники выясняют нужные адреса электронной почты: покупают списки на других теневых ресурсах и получают конкретный список для рассылки писем по действующим адресам либо путем внедрения вредоносного ПО, которое собирает адреса. Затем регистрируется домен и создается фальшивый веб-сайт, с правдоподобным видом, на который будут перенаправляться жертвы и на этом же этапе происходит составление фишинговых писем.

После этого мошенники реализуют атаку: отправляют письма и внедряют вредоносное ПО. Далее производится сбор информации, злоумышленники получают учетные данные или другие сведения о банковских счетах жертв, с помощью которых крадут данные и (или) денежные средства, они используют информацию в своих целях и шантажируют пользователей. Заключающим этапом структуры целевой фишинговой атаки является сокрытие присутствия злоумышленника в системе. Этот этап направлен на маскирование злоумышленника и, в отдельных случаях, на внедрение вредоносного ПО, который позволит скрыть метаданные злоумышленника и повлиять на системные журналы и журналы безопасности, которые могли зафиксировать те или иные действия злоумышленника в системе.

Рис. 1. Структура целевой фишинговой атаки

В зависимости от атакующего воздействия можно выделить несколько видов фишинговых писем:

1. Письмо, содержащее ссылку.

В таком мошенническом письме содержится ссылка, по которой должен перейти атакуемый. Атакуемый должен перейти на определенный веб-ресурс, где, используя уязвимости самого сайта или браузера пользователя, мошенники попытаются внедрить вредоносное ПО. Для проведения таких действий злоумышленниками специально создаются фишинговые сайты, время жизни которых невелико. Чаще всего они являются точными копиями известных сайтов, повторяя их дизайн, структуру и функциональность. При переходе по ссылке пользователь становится жертвой различных видов XSS-атак. Суть данных атак заключается в выполнении скрипта в браузере и последующем его взаимодействии с сервером злоумышленника. Эти операции позволяют получить доступ к данным браузера и дают возможность применять к нему эксплойты, а также получать cookie, данные авторизации или, например, выполнять HTTP-запросы от имени пользователя [4]. Сегодня злоумышленники даже рекламируют свои ресурсы в социальных сетях и поисковых системах и выводят в топы ссылки на свои фишинговые сайты.

2. Письмо с вредоносным вложением.

В качестве вложения в фишинговое письмо злоумышленник может поместить имитацию отчета коллеги за предыдущий месяц, задание от руководителя или сообщение от банка, приславшего пользователю иск за неуплату по кредиту. Вложения бывают в форматах *.doc или *.pdf. Файлы формата *.pdf часто содержат объекты JavaScript. Поэтому для злоумышленника достаточно просто создать некоторый скрипт, который использовал бы одну из уязвимостей движка от Adobe [5]. В документах Microsoft Office вредоносное ПО может загружаться при помощи макросов, которые содержит файл. При открытии документа исполнение макроса позволяет установить соединение с сервером злоумышленника и начать загрузку. Для защиты от данного вида писем в рамках поли-

тики безопасности в организациях необходимо отключать поддержку макросов. Но, если пользователь не соблюдает политику безопасности, то при использовании социальной инженерии, злоумышленник может заставить его отключить защиту от макросов [5], [6]. На данный момент большинство способов эксплуатации уязвимостей пакета прикладных программ Microsoft Office не требуют использования макросов. Например, используя самую популярную уязвимость 2017 года CVE-2017-0199 [7], при открытии вложенного *.rtf файла можно подгрузить HTA приложение, поддерживающее исполнение сценариев, со стороннего сервиса и запустить его. Помимо рассмотренных случаев существует множество других офисных продуктов и форматов, с которыми они работают. Но принцип атаки один и тот же– запустить скрытый сценарий, который позволит загрузить ПО злоумышленника на атакуемый компьютер. Самыми популярными инструментами для создания вредоносных вложений, отправляемых в фишинговых письмах, стали Microsoft Word Intruder (MWI) и Offensive Ware Multi Exploit Builder (OMEB) [2].

В недавней фишинговой кампании группа 74 (также известная как Sofact, APT28, Fancy Bear) нацелилась на профессионалов в области кибербезопасности. Было написано электронное письмо, якобы связанное с конференцией Cyber Conflict U. S. conference и мероприятиями, организованными United States Military Academy Army Cyber Institute, NATO Cooperative Cyber Military Academy и NATO Cooperative Cyber Defence Centre of Excellence. Хотя CyCon– это настоящая конференция, вложение являлось документом, содержащим вредоносный макрос Visual Basic для приложений (VBA), который загружал и запускал вредоносное программное обеспечение, называемое Seduploader [8]. Хотя атакуемыми были специалисты по безопасности, которые имеют обширные знания в области инструментария злоумышленников, атака была проведена успешно и, злоумышленником удалось получить личные данные большого количества специалистов по безопасности.

Еще одним ярким примером фишинговой атаки является атака Energetic Bear, которая включает в себя рассылку фишинговых писем с вредоносным содержимым. Основными целями этой атаки являются предприятия топливно-энергетического комплекса и другие промышленные предприятия. Проведение такой атаки помогает злоумышленнику провести сканирование скомпрометированных систем на наличие уязвимостей.

Из всех возможных вариантов получения несанкционированного доступа к учетной записи с помощью целевого фишинга самым эффективным на сегодняшний день является использование фишинг-движков, также называемых фейками [9]. Основан этот метод на веб-программировании и социальной инженерии. Движки выполняют три основные функции:

1. Имитация интерфейса по заданной ситуации, связанной с операциями пользователя.

2. Копирование и обработка незаконно полученных учетных данных пользователя.

3. Возврат пользователя на соответствующую ситуации страницу официального сервиса.

Движок состоит из элементов скопированного Интернет-ресурса, и программ скриптов, написанных злоумышленником. Собранный и готовый к работе движок злоумышленник размещает на сервере и присваивает ему подготовленное доменное имя.

В случае использования фишинга как инструмента комбинированный атаки фишинговое письмо может содержать вредоносный файл, например бэкдор, открывающий доступ злоумышленнику к операционной системе компьютера пользователя и его сетевому окружению.

В ходе подготовки к целенаправленной фишинговой атаке осуществляется изучение круга общения атакуемого, его интересов, сфера деятельности. Кроме этого, злоумышленникам необходимо понимать, каким программным обеспечением и устройствами пользуются атакуемый. В зависимости от ис-

пользуемых методов авторизации, просмотра писем необходимо подготовить интерфейс фишинг-движка. Также для злоумышленника важно знать, в какие периоды времени пользователь осуществляет обработку почты. Кроме того, злоумышленником собирается информация об используемых провайдерах и местах, где осуществляется подключение к сети «Интернет». Эти сведения необходимы для подготовки персонализированного фишинг-движка, а также планирования дальнейших действий злоумышленника.

2. Существующие меры защиты

2.1 Организационные меры

Обучение и осведомленность сотрудников компании являются основным фактором снижения риска целевого фишинга. Чтобы защититься от целевого фишинга, необходимо, в первую очередь, ввести определенные организационные меры, и обучить сотрудников распознаванию таких мошеннических писем.

Первое, на что стоит обратить внимание– это письма, в которых содержится просьба или указание ввести какие-либо данные, путем перехода по ссылке или каким-либо иным способом. Никакая служба не должна спрашивать данные пользователя, поскольку они и так уже есть в их системе.

Второй момент, который должен насторожить пользователя– указание в письме угрозы о блокировки учетной записи, если не последовать инструкции. Это пример манипуляции со стороны злоумышленников.

Конечно же, при получении письма на электронную почту стоит обратить внимание на адрес отправителя. В нем могут быть небольшие отличия от официального электронного адреса службы, например, одна лишняя буква, знак или замена буквы на цифру. В примере, приведенном раннее в этой статье, где недавно был произведен направленный фишинг с помощью письма, присланного от портала «Госуслуги», о том, что письмо мошенническое, ясно говорил адрес отправителя– info@mybusinessplan.ru. Но, тем не менее, даже, несмотря

на такой явный признак фишингового письма, многие атакуемые переходили по ссылкам, указываемым в этих письмах.

Однако, при совпадении адреса отправителя с официальным адресом не является стопроцентным доказательством того, что письмо не является фишинговым. Злоумышленники могут манипулировать отображением ссылки в адресной строке с помощью технологии «спуфинг» (англ. Spoofing– обман, мистификация). Злоумышленники также могут подделывать, даже SSL-сертификат– цифровое удостоверение сайта, которое подтверждает, что обмен данными между сайтом и браузером идет по защищенному каналу. Таким образом, использовать только организационные меры для защиты от целевых фишинговых атак нельзя.

2.2 Программно-аппаратные меры

Помимо организационных мер, которые, безусловно, помогут снизить риск атак целевого фишинга, существуют различные программные решения для обнаружения и пресечения направленного фишинга.

Фильтрация нежелательных писем– основной этап защиты в борьбе с фишингом. Распространенные системы фильтрации спама:

1. Анализ IP-адреса сервера отправителя, направленный на установление репутации IP отправителя, путем его поиска в «черных списках», защита эффективна лишь против массового фишинга.

2. Анализ тела письма, производит поиск словосочетаний, применяемых при фишинговых атаках.

3. SPF/DKIM-анализ. Широкое применение проверки электронной почты с помощью взаимодополняющих методов проверки подлинности писем и выявления почтовых сообщений от злоумышленников, таких как: SPF (Sender Policy Framework– вид проверки подлинности, помогает идентифицировать авторизованные почтовые серверы для конкретного домена) и DKIM (DomainKeys Identified Mail– криптографический способ проверки подлинности, позволяет проверить и определить авторизацию электронного письма, по-

лученного из данного домена) обеспечит эффективное противодействие целевому фишингу. Дополнительную защиту для писем, может также обеспечить очистка HTML, в случаях, когда с помощью SPF и DKIM не удается проверить подлинность сообщения. При использовании очистки HTML возможен просмотр скрытого, потенциально опасного содержимого, так как переход по URL-адресам невозможен и ссылки преобразуются в текст.

4. Анализ заголовков пакетов, заключающийся в работе межсетевого экрана, осуществляющего контроль и фильтрацию сетевого трафика.

5. Анализ загружаемого или работающего ПО, посредством антивирусных решений, с использованием таких методов, как: сигнатурный и эвристический анализы, песочница.

Еще одним методом для борьбы с целевым фишингом может выступить выявление фактов неавторизованного доступа к компьютеру и выявления вредоносного ПО с помощью системы обнаружения вторжений (IDS), а также система предотвращения вторжений (IPS). Первая система осуществляет поиск злонамеренных файлов сигнатурным анализом, при котором эксплуатация уязвимостей нулевого дня останется незамеченной. IPS же проводит ответные действия на нарушение, чем в большей степени полезна для обеспечения безопасности.

Также могут использоваться комплексные решения, к примеру, UTM- системы, включающие в себя сразу вышеперечисленные решения: межсетевой экран, фильтр URL, антивирусное решение, спам-фильтры, IDS/IPS. Их применение упрощает настройки и обучение персонала, а также снижает затраты на защиту.

Одно из комплексных решений представляет компания Cisco– комплексное средство защиты IronPort, которое направлено, именно на борьбу с целевым фишингом. Данное средство защиты обеспечивает защиту от целевого фишинга путем мониторинга писем и веб-трафика, и технологии проверки подлинности сообщений. Эффективно выявлять и блокировать целенаправленные фишинго-

вые атаки, средству защиты IronPort, позволяет сеть SenderBase, где выполняется постоянный мониторинг более чем 30% мирового почтового трафика и веб-трафика.

Обладая информацией об IP-адресах, SenderBase отслеживает необходимые параметры, (объем письма при отправке и объем трафика с веб-сайта, уровни жалоб, параметры учета в «ловушках спама», разрешение имен DNS, страна происхождения и наличие в черном списке, когда было зарегистрировано доменное имя и др.) используя которые, в дальнейшем, определяет показатель репутации и уровень угрозы письма. Присвоив URL-адресу показатели репутации, посредством фильтра веб-репутации IronPort Web Reputation Filters, устройства IronPort вправе разрешить пометить или заблокировать письма от отправителей [10].

Использование таких комплексных решений позволит во много раз снизить вероятность проведения успешной целевой фишинговой атаки.

Выводы

Знание специалистами основ и тактик применения социальной инженерии, и в частности, механизмов фишинговых атак, способно существенно усовершенствовать систему защиты информации на предприятии в силу того, что почти все атаки начинаются с этапа разведки. Понимание основных принципов социальной инженерии должно учитываться при проектировании системы защиты информации, разработки регламентов информационной безопасности, политики безопасности и, несомненно, поможет при расследовании уже произошедших инцидентов информационной безопасности.

По причине того, что специализированные средства защиты информации, способные обнаружить фишинговые письма, сейчас мало используются на предприятиях, а нормативные правовые акты, которые регламентировали бы сферу социальной инженерии и фишинга практически отсутствуют в нашей стране, проблемы, поднятые в данной статье актуальны и требуют дальнейшего изучения.

СПИСОК ЛИТЕРАТУРЫ

1. Verizone. 2020 Data Breach Investigations Report [Электронный ресурс] URL: https://enterprise.verizon.com/resources/reports/dbir/ (дата обращения: 27.03.2021)
2. High-Tech Crime Trends 2017 [Электронный ресурс] URL: https://www.group-ib.ru/resources/threat-research/2017-report.html (дата обращения: 27.03.2021)
3. Мошенники придумали новую схему обмана россиян под видом выплат с «Госуслуг» [Электронный ресурс] URL: https://iz.ru/1131861/2021-03-03/moshenniki-pridumali-novuiu-skhemu-obmana-rossiian-pod-vidom-vyplat-s-gosuslug (дата обращения: 02.04.2021)
4. Защита внешнего информационного периметра организации от целевого фишинга [Электронный ресурс] URL: https://www.unido.org/sites/default/files/files/2019-05/Zhurin_Paper.pdf (дата обращения: 07.04.2021)
5. Dissecting Spear Phishing Emails for Older vs Young Adults: On the Interplay of Weapons of Influence and Life Domains in Predicting Susceptibility to Phishing [Электронный ресурс] URL: https://dl.acm.org/citation.cfm?Id=3025831 (дата обращения: 08.04.2021)
6. Individual Cyber Security: Empowering Employees to Resist Spear Phishing to Prevent Identity Theft and Ransomware Attacks [Электронный ресурс] URL: https://papers.ssrn.com/sol3/papers.cfm?Abstract_id=3171727 (дата обращения: 08.04.2021)
7. National vulnerability Database [Электронный ресурс] URL: https://nvd.nist.gov/vuln/detail/cve-2017-0199 (дата обращения: 12.04.2021)
8. Типы фишинговых атак и способы их выявления [Электронный ресурс] URL: https://www.osp.ru/winitpro/2019/03/13054903 (дата обращения: 05.04.2021)
9. Масалков, А.С. Особенности киберпреступлений: инструменты нападения и защиты информации. – М.: ДМК Пресс, 2018. – 226 с.
10. Cisco. Целевой фишинг [Электронный ресурс] URL: https://www.cisco.com/c/dam/global/ru_ru/downloads/broch/ironport_targeted_phishing.pdf (дата обращения: 02.04.2021)

УДК 004.82

Ю. С. ДЬЯКОНОВА
djs237@yandex.ru
Науч. руководитель – канд. техн. наук, доц. В. Е. КЛАДОВ

Уфимский государственный авиационный технический университет

DEEPFAKE: ПОНЯТИЕ И МЕТОДЫ БОРЬБЫ

Аннотация. В данном материале раскрывается понятие дипфейка, рассказывается о принципах работы и описываются методы борьбы с ними.
Ключевые слова: deepfake; дипфейк; искусственный интеллект; генеративно-состязательная нейросеть (GAN).

В начале февраля 2020 года широкий резонанс вызвала новость о том, что индийский политик Маной Тивари эффективно использовал специализированное программное обеспечение «подмены лиц» Deepfake для того, чтобы создать «дипфейк» собственного рекламного ролика на разных языках для того, чтобы привлечь больше избирателей. Данное событие стало очередной убедительной иллюстрацией как значительного политического и маркетингового потенциала дипфейков, так и возможных угроз, исходящих от их применения [1].

В 2018 году появилась первая публичная программа для подмены лиц под названием FakeApp, которая открыла дипфейк-инструменты простому обывателю. Наборы для создания такого контента находятся с тех пор в свободном доступе и легки в освоении. Любой человек, который имеет доступ к интернету, свободное время, цели и мотивацию, может в режиме реального времени создавать фальшивый контент и наполнять им каналы социальных сетей [2].

Технология «Дипфейк» появилась в 2014-м. Алгоритм создал студент Стэнфордского университета Ян Гудфеллоу. Термин «дипфейк» происходит от слов «deep learning», то есть «глубокое изучение» и «fake» - «подделка» [3]. Дипфейки — результат достижений в сфере искусственного интеллекта, к которому нередко прибегают злоумышленники, использующие эту технологию для генерации все более реалистичных и убедительных фальшивых изображений, видео, голосовых записей и текстов. Эти видео создаются путем наложе-

ния существующих изображений, аудио и видео на исходные медиафайлы с помощью передового метода глубокого обучения под названием «генеративно-состязательные нейросети» (generative adversarial network, или GAN). GAN — относительно новая концепция в области искусственного интеллекта, целью которой является синтез искусственных изображений, неотличимых от подлинных. В методике GAN одновременно задействованы две нейросети: одна сеть, называемая «генератор», использует набор данных для создания образца, имитирующего их. Другая сеть, известная как «дискриминатор», оценивает, насколько генератору это удалось. При многократном повторении оценки дискриминатора оказывают влияние на оценки генератора. Прогрессирующее совершенствование методики GAN привело к созданию еще более убедительных дипфейков, которые практически невозможно разоблачить, и результат намного превосходит по скорости, масштабу и точности тот, которого могли бы достичь люди-эксперты [4].

Дипфейки представляют собой серьезную угрозу, так как подобного рода контент является, по сути, информационной атакой. IT-аналитики заявляют, что технология Deepfake может стать самой опасной в цифровой сфере за последние десятилетия. Уже в ближайшем будущем дипфейк может затронуть различные уровни общественной и политической жизни и способствовать распространению широкого спектра угроз: от репутационных рисков для знаменитостей и обычных граждан, до развития организованной преступности и проблем социальной стабильности и национальной безопасности [2].

Как с ними бороться?

Проблема дипфейков кажется весьма сложной. Поскольку они создаются с помощью искусственного интеллекта, для борьбы с ними нужно использовать нечто аналогичное.

В настоящее время рынок ИБ не предлагает специальных технологий и решений для защиты от дипфейков. Тем не менее, определенные шаги в данном направлении совершаются. Например, Facebook, Microsoft и исследователи из

американских университетов начали разработку инструментов для обнаружения подобных подделок, а также в сотрудничестве с Amazon решили провести конкурс Deepfake Detection Challenge на лучший способ определения дипфейк-видео. Управление перспективных исследовательских проектов Министерства обороны США (DARPA) запустило алгоритм выявления поддельных видеоматериалов. В статье, опубликованной в июне 2018 года [5], рассказывается о том, как анализ частоты моргания может помочь обнаружить дипфейк. Идея такова: обычно в открытом доступе трудно найти фотографии человека в момент моргания, так что нейронной сети просто не на чем учиться генерировать подобные кадры. Кроме того, у оригинала и подделки могут различаться некоторые примечательные части лица (подбородок, брови, скулы, усы и борода, веснушки и родимые пятна); любое несоответствие – свидетельство дипфейка. В качестве примера можно это увидеть на видео «Билл Хейдер пародирует Тома Круза с помощью нейросети».

Ученые по всему миру сейчас увлечены технологиями машинного обучения, а проблема дипфейков выглядит достаточно сложной и интересной, чтобы заинтересовать многих из них. Поэтому выявлению дипфейков с помощью анализа изображений посвящено изрядное количество исследовательских проектов.

Например, авторы двух работ, опубликованных в ноябре 2018 года, порекомендовали искать артефакты искажения лица и несоответствия положений головы [6]. Их метод основан на наблюдениях, что текущий алгоритм deepfake может генерировать изображения только с ограниченным разрешением, которые необходимо дополнительно исказить, чтобы они соответствовали оригинальным лицам в исходном видео. Такие преобразования оставляют характерные артефакты в результирующих видео deepfake, и авторы показывают, что они могут быть эффективно захвачены сверточными нейронными сетями (CNN). По сравнению с другими методами, которые используют большое количество реальных и поддельных изображений, сгенерированных для обучения

классификатора CNN, данному методу не нужны поддельные изображения, сгенерированные в качестве негативных обучающих примеров, так как они ориентируются на артефакты в аффинной деформации лица как на отличительную особенность для различения реальных и поддельных изображений. Преимущества данного метода заключаются в двух аспектах:

1. Такие артефакты могут быть смоделированы непосредственно с помощью простых операций обработки изображений на изображении, чтобы сделать его негативным примером. Поскольку обучение модели глубокой подделки для создания негативных примеров требует много времени и ресурсов, описываемый метод экономит много времени и ресурсов при сборе обучающих данных;

2. Поскольку такие артефакты обычно присутствуют в видео deepfake из разных источников, данный метод более надежен по сравнению с другими. Он оценивается на двух наборах наборов данных видео deepfake на предмет его эффективности на практике.

В другой статье, за 2019 год, описана довольно сложная техника анализа выражения лица и мимики, характерных для конкретного человека [7]. Ученые предполагают, что, когда человек говорит, у него есть различные выражения лица и движения. Учитывая одно видео в качестве входных данных, они начинают с отслеживания движений лица и головы, а затем извлекают присутствие и силу конкретных единиц действия. Затем создают модель обнаружения новизны, которая отличает человека от других людей, а также комедийных подражателей и глубоко фальшивых подражателей.

Однако эти методы вряд ли окажутся успешными в долгосрочной перспективе. В конечном счете упомянутые исследования подсказывают создателям дипфейков, как улучшать дискриминативные сети, что, в свою очередь, приводит к более тщательному обучению генеративных сетей — и как следствие, повышает качество подделок.

Нейросетевые технологии машинного обучения стремительно совершенствуются, на основании чего можно сделать вывод, что создание абсолютно до-

стоверных дипфейк-видео, которые будет невозможно, подвергнув экспертизе, отличить от реально снятых кадров, не «за горами». Если верить прогнозу одного из пионеров всемирной индустрии дипфейк-видео, профессора Хао Ли, «счет идет на месяцы, а не на годы» [8].

СПИСОК ЛИТЕРАТУРЫ

1. Игнатовский Я., Иванов В. Deepfakes: где начинается угроза для личности и национальной безопасности? // Политген. 05.03.2020. URL: https://www.politgen.ru/analytics/reports/deepfakes-gde-nachinaetsya-ugroza-dlya-lichnosti-i-natsionalnoy-bezopasnosti/.
2. Панасенко А. Технологии Deepfake как угроза информационной безопасности // URL: https://www.anti-malware.ru/analytics/Threats_Analysis/Deepfakes-as-a-information-security-threat
3. Как делают дипфейки // URL: https://pikabu.ru/story/kak_delayut_dipfeyki_8035001
4. Deepfakes Lab: распознавание дипфейков и защита от них с помощью ИИ // URL: https://www.it-world.ru/news-company/projects/168075.html
5. In Ictu Oculi: Exposing AI Generated Fake Face Videos by Detecting Eye Blinking // URL: https://www.researchgate.net/publication/325680345_In_Ictu_Oculi_Exposing_AI_Generated_Fake_Face_Videos_by_Detecting_Eye_Blinking
6. Exposing DeepFake Videos By Detecting Face Warping Artifacts // URL: https://arxiv.org/abs/1811.00656
7. Yuming Gu, Mingming He, Koki Nagano, and Hao Li. Protecting World Leaders Against Deep Fakes / USC Institute for Creative Technologies Los Angeles CA, USA // URL: https://openaccess.thecvf.com/content_CVPRW_2019/papers/Media%20Forensics/Agarwal_Protecting_World_Leaders_Against_Deep_Fakes_CVPRW_2019_paper.pdf
8. Носков А. Пионер технологии поддельных видео Хао Ли «подкорректировал» прогноз. // URL: https://hightech.plus/2019/09/24/dipfeiki-stanut-neotlichimi-ot-originalov-v-techenie-6-12-mesyacev

УДК 004.056.53

М. О. ЗАИД АЛКИЛАНИ
Muhannad.killani@Gmail.com
Науч. руководд. – д-р техн. наук, проф. И. В. МАШКИНА

Уфимский государственный авиационный технический университет

OVERVIEW CURRENT PROBLEMS IN THE FIELD OF SAFETY OF ICS

Abstract. Industrial control system ICS is one of the various types of control systems used to monitor production processes. ICSs are used in many industries, including electric power, water supply and wastewater disposal, petroleum and natural gas, chemical and pharmaceutical, pulp and paper, food and beverage, and discrete manufacturing (e.g., automotive, aerospace, and durable goods). Because there are many different types of ICS with varying potential for risk and hazard, this document lists many different methods and techniques for securing ICS TP.
Keywords**:** system; Industrial control system ICS; cyber threats; risks; EPC models; Supervisory Control and Data Acquisition (SCADA); (MOS) model-based design approach; The Process Control Security Requirements Forum (PCSRF).

In the article [8] the article discusses aspects of the creation and development of automated control systems for technological processes. The analysis of the main types of ICS, as well as the scope of their application, is carried out. Determined the search for ways to increase the intellectualization of automated control systems.

In the article [4] 2018, Kaspersky, together with the ARC Advisory Group, conducted a study of information security of process control systems, also touching upon the priorities, concerns and problems of industry representatives. The purpose of the study is to gain an understanding of the measures and processes associated with prevention. The most frequently used solutions are the detection of unauthorized access to the industrial network, the detection of anomalies in industrial processes and monitoring the industrial network for vulnerabilities.

Companies need to take additional measures in order to successfully counter cyber threats. This includes the organization of advanced ICS cybersecurity trainings covering, inter alia, the configuration and maintenance of ICS security components, as well as advanced update management.

In the article [6], the author talks about the development of an automated process control system that combines the production system with the operating system

and talks about risks (threats and attacks), identifies the main risks, organizational and technical measures to protect information in an automated process control system, and develops information security strategies for enterprises by industry, taking into account their specifics.

This research helped create some forms for identifying anticipated threats before they happen.

In the article [1], to determine all information assets in the ICS that are subject to protection, and the sources of threats, a comprehensive model of threats to infringement of IS in the ICS is developed in the form of a fuzzy cognitive map. The input concepts in the presented model are the sources of threats; the output components of the ICS contain information assets to be protected. Intermediate concepts are the means of switching and protecting information about the way of carrying out an attack. Possible sources of attacks on important objects have been identified. Vulnerabilities of the IT infrastructure have been identified. The results of calculations of the numerical assessment of the risk of violation of the IS of the ICS are presented.

In the article [2] This paper presents the results of the analysis of threats to information security breaches of automated process control systems. EPC-models of threats to infringement of information security of modern information and control systems of industrial enterprises are presented. EPC-models allow you to describe in detail the ways of implementing threats. security gaps and weak points in the system. The system has three levels. data, SCADA server, automated workstations of operators (dispatchers). The middle level (automatic control level) contains automation tools such as programmable logic controllers (PLC). Actuators and sensors are located on the lower level. The internal subnet, which includes workstations and ICS servers, is separated from the external subnet by an additional cluster of firewalls.

In this work, to simulate threats to the information security of an automated process control system, the graphical notations EPC (Event-Driven Process Chain) are used, the key elements of which are Events and Functions related to each other. both logical and operational for branching a process, logical relations are used, de-

scribed by the symbols "AND" (/\) "key OR" (\/) and "Exclusive OR" (XOR). It is based on simulating the one who hacked the device using a trojan. The penetration process is tracked by the EPC. In several scenarios, the attack host is different (PC, SCADA, OPC, PLC).

In the article [3], this article discusses a number of examples of industrial cybersecurity and the lessons they can teach us about the dangers of blindly adopting cybersecurity strategies in a factory. We then discuss a set of recommendations for a sustainable approach to Internet adoption.

In the article [5], the author talks about the components of an industrial system (ISC), the main system used (SCADA), (DCS), the life of this system and how to create a policy to solve this problem.

The Process Control Security Requirements Forum (PCSRF) uses common criteria to develop IT security specifications for process control systems. During the initial gathering of information, PCSRF plans to identify IT vulnerabilities in the various industries involved in the project. The results of the individual vulnerability assessments will be analyzed and compiled by the PCSRF into comprehensive vulnerability reports that will be used in the development of the protection profile (s). These protection profiles will be used in the procurement, development and modernization of industrial control systems to improve safety performance.

In [7] this dissertation For Automated process control systems, a reliability analysis system for hazardous industries for the development of safe and fail-safe systems, it is necessary to analyze the corresponding reliability indicators at various stages of development.

The dissertation addresses the analysis of methods for increasing reliability at the various stages of the life cycle of an automated process control system; development of a methodology for multi-attribute decomposition of an automated process control system; development of an algorithm for accounting for the dangers of potential failures; development of a reliability analysis system of an algorithm for entering blocking modules into the structure of an automated process control system when

forming its structure; development of a simulation model for analyzing the reliability of the formed structure of an automated process control system; software development, the development, the development, and implementation of the pillar To achieve the goals and solve problems, methods of probability theory, graph theory, theory of computational processes, reliability theory and the Monte Carlo method were used.

In [9] this article tests applied software at all stages of creating systems, the MOS approach (model-based design approach) is used, The MOS approach provides an increase in the reliability of the created software, The MOS approach based on the concept of "in-the-loop testing".

A variant of the development of the HiL method is proposed, which makes it possible not only to check the created systems for design and development errors, but also to ensure the control of the compatibility of components of two different systems of the same purpose. On the created complex, the problem posed in the article was solved by modifying the HiL method. Debugging of prototypes of software and hardware at the developer's level is carried out using local tests aimed at checking the correctness of the control algorithm.

describing the algorithms for the functioning of technological equipment and ICS, and the mathematical description of the relationship between parameters and variables, this algorithm converts the virtual value of a variable from a physical quantity to a code value normalized to the range of sensor values. The main task of the simulation software and hardware complex is to create an environment where controllers function completely identically to the real ones in external signals. The main task of the simulation software and hardware complex is to create an environment for the operation of controllers that is completely identical to the real ones in external signals. The adequacy of the generated test sequence of signals is determined by the accuracy of the formation of this set of signals and its time parameters.

In [10], this article is an attempt to determine the subject of cybersecurity in ICS and its place in ensuring industrial security and economic efficiency. Currently, a number of researchers have proposed considering cybersecurity through the prism of

a goal or mission. Within the development of this concept, it is proposed to consider the issue of cybersecurity using the methodological apparatus of three disciplines: industrial security, functional security, and information security (centric approach to cybersecurity).

In [11] of this article, for large industrial facilities with an increased technologist hazard, which include, among other things, gas pipeline facilities, the most important requirement is the increased reliability of automation systems. A method for assessing information security threats in automated process control systems ICS of the gas industry based on international standards, its role in the process of assessing safety risks and the method of application. The sources of threats for ICS of gas transmission enterprises are highlighted.

To determine the level of IS threat, the CVSS vulnerability assessment system standard adapted for threat assessment is applied.

In [12], the article proposes a method for predictive control of information security of an object, based on predicting the consequences of the implementation of a particular control command. and also using modern computing facilities. A complex model of a technical automation object is presented. The consequences of the implementation of threats to information security at different levels of the integrated model of the automation object are described. The proposed predictive protection method is aimed at ensuring the security of an integrated technical system, including both the nuclear power plant and the control object. It is important to note that with this approach, safety management is carried out taking into account the target tasks solved by the integrated system.

СПИСОК ЛИТЕРАТУРЫ

1. И.Р.ГАРИПОВ Расчет риска нарушения информационной безопасности Автоматизированная система управления технологическим процессом АСУ ТП/ Технические науки 41//2019. № 1 (20)// ул. К. Маркса, 12, г. Уфа, 450008, Россия.

2. Ирина В. Машкина, Ильдар Р. Гарипов /Разработка EPC-моделей угроз нарушения информационной безопасности АСУ ТП / Ирина В. Машкина, Ильдар Р. Гарипов//БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ = IT Security, Том 26, № 4 (2019)// Поступила в редакцию – 19 января 2019 г. Окончательный вариант – 7 ноября 2019 г// ул. К. Маркса, 12, г. Уфа, 450008, Россия.

3. Eric Byres, P.E., Dr. Dan Hoffman, /The Myths and Facts behind Cyber Security Risks for Industrial Control Systems//Associate Professor BCIT Internet Engineering Lab University of Victoria, Dept. of Computer Science, Burnaby BC, V5G 3H2 Victoria, BC, V8W 3P6.
4. Томас Менце/ Кибербезопасность систем промышленной автоматизации в 2019 году//ARC Group Kaspersky/ Июль 2019 г.
5. Joe Falco, Keith Stouffer, Albert Wavering, Frederick Proctor Intelligent Systems Division/ IT Security for Industrial Control Systems In coordination with the Process Control Security Requirements Forum (PCSRF)// National Institute of Standards and Technology (NIST) Gaithersburg, MD//(http://www.isd.mel.nist.gov/projects/processcontrol/).
6. I.R. Garipov, I.V. Mashkina / The analysis of the problems of supporting information security in industrial control systems// Department of Computer Science and Robotics, Department of Computer Science and Robotics, Ufa State Aviation Technical University, Ufa, Russia /Page 28-32.
7. Кузнецов Петр Анатольевич/ Автоматизированная система анализа надежности перевозчиков опасной продукции // Защита состоится «20» декабря 2019 г. в __ часов на заседании диссертационного совета Д 212.249.05, созданного на базе Сибирского государственного университета науки и технологий имени академика М.Ф. Решетнева по адресу: 660037 г. Красноярск, проспект имени газеты «Красноярский рабочий», 31.
8. Lukov D.K. /AUTOMATED CONTROL SYSTEM OF TECHNOLOGICAL PROCESS (ACS TP)// INSTITUTE OF MICRO DEVICES AND CONTROL SYSTEMS, NATIONAL RESEARCH UNIVERSITY OF MOSCOW INSTITUTE OF ELECTRONIC TECHNOLOGY, ZELENOGRAD/ УДК 681.5.017 - ▪ European science № 2 (44) p19-24
9. Журавлев С. С., Рудометов С. В., Окольнишников В. В., Шакиров С. Р. Применение модельно-ориентированного проектирования к созданию АСУ ТП опасных промышленных объектов // Вестн. НГУ. Серия: Информационные технологии. 2018. Т. 16, № 4. С. 56–67.
10. Гордейчик Сергей Владимирович/ МИССИОЦЕНТРИЧЕСКИЙ ПОДХОД К КИБЕРБЕЗОПАСНОСТИ АСУ ТП// Гордейчик Сергей Владимирович, г. Москва/ Вопросы кибербезопасности №2(10)(56- 59) – 2015
11. С.В. Кирсанов/ Метод оценки угроз информационной безопасности АСУ ТП газовой отрасли// Кирсанов Сергей Владимирович Зам. нач. отд. информационной безопасности ООО «Газпром трансгаз Томск»// Доклады ТУСУРа, № 2 (28) стр (112-115), июнь 2013
12. Гарбук С.В, Правиков Д.И, Полянский А.В, Самарин И.В/ Обеспечение безопасности информации АСУ ТП с использованием метода превентивной защиты//Вопросы кибербезопасности. 2019. №3(31) (63-71)

УДК 004.056

Р. А. ИСЛАМОВ
m1bo@mail.ru
Науч. руководитель – канд. техн. наук, доц. В. Е. КЛАДОВ

Уфимский государственный авиационный технический университет

КРИПТОДЖЕКИНГ

Аннотация. Задачи данной статьи акцентировать внимание на метод атаки на криптокошельки пользователей – Криптоджекинг. Рассмотреть принципы и характерные черты данной атаки, а так же рекомендации по обнаружению и предотвращению заражением зловредным программным обеспечением.
***Ключевые слова*:** криптография; хакинг; криптоджекинг; киберпреступник.

Криптоджекинг – это вредоносный криптомайнинг, который происходит, когда киберпреступники взламывают как рабочие, так и персональные компьютеры, ноутбуки и мобильные устройства для установки программного обеспечения. Это программное обеспечение использует мощность и ресурсы компьютера для добычи криптовалют или кражи криптовалютных кошельков, принадлежащих ничего не подозревающим жертвам. Код прост в развертывании, выполняется в фоновом режиме и его трудно обнаружить.

С помощью всего нескольких строк кода хакеры могут захватить ресурсы любого компьютера и оставить ничего не подозревающих жертв с более медленным временем отклика компьютера, увеличением использования процессора, перегревом компьютерных устройств и более высокими счетами за электроэнергию. Хакеры используют эти ресурсы, чтобы украсть криптовалюту из других цифровых кошельков и позволить угнанным компьютерам выполнять работу, чтобы они могли добывать ценные монеты.

Основная идея криптоджекинга заключается в том, что хакеры используют рабочие, персональные компьютеры и ресурсы устройств для выполнения своей работы по майнингу за них. Киберпреступники выкачивают валюту, которую они либо зарабатывают, либо крадут в свой собственный цифровой кошелек, используя эти захваченные компьютеры. Эти захваченные компьютеры

скомпрометированы замедлением работы процессора и использованием большего количества электроэнергии для обработки. Криптоджекинг стал серьезной глобальной проблемой, когда киберпреступники получают несанкционированный доступ к компьютерным системам, чтобы заработать деньги с минимальным риском и усилиями. Криптоджекинг находится на подъеме, и хакеры придумывают новые способы кражи компьютерных ресурсов и добычи криптовалют.

Криптоджекинг впервые появился на свет в сентябре 2017 года, когда биткоин был на пике. Код, опубликованный организацией Coinhive на их веб-сайте, который закрылся в начале 2019 года, должен был стать инструментом майнинга для владельцев веб-сайтов, чтобы пассивно зарабатывать деньги — альтернатива показу рекламы на своем сайте для получения дохода. Вместо этого киберпреступники поняли, что они могут использовать этот код для встраивания своих собственных скриптов криптомайнинга. Они смогли использовать вычислительные ресурсы посетителей веб-сайта для майнинга криптовалюты Monero, которая с тех пор была вовлечена в другие расследования криптоджекинга.

Криптоджекинг становится все более популярным среди хакеров. Используемое программное обеспечение легче развернуть и труднее обнаружить, чем традиционные методы взлома. Готовые программы легко получить в Интернете, и как только компьютер заражен, код криптомайнинга работает за кулисами и может оставаться незамеченным в течение длительного периода времени.

При обнаружении криптоджекинга очень трудно отследить хакера. К этому времени киберпреступники свободно тратили свои незаконные криптовалютные доходы, оставляя предприятия с негативными последствиями, включая замедление работы сетей и финансовые последствия того, что их ИТ-команде приходится устранять компьютерные сбои.

Существует три основных метода, которые криптоджекеры используют для злонамеренного майнинга криптовалют: загрузка вредоносного ПО для выполнения скриптов криптомайнинга, захват ИТ-инфраструктуры и доступ к облачным сервисам.

При криптоджекинге на основе файлов вредоносное ПО загружается и запускает исполняемый файл, который распространяет сценарий криптомайнинга по всей ИТ-инфраструктуре.

Одним из наиболее распространенных способов возникновения криптоджекинга является использование вредоносных электронных писем. Отправляется электронное письмо, содержащее вложение или ссылку, которая выглядит законной. Когда пользователь нажимает на вложение или ссылку, выполняется код, который загружает скрипт криптомайнинга на компьютер. Этот скрипт работает в фоновом режиме без ведома пользователя.

Атаки криптоджекинга могут происходить непосредственно в веб-браузере, используя ИТ-инфраструктуру для добычи криптовалюты.

Хакеры создают скрипт криптомайнинга, используя язык программирования, а затем встраивают этот скрипт в многочисленные веб-сайты. Скрипт запускается автоматически, а код загружается на компьютер пользователя. Эти вредоносные скрипты могут быть встроены в рекламу и уязвимые и устаревшие плагины WordPress. Криптоджекинг также может возникнуть через атаку на цепочку поставок, где код криптомайнинга компрометирует библиотеки JavaScript.

Когда хакеры используют облачный криптоджекинг, они ищут в файлах организации и коде ключи API для доступа к своим облачным сервисам. Как только доступ получен, хакеры выкачивают неограниченные ресурсы процессора для криптомайнинга, что приводит к огромному увеличению затрат на учетную запись. Используя этот метод, хакеры могут значительно ускорить свои усилия по криптоджекингу для незаконной добычи валюты.

Как работает криптоджекинг? Хакеры компрометируют актив, встраивая код криптомайнинга с использованием одного из трех методов, указанных выше. После внедрения криптоджекеры рассчитывают на жертв для выполнения скрипта. Пользователи либо нажимают на вложение или ссылку, чтобы выполнить и запустить скрипт криптомайнинга, либо переходят на веб-сайт с зараженной рекламой. После выполнения скрипт криптомайнинга запускается в фоновом режиме, без ведома пользователя. Сценарий использует вычислительную мощность для решения сложных алгоритмов для добычи так называемого «блока». Эти блоки добавляются в блокчейн, технологию, которая хранит цифровую информацию о криптовалюте. Каждый раз, когда хакер добавляет новый блок в цепочку, он получает криптовалютные монеты. Без очень небольшой работы или риска эти злоумышленники могут получить вознаграждение в криптовалюте, которое они могут анонимно положить непосредственно в свои цифровые кошельки.

Как обнаружить криптоджекинг? Криптоджекинг может повлиять на всю информационную систему. Определить, какие из систем были скомпрометированы, может быть сложно. Код в скриптах криптомайнинга может легко избежать обнаружения, что означает, что ИТ-команда компании должны быть чрезвычайно бдительными.

Методы, которые можно использовать в обнаружении криптоджекинга:

− Снижение производительности

Одним из главных симптомов криптоджекинга является снижение производительности вычислительных устройств. Это включает в себя настольные компьютеры, ноутбуки, планшеты и мобильные устройства. Более медленные системы могут быть первым признаком криптомайнинга.

− Перегрев

Ресурсоемкий процесс криптоджекинга может привести к перегреву вычислительных устройств. Это может привести к повреждению компьютера или

сократить срок их службы. Также с перегревом устройств связаны вентиляторы, которые работают дольше, чем должны, в попытке охладить систему.

- Проверка загрузки ЦП

Необходимо отслеживать и анализировать использование центрального процессора (ЦП) для персональных компьютеров. Это можно сделать с помощью монитора активности или диспетчера задач. Если наблюдается увеличение использования ЦП, когда пользователи находятся на веб-сайте с небольшим количеством мультимедийного контента или вообще без него, это признак того, что скрипты криптомайнинга могут быть запущены.

- Мониторинг веб-сайтов

Киберпреступники ищут сайты, где они могут встраивать код криптомайнинга. Регулярно отслеживайте свои собственные веб-сайты на наличие изменений в веб-страницах или любых файлах на веб-сервере. Это раннее обнаружение может предотвратить компрометации ваших систем криптоджекингом.

- Сканирование на наличие вредоносных программ

Вредоносное ПО, созданное для криптомайнинга, использует системные ресурсы почти так же, как скрипты криптоджекинга. Вредоносное ПО может использоваться для заражения компьютеров, шифрования файлов и хранения их для выкупа Bitcoin. Использование программного обеспечения безопасности для поиска вредоносных программ может помочь идентифицировать эти вредоносные сценарии. Также можно использовать программное обеспечение, такое как PowerShell, для обнаружения атаки криптоджекинга.

Как предотвратить криптоджекинг.

Хотя трудно обнаружить, когда компьютерная система была скомпрометирована криптоджекингом, есть некоторые превентивные меры, которые можно предпринять для защиты компьютерных и сетевых систем и собственных криптоактивов:

- Использование расширений антикриптомайнинга

Скрипты криптоджекинга часто развертываются в веб-браузерах. Используйте расширения браузера для блокировки криптомайнеров в Интернете, например minerBlock, No Coin и Anti Miner.

− Использование блокировщиков рекламы

Веб-реклама является общим местом для внедрения скриптов криптоджекинга. Использование блокировщика рекламы может как обнаруживать, так и блокировать вредоносный код криптомайнинга.

− Отключить JavaScript

При просмотре в Интернете отключение JavaScript может предотвратить заражение компьютера кодом криптоджекинга. Нужно иметь в виду, что отключение JavaScript заблокирует многие функции, необходимые при просмотре.

СПИСОК ЛИТЕРАТУРЫ

1. Что такое криптоджекинг [электронный ресурс] URL: https://habr.com/ru/post/535932/
2. Энциклопедия Касперского «Криптоджекинг» [электронный ресурс] URL: https://encyclopedia.kaspersky.ru/glossary/cryptojacking/
3. Rob Sobers is a software engineer specializing in web security and is the co-author of the book Learn Ruby the Hard Way. Blog: What is Cryptojacking? [электронный ресурс] URL: https://www.varonis.com/blog/cryptojacking/

УДК 004.056.5

КАМБАМБИ ПАУЛУ МАРТИНШ

Уфимский государственный авиационный технический университет

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ЗДРАВООХРАНЕНИИ

Аннотация. В статье рассматриваются проблемы защиты информации, с которыми сталкиваются медицинские учреждения и методы решения существующие проблемы с обеспечением *информационной безопасности*.
Ключевые слова: *и*нформационная безопасность, защита информации данных; медучреждения; здравоохранения.

Клиники, медицинские центры, другие учреждения здравоохранения сталкиваются с большим количеством персональных данных как сотрудников, так и клиентов. Многие документы попадают в категорию врачебной тайны. Поэтому информационная безопасность в медицине переходит на новый уровень.

Медучреждения переходят на электронный документооборот, автоматизируется ведение электронного учета или медицинских карт пациентов. Нельзя сказать, что вопросом оптимизации регистратур или безопасности баз данных заинтересовались в системе здравоохранения только сейчас. Впервые хранить документацию, используя компьютер, предложил Николай Амосов (знаменитый советский хирург). С развитием информационных технологий ускорился и переход медучреждений на новый уровень обработки и хранения персональных данных.

Во время перехода от бумажных носителей к электронным становится очевидно, что не все медицинские организации готовы уделять должное внимание обеспечению ИБ, увеличивать расходы на это. А расходы на обеспечение информационной безопасности необходимы, нужно устанавливать и обслуживать системы защиты информации, обучать персонал, нанимать специалистов по информационной безопасности (ИБ).

Решить существующие проблемы с обеспечением ИБ должна программа ЕГИСЗ. В рамках программы предусмотрено обеспечение медучреждений тех-

никой, наличие всероссийского центра обработки информации, создание норм электронного документооборота между медицинскими организациями. Например, положения ЕГИСЗ регламентируют, какая именно информация из сервиса может быть предоставлена и кому — это должно сократить частоту утечек данных.

«Универсального метода, который обеспечит 100% защиту информации, не существует. Для того чтобы обезопасить информационную систему, обычно используется комплекс методов и программ, создаются регламенты по работе с данными для персонала — и чем продуманнее эти меры, тем выше вероятность сохранения данных в неприкосновенности»

Методы защиты информации

Обеспечение безопасности медицинской информации законодательно регламентировано на федеральном уровне. Для защиты сведений применяют следующие методы:

– организационно-управленческие (обозначение рамок и условий работы ресурсов, регламентация системы взаимодействия между пользователями и администратором сети);

– правовые (ответственность за нарушение правил);

– технические (программное и аппаратное обеспечение, которое защищает от несанкционированного доступа и обеспечивает авторизацию пользователей).

В РФ создают Единую государственную информационную систему в сфере здравоохранения (ЕГИСЗ). Согласно проекту ЕГИСЗ, сейчас выполняются следующие работы:

– создаются региональные программы модернизации здравоохранения;

– медучреждения оснащают телекоммуникационным и компьютерным оборудованием, а также средствами информационной безопасности;

– вводятся стандарты информационного обмена в пределах системы;

– создается федеральный центр обработки данных.

Выводы

Медицинские организации, прежде всего их ИТ-отделы, должны внедрить комплексные высокоэффективные меры цифровой безопасности, которые позволят должным образом управлять данными и защищать их — не только для галочки (лишь бы умиротворить регуляторов) или из страха столкнуться со штрафами и репутационными издержками, но и для того, чтобы пациенты начали осознавать пользу обмена информацией в медицине, будучи уверенными в том, что их данные надежно защищены.

Одна из величайших возможностей XXI века — возможность безопасно пользоваться преимуществами технологической революции, которая уже изменила наше общество. Это поможет решить непростые задачи по улучшению медицинского обслуживания для всех.

СПИСОК ЛИТЕРАТУРЫ

1. Федеральный Закон от 27.07.2006 г. № 152-ФЗ «О персональных данных» (далее – ФЗ «О персональных данных»), устанавливающий основные принципы и условия обработки ПДн, права, обязанности и ответственность участников отношений, связанных с обработкой ПДн.
2. «Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденное Постановлением Правительства РФ от 17.11.2007 г. № 781
3. «Порядок проведения классификации информационных систем персональных данных», утвержденный совместным Приказом ФСТЭК России № 55, ФСБ России № 86 и Мининформсвязи РФ № 20 от 13.02.2008 г.
4. «Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», утвержденное Постановлением Правительства РФ от 15.09.2008 г. № 687
5. «Требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных», утвержденные Постановлением Правительства РФ от 06.07.2008 г. № 512

УДК 004.021

В. Б. КОСТЕРОВ
zalaman42@ya.ru
Науч. руководов. – канд. техн. наук, доц. Т. А. ИВАНОВА

Уфимский государственный авиационный технический университет

СПОСОБЫ АУТЕНТИФИКАЦИИ ПО ПАРОЛЮ В ВЕБ-ПРИЛОЖЕНИЯХ

Аннотация. В данной статье рассматриваются основные способы аутентификации пользователей в веб-приложениях с использованием пары логин-пароль.
Ключевые слова: идентификация; аутентификация; авторизация; веб-приложения.

На сегодняшний день интернет-технологии встречаются повсеместно, и создаются множество сервисов, которые связывают человека с его активностью на сервисе. Из-за этого проблема безопасной аутентификации становится как никогда актуальной.

3 основных понятия:

1) Идентификация — это заявление о том, кем является пользователь.

2) Аутентификация — предоставление доказательств, что пользователь на самом деле есть тот, кем идентифицировался (от слова “authentic” — истинный, подлинный).

3) Авторизация — проверка, что пользователю разрешен доступ к запрашиваемому ресурсу.

В сфере веб-приложений идентификацией является предоставление пользователем логина, адреса электронной почты, номера учетной записи или телефона, и т.д. Под аутентификацией подразумевается проверка, что пользователь знает пароль от этого аккаунта, имеет доступ к привязанному номеру телефона или адресу электронной почты и т.д..

Первый тип аутентификации – по паролю. Этот метод основывается на том, что пользователь предоставляет системе логин и пароль, заданный им на стадии регистрации. Рассмотрим некоторые стандартные протоколы аутентификации по паролю.

HTTP authentification – очень старый протокол, описанный в стандартах HTTP 1.0/1.1. Применительно к веб-сайтам работает следующим образом:

1) Сервер, при обращении неавторизованного клиента к защищенному ресурсу, отсылает HTTP статус “401 Unauthorized” и добавляет заголовок “WWW-Authenticate” с указанием схемы и параметров аутентификации.

2) Браузер, при получении такого ответа, автоматически показывает диалог ввода username и password. Пользователь вводит детали своей учетной записи.

3) Во всех последующих запросах к этому веб-сайту браузер автоматически добавляет HTTP заголовок “Authorization”, в котором передаются данные пользователя для аутентификации сервером.

4) Сервер аутентифицирует пользователя по данным из этого заголовка. Решение о предоставлении доступа (авторизация) производится отдельно на основании роли пользователя, ACL или других данных учетной записи.

Т.к. протокол существует длительное время и является частью стандарта HTTP, его поддержка имеется в большом количестве браузеров и веб-серверов. Существует несколько схем такой аутентификации, различных по уровню безопасности:

1. Basic — наиболее простая схема, при которой username и password пользователя передаются в заголовке Authorization в незашифрованном виде (base64-encoded). Однако при использовании HTTPS (HTTP over SSL) протокола, является относительно безопасной.

2. Digest — challenge-response-схема, при которой сервер посылает уникальное значение nonce, а браузер передает MD5 хэш пароля пользователя, вычисленный с использованием указанного nonce. Более безопасная альтернатива Basic схемы при незащищенных соединениях, но подвержена man-in-the-middle attacks (с заменой схемы на basic). Кроме того, использование этой схемы не позволяет применить современные хэш-функции для хранения паролей пользователей на сервере.

3. NTLM (известная как Windows authentication) — также основана на challenge-response подходе, при котором пароль не передается в чистом виде. Эта схема не является стандартом HTTP, но поддерживается большинством браузеров и веб-серверов. Преимущественно используется для аутентификации пользователей Windows Active Directory в веб-приложениях. Уязвима к pass-the-hash-атакам.

4. Negotiate — еще одна схема из семейства Windows authentication, которая позволяет клиенту выбрать между NTLM и Kerberos аутентификацией. Kerberos — более безопасный протокол, основанный на принципе Single Sign-On. Однако он может функционировать, только если и клиент, и сервер находятся в зоне intranet и являются частью домена Windows.

В отличие от других методов аутентификации, у HTTP-аутентификации нет возможности выйти из веб-приложения. Выход можно осуществить только закрыв все окна браузера

Forms authentication - для этого протокола нет определенного стандарта, поэтому все его реализации специфичны для конкретных систем, а точнее, для модулей аутентификации фреймворков разработки.

Схема работы этого протокола заключается в следующем: в веб-приложении создается HTML-форма, в которую пользователь вводит свои данные. После ввода данных браузер отправляет на сервер эту форму через POST-запрос по протоколу HTTP(S). В случае успеха, веб-приложение создает токен сессии (session token), который затем сохраняется в куки браузера. При следующих запросах браузер автоматически передаст токен на сервер и приложение будет знать, что это тот же пользователь, который ранее успешно прошел аутентификацию.

Приложение может создать session token двумя способами:

1. Как идентификатор аутентифицированной сессии пользователя, которая хранится в памяти сервера или в базе данных. Сессия должна содержать

всю необходимую информацию о пользователе для возможности авторизации его запросов.

2. Как зашифрованный и/или подписанный объект, содержащий данные о пользователе, а также период действия. Этот подход позволяет реализовать stateless-архитектуру сервера, однако требует механизма обновления сессионного токена по истечении срока действия. Несколько стандартных форматов таких токенов рассматриваются в секции «Аутентификация по токенам».

Несмотря на то, что все действия по протоколу «Forms authentication» можно проводить и по незащищенному HTTP-протоколу, это не рекомендуется, так как наличие у злоумышленника токена сессии равносильно наличию у него логина и пароля, поэтому рекомендуется использовать защищенный протокол HTTPS.

Два протокола, описанных выше, успешно используются для аутентификации пользователей на веб-сайтах. Но при разработке клиент-серверных приложений с использованием веб-сервисов (например, iOS или Android), наряду с HTTP аутентификацией, часто применяются нестандартные протоколы, в которых данные для аутентификации передаются в других частях запроса.

Существует всего несколько мест, где можно передать username и password в HTTP запросах:

1. URL query — считается небезопасным вариантом, т. к. строки URL могут запоминаться браузерами, прокси и веб-серверами.

2. Request body — безопасный вариант, но он применим только для запросов, содержащих тело сообщения (такие как POST, PUT, PATCH).

3. HTTP header —оптимальный вариант, при этом могут использоваться и стандартный заголовок Authorization (например, с Basic-схемой), и другие произвольные заголовки.

Аутентификации по паролю считается не очень надежным способом, в основном, из-за человеческого фактора. Пользователи зачастую используют

слабые пароли, которые легко запоминаются и уязвимы к подбору путем полного перебора или перебора по словарю и используют один пароль повсеместно. Из-за этого при утечке пароля, скомпрометированными оказываются все учетные записи пользователя. Если же принудительно требовать от пользователей составления сильных, трудно запоминаемых паролей, содержащих большое количество символов в, то эти пароли зачастую хранятся с нарушением мер информационной безопасности (в открытом виде в текстовых файлах на компьютерах, на бумажках на столе и т.д.). Однако, и сами веб-приложения могут содержать уязвимости в реализации аутентификации по паролю, которые уменьшают безопасность аутентификации. Список самых распространенных уязвимостей:

1. Веб-приложение позволяет пользователям создавать простые пароли.
2. Веб-приложение не защищено от возможности перебора паролей (brute-force attacks).
3. Веб-приложение само генерирует и распространяет пароли пользователям, однако не требует смены пароля после первого входа (т.е. текущий пароль где-то записан).
4. Веб-приложение допускает передачу паролей по незащищенному HTTP-соединению, либо в строке URL.
5. Веб-приложение не использует безопасные хэш-функции для хранения паролей пользователей.
6. Веб-приложение не предоставляет пользователям возможность изменения пароля либо не нотифицирует пользователей об изменении их паролей.
7. Веб-приложение использует уязвимую функцию восстановления пароля, которую можно использовать для получения несанкционированного доступа к другим учетным записям.
8. Веб-приложение не требует повторной аутентификации пользователя для важных действий: смена пароля, изменения адреса доставки товаров и т. п.

9. Веб-приложение создает session tokens таким образом, что они могут быть подобраны или предсказаны для других пользователей.

10. Веб-приложение допускает передачу session tokens по незащищенному HTTP-соединению, либо в строке URL.

11. Веб-приложение уязвимо для session fixation-атак (т. е. не заменяет session token при переходе анонимной сессии пользователя в аутентифицированную).

12. Веб-приложение не устанавливает флаги HttpOnly и Secure для browser cookies, содержащих session tokens.

13. Веб-приложение не уничтожает сессии пользователя после короткого периода неактивности либо не предоставляет функцию выхода из аутентифицированной сессии.

СПИСОК ЛИТЕРАТУРЫ

1. Васильков, А.В. Безопасность и управление доступом в информационных системах: Учебное пособие / А.В. Васильков, И.А. Васильков. — М.: Форум, НИЦ ИНФРА-М, 2013. — 368 с.
2. Волков, В.С. Основы расчета систем автомобилей, обеспечивающих безопасность движения: Учебное пособие / В.С. Волков. — СПб.: Лань, 2015. — 144 с.
3. Дейтел, Х.М. Операционные системы. Т. 2. Распределенные системы, сети, безопасность / Х.М. Дейтел, П.Д. Дейтел, Д.Р. Чофнес; Пер. с англ. С.М. Молявко… — М.: БИНОМ, 2013. — 704 с.
4. Емельянов, С.В. Труды ИСА РАН: Системы управления и моделирование. Динамические системы. Управление рисками и безопасностью. Методы и модели в экономике. Прикладные а / С.В. Емельянов. — М.: Красанд, 2014. — 124 с.
5. Ерохин, В.В. Безопасность информационных систем: учеб пособие / В.В. Ерохин, Д.А. Погонышева, И.Г. Степченко. — М.: Флинта, 2016. — 184 с.
6. Запечников, С.В. Информационная безопасность открытых систем. В 2-х т. Т.1 — Угрозы, уязвимости, атаки и подходы к защите / С.В. Запечников, Н.Г Милославская. — М.: ГЛТ, 2006. — 536 с.
7. Максимов, С.Н. Экономическая безопасность России: системно-правовое исследование / С.Н. Максимов. — М.: МПСИ, МОДЭК, 2008. — 56 с.
8. Скопинцев, В.А. Качество электроэнергетических систем. Надежность, безопасность, экономичность, живучесть. 2-е изд., пер. и доп. / В.А. Скопинцев. — М.: Машиностроение, 2015. — 352 с.
9. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей: Учебное пособие / В.Ф. Шаньгин. — М.: ИД ФОРУМ, НИЦ ИНФРА-М, 2013. — 416 с.
10. Ярочкин, В.И. Безопасность банковских систем / В.И. Ярочкин. — М.: Ось-89, 2012. — 416 с

УДК 004.056.5

В. А. КУЛАГИН, Р. Р. ФАХРЕТДИНОВ
lander220138@gmail.com
Науч. руководов. – канд. техн. наук, доц. Р. Т. КУДРЯВЦЕВА

Уфимский государственный авиационный технический университет

ВАРИАНТЫ ОБХОДА DLP СИСТЕМ

***Аннотация*.** В данной статье рассмотрены варианты обхода DLP систем, методы борьбы с инцидентами.
***Ключевые слова*:** DLP; шифрование; кодирование; хищение информации.

DLP, Data Leak Prevention - технологии предотвращения утечек конфиденциальной информации из информационной системы во вне, а так же технические устройства (программные или программно-аппаратные) для такого предотвращения утечек.

DLP-системы строятся на анализе потоков данных, пересекающих периметр защищаемой информационной системы. При детектировании в этом потоке конфиденциальной информации срабатывает активная компонента системы, и передача сообщения (пакета, потока, сессии) блокируется.

Все DLP-системы можно разделить по ряду признаков на несколько основных классов. По способности блокирования информации, опознанной как конфиденциальная, выделяют системы с активным и пассивным контролем действий пользователя.

Первые умеют блокировать передаваемую информацию, вторые, соответственно, такой способностью не обладают. Первые системы гораздо лучше борются со случайными утечками данных, но при этом способны допустить случайную остановку бизнес-процессов организации, вторые же безопасны для бизнес-процессов, но подходят только для борьбы с систематическими утечками.

Еще одна классификация DLP-систем проводится по их сетевой архитектуре. Шлюзовые DLP работают на промежуточных серверах, в то время как хостовые используют агенты, работающие непосредственно на рабочих станциях

сотрудников. Сегодня наиболее распространенным вариантом является совместное использование шлюзовых и хостовых компонентов.

1. Отправка после окончания рабочего дня

Самое простое и банальное, что может получиться это просто отправить письмо на нужный адрес электронной почты после окончания рабочего дня. Данный метод успешен в случае, если система настроена на перехват почтовых сообщений, например, с 9-00 до 18-00 по рабочим дням и их блокировку в указанное время. Это связано с тем, что безопасники, которые смогут в случае чего разблокировать застрявшее письмо работают по трудовому договору в те же часы, что и Вы, поэтому после окончания рабочего дня они отключают систему или она останавливается автоматически. Вы можете проверить актуальна ли эта настройка, отправив пару безобидных сообщений после 18-00 и посмотреть дойдут ли сразу сообщения, которые, например не доходили сразу в течении рабочего дня. *Не самый лучший вариант*, так как независимо от результата отправки в системе останется след того, что Вы отправили, и в случае грамотного мониторинга системы безопасниками они увидят Вашу отправку.

2. Удаление слов маячков

Этот метод предполагает настройку DLP на поиск по ключевым словам, т.е. в отправленном документе он ищет совпадения по словарю. В случае мониторинга откатов такой словарь может содержать следующую группу слов: бабки, кэш, наличка и т.д. В случае же предотвращения утечек конфиденциальной информации данный словарь может содержать следующий словарный набор: коммерческая тайна, секрет фирмы, конфиденциально, ДСП, персональные данные, снилс, доверенность, паспорт, серия номер и т.д. Метод заключается в удалении таких слов, которые явно будут присутствовать в конфиденциальном документе и идентифицировать его к закрытой информации. Просмотрите документ, который необходимо отправить, на наличие таких слов и удалите. Метод также не самый лучший так как конкретный набор слов, содержащийся в словаре, Вам никто никогда не скажет.

3. Архив с паролем

Данный метод заключается в шифровании документа в стандартном *.rar архиве и направлении на электронную почту. Сразу можно отметить, что архив под паролем сразу вызывает подозрения и во многих системах блокируется, и даже расшифровывается. Чтобы максимально обезопасить себя необходимо:

а) При установке пароля на архив поставить галочку на значении «шифровать имена файлов». Это необходимо для того, чтобы имена файлов в архиве были не видны до открытия архива паролем.

б) При выборе пароля стоит обратить внимание на его длину и сложность. Это необходимо для предотвращения перебора по словарю, если такой используется в системе. Необходимо использовать минимум 10 символов, содержащих буквы строчного и прописного регистров, специальные символы, пробелы, цифры. Например, если пароль будет таким $Op123KLM!987@. Прежде чем набирать его в поле ввода, посмотрите часть «в».

в) *Самое главное правильно ввести пароль в поле ввода* в архиваторе. Дело в том, что на агенты, установленные на АРМ’ах работников, может содержаться функционал клавиатурного шпиона, записывающий все Ваши действия (нажатия клавиш) на клавиатуре. Стоит отметить, что запись ввода клавиш привязана к определенному процессу, где осуществляется набор (word, exel, winrar и т.д.).

Таких виртуальных клавиатур много в интернете. Стоит отметить, что Вы можете как угодно экспериментировать — набирать неправильный пароль, стирать, перемещать символы, при этом в системе слежения будет отображаться полная каша.

4. Кодировка онлайн

Для передачи документа проще всего использовать онлайн-сервисы обмена файлами, для примера мы рассмотрим https://transfiles.ru/

Заливаем наш файл «База агентов.docx» туда и получаем ссылку:

Теперь нам необходимо зашифровать ссылку и передать ее письмом. Для примера шифрования используем онлайн-сервис http://crypt-online.ru/crypts/aes/ с симметричным алгоритмом AES. В поле текста вставляем адрес нашей ссылки, выбираем размер ключа шифрования 128-256 бит. Вводим пароль, в данном случае «Мы любим ИБ», нажимаем кодировать и получаем шифрованный текст:

Копируем полученный результат и отправляем в электронном сообщении, сообщив пароль и *длину ключа* по альтернативному каналу связи (телефону). Получатель проделывает обратное преобразование, вводит шифрованный текст и пароль и получает ссылку.

4. Хитрости с форматом файла

Для начала архивируем текстовый файл архиватором (например, 7-zip) в формат «.rar» и получаем Doc.rar.

Теперь чтобы слепить их набираем в командной строке :

D:\shared>copy /b picture.Jpg+doc.rar rezult.jpg

И получаем файл «rezult.jpg» который содержит документ.

Защита от атак в представленных случаях:

1. Постоянно вести перехват информации пока пользователь в системе, в более продвинутых DLP-системах может работать запись микрофона в режиме ожидания.

2. В более продвинутых версиях DLP-системах аналитика строится на сложных поисковых политиках, а не на словах – маячках. То есть документ даже похожий по смыслу может быть обнаружен.

3. Не ограничиваться настройками по умолчанию. Во многих DLP-системах присутствует возможнось снимать видео, где можно с легкостью определить кто и когда создавал архив или документ.

Для своевременного контроля стоит установить дополнительные компоненты программного комплекса, например Searchinform. Также стоит отметить,

что регулярное обновление системы позволит установить гораздо больше компонентов для обеспечения безопасности.

Также стоит отметить и социальную инженерию. Тщательный выбор сотрудников по обеспечению безопасности может предотвратить утечку информации и обеспечить защиту системы на более высоком уровне.

Заключение

Недостаточная степень защищенности или вредоносное ПО помогают злоумышленникам проникать в информационные системы организации. Не зависимо от того, крадут ли информацию инсайдеры самостоятельно, или привлекают пособников, ясно, что простые способы управления доступом и межсетевой защиты не способны полностью обезопасить данные от несанкционированного доступа. Современные DLP-системы способны минимизировать хищение информации только при условии ее постоянной поддержки и обновлении баз знаний.

СПИСОК ЛИТЕРАТУРЫ

1. Доктрина информационной безопасности Российской Федерации
2. Отчет “DLP системы и человеческий фактор” от компании falcongaze [Электронный ресурс] / – Режим доступа: https://falcongaze.com/ru/pressroom/publications/research/dlp-sistemy-i-chelovecheskij-faktor.html
3. DLP-системы и их роль в защите от утечек конфиденциальной информации [Электронный ресурс] / – Режим доступа: https://cyberleninka.ru/article/n/dlp-sistemy-i-ih-rol-v-zaschite-ot-utechek-konfidentsialnoy-informatsii/viewer
4. ARIC White Label [Электронный ресурс] / – Режим доступа: https://www.featurespace.com/
5. Анализ современных методов шифрования [Электронный ресурс] / – Режим доступа: https://cyberleninka.ru/article/n/analiz-sovremennyh-metodov-shifrovaniya/viewer

УДК 004.056

Д. З. КУТЛЫЕВ, А. В. ШМАНИНА
Tonyhawk340@gmail.com
Науч. руководв. – канд. техн. наук, доц. А. М. ВУЛЬФИН

Уфимский государственный авиационный технический университет

ИСПОЛЬЗОВАНИЕ АЛГОРИТМОВ МАШИННОГО ОБУЧЕНИЯ ДЛЯ ЗАЩИТЫ ОТ URL-ФИШИНГА

Аннотация. Фишинг – легчайший способ получения личной информации о ничего не подозревающих пользователях. Ввиду популярности данного способа среди злоумышленников, обнаружение фишинга становится популярным направлением для исследований, направленных на противодействие реализации подобных атак. В данной статье рассматривается один из видов фишинга – URL фишинг, а также алгоритмы машинного обучения, используемые для противодействия атаке.
Клевые слова: фишинг; машинное обучение; URL-фишинг; кибербезопасность; глубокое обучение; алгоритмы машинного обучения.

Введение

Фишинг является атакой, нацеленной в первую очередь на неопытных пользователей. Одними из главных причин, по которым пользователи становятся жертвами злоумышленников посредством фишинга, являются – недостаточные знания о маркерах безопасности злоумышленники могут подделывать и маркеры), отсутствие внимания к URL сайта или же невнимательность относительно аномального поведения панели инструментов сайта [1]. Фишинг впервые был использован в 1996 году для кражи данных финансовой системы America Online, что дало злоумышленникам доступ к данным пользователей [2]. Фишинг является большой проблемой как для обычных пользователей, так и для корпоративных сетей. URL – фишинг является одним из самых распространенных видов, для противодействия которому необходимо использование машинного обучения. В конце статьи были рассмотрены алгоритмы машинного обучения для противодействия URL – фишингу.

Примеры инцидентов

Secure list сообщил о фишинг-атаке на добровольческую гуманитарную компанию, запущенной в Венесуэле в 2019 году. Ввиду данной кампании, был

создан веб-сайт, на котором добровольцы могли зарегистрироваться для участия в гуманитарной акции, а сайт требовал при регистрации от них указать имя, удостоверение личности, номер мобильного телефона, домашний адрес и многое другое. Злоумышленник создал практически идентичный сайт с похожим доменом. Хакер создал поддельный домен, используя IP-адрес легитимного сайта, что приводило к тому, что каждый раз как пользователь вводил данные, они фильтровались на поддельный сайт, что привело к краже данных тысяч добровольцев.

Следующим примером от специалиста из Великобритании Бена Ловджоя является демонстрация возможности перехода по ссылке из электронных писем на поддельный веб-сайт, у которого в адресной строке браузера на первый взгляд написан правильный URL, но на самом деле будут использованы символы, похожие на законное доменное имя.

Выше были перечислены примеры использования URL-фишинга, которыми пользуются злоумышленники для кражи личных данных, что даст пользователю возможность себя обезопасить. Но довольно часто ввиду разных факторов можно и не заметить ошибку в адресе сайта или то, что полученное письмо на самом деле поддельное. Фишинг данного вида является большой угрозой для обычных пользователей, которые могут не заметить тех уловок, что используются злоумышленниками для кражи личных данных пользователей. Далее будет рассмотрен детально метод URL-фишинга, а также, используемые в машинном обучении алгоритмы для защиты от URL-фишинга.

Фишинг на основе подмены URL

Фишинг на основе подмены адреса URL происходит искажением, а также добавлением специальных символов или слов в саму ссылку. Киберпреступник может использовать:

1. Секретные символы или слова, предназначенные для перенаправления;
2. Слова, написанные с орфографическими ошибками;

3. Сокращенные адреса URL;

4. Специальные файлы, встраиваемые в ссылку.

Таким образом, обфускацию URL-адреса можно провести различными способами [3].

Одним из примеров может служить смешивание с другими доменами. В адрес добавляется дополнительный домен, который перенаправит потенциальную жертву на нежелательный сайт. Пример фальшивого адреса может быть таким: http://triada1.ru/4221/www.example.com/8800555.

Служба сокращений URL-адресов активно используется в качестве фишинговой атаки. Существует несколько поставщиков услуг, которые могут использоваться для обфускации целевого URL, например, http://tinyurl.com. http://bitly.com, http://goo.gl. Злоумышленник отправляет сокращенный URL-адрес http://bit.ly/Nft1P5 по электронной почте, где содержимое убеждает пользователя перейти по этой ссылке.

Следующий тип, который можно выделить – использование доменов с опечатками. Это наиболее распространенный метод, используемый злоумышленниками. Например, подлинный банк зарегистрировал доменное имя сайта транзакций клиентов http://www.pay.examplebank.ru, в то время, как киберпреступник исказил название: http://www.pay.examplebanks.ru.

Не менее известный метод записи IP-адресов в шестнадцатеричной и восьмеричной системе счисления также используется мошенниками, где они могут использовать IP-адрес как часть URL, чтобы скрыть имя хоста или скрыть пункт назначения от пользователя. В результате ссылка принимает вид: http://173.193.130.8/http://example.com.

Обнаружение фишинговый сайтов

Далее будут перечислены алгоритмы машинного обучения, наиболее часто используемые исследователями в литературе по обнаружению фишинговых сайтов на основе подмены URL-адреса.

Метод опорных векторов

Метод опорных векторов (SVM) – типичный, но мощный алгоритм в технологии машинного обучения. Основная идея SVM заключается в рисовании гиперплоскостей для разделения классов. Например, есть n объектов в наборе данных. Затем для каждых данных необходимо построить точку в n-мерном пространстве, где каждое значение признака является конкретной координатой. Алгоритм начинается с определения подмножества обучающего набора данных, известного как опорные векторы. Цель – эффективно разделить опорные векторы двух разных классов. В двухмерных пространствах SVM фокусируется на рисовании линии, чтобы достичь максимального расстояния от опорных векторов каждого класса и минимизировать неправильные вхождения с каждой стороны. Но рисование линейной гиперплоскости не подходит в случае пространства размерности, где n относительно больше. Для решения этой проблемы вектор SVM использует ядерный метод, который преобразует пространство более низкой размерности в пространство более высокой размерности.

Сверточная нейронная сеть

Сверточная нейронная сеть (CNN) — это широко используемый метод классификации изображений. CNN может использоваться для обнаружения фишинговых URL-адресов, поскольку она включает обнаружение с помощью некоторых ключевых токенов. Эта задача выполняется путем работы с встраиваемыми уровнями символов. Например, моделируются URL-адреса на уровне символов и формируется пространство для встраивания на уровне символов, за которым следует извлечение признаков с использованием сверточного слоя. Сети CNN содержат слой свертки, уровень пула и полностью подключенную сеть с функцией нелинейной активации. Когда входные данные являются текстовыми, сеть CNN состоит из сверточного 1-го слоя, пульного 1-го уровня и полностью подключенной сети с нелинейной функцией активации [6].

Случайный лес

Алгоритм случайного леса – один из самых мощных алгоритмов в технологии машинного обучения, основанный на концепции алгоритма дерева реше-

ний. Метод создает лес с количеством деревьев решений. Большое количество таких деревьев обеспечивает высокую точность обнаружения. Создание деревьев основано на методе бутстрэпа. В нем функции и образцы набора данных выбираются случайным образом с заменой для построения единого дерева. Среди случайно выбранных характеристик алгоритм выбирает лучший разделитель для классификации, как и алгоритм дерева решений. Алгоритм случайного леса также использует индекс Джини и методы сбора информации для поиска лучшего разделителя [4]. Этот процесс будет продолжаться до тех пор, пока случайный лес не создаст n деревьев. Каждое дерево в лесу предсказывает целевое значение, а затем алгоритм вычисляет голоса для каждой прогнозируемой цели. Наконец, алгоритм случайного леса рассматривает прогнозируемую цель с высоким числом голосов в качестве окончательного прогноза.

Наивный байесовский классификатор

Алгоритм классификации основан на применении теоремы Байеса, который также известен как вероятностный алгоритм. Этот алгоритм используется при классификации из-за его простоты как на этапе обучения, так и на этапе классификации. Еще одним преимуществом этого алгоритма является меньший объем данных, необходимых на этапе обучения, по сравнению с другими алгоритмами классификации, основанными на машинном обучении.

Одной из основных проблем обзора различных методов обнаружения фишинговых сайтов на основе подмены адреса URL — нехватка наборов данных. Хотя уже опубликовано много научных статей по данной теме, самыми полярными наборами остаются Alexa, DMOZ для подлинных сайтов и PhishTank, OpenPhish для фишинговых [5]. Кроме того, можно обнаружить, что большинство исследований сосредоточено на несбалансированных данных, в которых большинство классов составляют официальные сайты. Это приводит к смещению оценок, выдаваемых алгоритмами. Иными словами, результат является необъективным, хотя он имеет высокий уровень ложных срабатываний.

Заключение

В данной работе представлено краткое описание фишинга, примеры инцидентов и экспериментов специалистов, описание URL-фишинга и используемые для защиты алгоритмы машинного обучения.

СПИСОК ЛИТЕРАТУРЫ

1.Routhu Srinivasa Rao & Alwyn Roshan PaisNeural «Detection of phishing websites using an efficient feature-based machine learning framework» //Computing and Applications volume 31, pages 3851–3873(2019)
2.B. B. Gupta, Nalin A. G. Arachchilage & Kostas E. Psannis «Defending against phishing attacks: taxonomy of methods, current issues and future directions» //Telecommunication Systems volume 67, pages247–267(2018)
3. S. Marchal, J. Francois, R. State, T. Engel, “PhishStorm: detecting phishing with streaming analytics” // in IEEE Transactions on Network and Service Management, vol.11, no.4, pp.458-471, 2014.
4. Rishikesh Mahajan, Irfan Siddavatam Phishing Website Detection using Machine Learning Algorithms // International Journal of Computer Applications 181(23):45-47, 2018.
5. Eint Sandi Aung, Chaw Thet Zan, Hayato Yamana A Survey of URL-based Phishing Detection // Department of Computer Science and Communication Engineering, Graduate School of Fundamental Science and Engineering, Waseda University, Tokyo, 159-8555, 2019.
6. M. A. Adebowale, K. T. Lwin, M. A. Hossain Deep Learning with Convolutional Neural Network and Long Short-Term Memory for Phishing Detection // 13th International Conference on Software, Knowledge, Information Management and Applications Island of Ululhas, Maldives, 2019.

УДК 004.65

Н. В. КУЧКАРОВА
nailya_kuchkarov@mail.ru

Уфимский государственный авиационный технический университет

ИССЛЕДОВАНИЕ ВОЗМОЖНОСТИ ИСПОЛЬЗОВАНИЯ КЛАСТЕРНОГО АНАЛИЗА ДАННЫХ ПРИ ОЦЕНКЕ СЦЕНАРИЕВ РЕАЛИЗАЦИИ УГРОЗ БЕЗОПАСНОСТИ

Аннотация. Целью исследования является определение возможности эффективного использования методов кластеризации данных при оценке сценариев реализации угроз безопасности. В работе проведен анализ статистических исследований киберинцидентов в некоторых отраслях экономики. Дан обзор публикаций об использовании методов кластеризации и интеллектуального анализа текстов при решении прикладных задач, в т.ч. и в области информационной безопасности.
***Ключевые слова*:** информационная безопасность; кластеризация; интеллектуальный анализ текстов.

Активно развивающаяся сфера информационных технологий и переход на удаленный формат работы, вызванной пандемией коронавирусной инфекции в 2019–2020 годах спровоцировал высокую активность киберпреступников. По данным компании Positive Technologies [1] в 2020г. количество киберинцидентов выросло на 51% по сравнению с 2019, 70% атак носили целенаправленный характер. Количество атак на медицинские учреждения и промышленные предприятия выросло на 91 %! Реализация угроз в промышленной отрасли может повлечь за собой катастрофические последствия. Так, киберпреступники, атаковавшие систему канализации и водоснабжения Израиля, планировали изменить концентрацию хлора, подаваемого в питьевую воду города, что в случае успешной реализации атаки, вызвало бы массовое отравление населения города.

Одними из важнейших задач для специалистов по информационной безопасности являются: определение возможности реализации угроз и оценка масштабов последствий на объектах критической информационной инфраструктуры. Целью методики оценки угроз безопасности информации, опубликованной ФСТЭК России (далее Методика) 5 февраля 2021 года, является оценка актуальных угроз безопасности информации (УБИ) [2]. Для достижения этой цели предлагается решить шесть задач (рисунок 1).

Рис. 1. Задачи, решаемые в ходе оценки угроз безопасности

За исходными данными для решения поставленных задач предлагается обратиться к банку данных угроз (БДУ) ФСТЭК России, модели угроз безопасности информации, разработанной ФСТЭК России, различным базам данных, содержащих описания векторов атак такие как: CAPEC (Common Attack Pattern Enumeration and Classification) – словарь (классификатор) известных шаблонов атак , ATT&CK (Adversarial Tactics, Techniques & Common Knowledge - это общедоступная база знаний, разработанная и поддерживаемая корпорацией MITRE, содержащая структурированный набор тактик и техник, используемых злоумышленниками, OWASP (Open Web Application Security Project) - открытый проект обеспечения безопасности веб-приложений, STIX (Structured Threat Information eXpression) - язык и формат данных, используемый для обмена информацией о киберугрозах через протокол TAXII и др. В соответствии с Мето-

дикой: «При наличии хотя бы одного сценария угрозы безопасности информации такая угроза признается актуальной…». Для корректной оценки сценариев реализации угроз необходимо сопоставить угрозы тактикам, техникам и уязвимостям, которыми воспользуется злоумышленник для их реализации. Поскольку количество уязвимостей, описанных в БДУ ФСТЭК превышает, на момент публикации статьи, 35 тысячи, угроз – 220, а количество тактик и соответствующих им техник из Методики – свыше 150, то «ручное» сопоставление такого объема текстовых описаний представляется затруднительным. В предыдущих публикациях автора этой статьи (в соавторстве) [3,4] представлены возможности применения технологии интеллектуального анализа для сопоставления угроз и уязвимостей. Дальнейшее изучение описанной проблемы показало возможную эффективность применения методов кластеризации в задачах оценки сценариев реализации УБИ. Ниже будет дан обзор применения кластерного анализа данных при решении различных прикладных задач в том числе и в области информационной безопасности.

В статье [5] освещена проблема кластеризации текстовых документов, в данном случае научных статей, с использованием алгоритмов word2vec, paragraph2vec. В данной работе рассмотрены и экспериментально исследованы методы кластеризации текстовых документов. Каждый метод состоял из трех последовательных этапов: предварительная обработка текста; векторизация предобработанного текста; кластеризация векторов. Экспериментальное исследование показало, что лучшим методом (при условии оптимизации параметров с помощью внутренней меры эффективности) является k-means с векторизацией Paragraph Vectors для всех наборов данных кроме Krapivin. В работе [6] проводится сравнительный анализ методов кластеризации таких как: метод Custom Search Folders, LSA/LSI , STC, Single Link, K-means и др. Проведенный анализ позволил сделать вывод о том, что наилучшими является алгоритм STC поскольку обладает хорошим сочетанием скорости и точности, а также кластеры, полученные с помощью этого метода, имеют читаемое название и могут быть

использованы для описания рубрик. В обзоре методов кластеризации [7] описаны два типа алгоритмов кластеризации: с заранее определенным числом категорий и неизвестным числом категорий, а также предложена классификация методов кластеризации по различным признакам: по типу связей в получаемом разбиении (жесткие и нечеткие), по способу измерения расстояний между кластерами (иерархические и плоские). В статьях [8] предложен метод кластерного анализа пространственно-временной модели угроз (МУ) для распределенной автоматизированной системы управления процессом транспортировки нефтегазового сырья. Особенностью данных работ является исследование частных моделей угроз для различных подсистем распределенных АСУ, позволяющих снизить временные и стоимостные затраты на создание и модернизацию СЗИ. В работе [9] предлагается подход к проведению кластерного анализа угроз информационной безопасности, позволяющий получить группы сходных угроз и выявить возможность уменьшения ущерба от их реализации.

Дальнейшие исследования в области применения технологий кластерного анализа плохо структурированных текстовых данных выгладят перспективными. Предполагается, что данная технология позволит специалистам по информационной безопасности сократить трудозатраты на обработку данных, содержащих описания угроз и уязвимостей, ускорить время принятия решений, что позволит обеспечить более эффективную защиту информационных систем от киберугроз.

Заключение

В статье проведен анализ актуальных киберугроз. Описаны основные задачи, решаемые в ходе оценки угроз безопасности, предложенные в Методике. Проведен обзор публикаций, посвященный применению кластерного анализа данных при решении прикладных задач.

Автором статьи планируется провести дальнейшие исследования с целью разработки автоматизированной системы, сочетающей в себе технологии интеллектуального анализа текста и методов кластеризации для решения задачи

сопоставления угроз, уязвимостей, техник и соответствующих им тактик, с целью выявления актуальных угроз безопасности информационных систем.

Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 20-08-00668 А.

СПИСОК ЛИТЕРАТУРЫ

1. Актуальные киберугрозы: итоги 2020 года. Positive Technologies. [Электронный ресурс]. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2020/ (дата обращения 25.09.2021).
2. Методика оценки угроз безопасности информации. Методический документ ФСТЭК России [Электронный ресурс]. URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/2170-metodicheskij-dokument-utverzhden-fstek-rossii-5-fevralya-2021 (дата обращения 25.09.2021).
3. Васильев В.И., Вульфин А.М., Кучкарова Н.В. Система поддержки принятия решений при оценке актуальных угроз и уязвимостей на основе семантического анализа // Мавлютовские чтения : XIV Всероссийская молодежная научная конференция, 1-3 ноября 2020 г. С.120-131
4. Васильев В.И., Вульфин А.М., Кириллова А.Д., Кучкарова Н.В. Методbка оценки актуальных угроз и уязвимостей на основе технологий когнитивного моделирования и Text Mining // Системы управления, связи и безопасности. 2021. №3. С.110-134. DOI: 10:24412/2410-9916-2021-3-110-134.
5. Пархоменко П.А., Григорьев А.А., Астраханцев Н.А. Обзор и экспериментальное сравнение методов кластеризации текстов. Труды ИСП РАН, 2017 г., Том 29, вып. 2, С. 161-200.
6. Кириченко К.М, Герасимов М.Б. Обзор методов кластеризации текстовой информации. Диалог: Сборник трудов международной научной конференции. 2001. [Электронный ресурс]. URL: http://www.dialog-21.ru/digest/2001/articles/kirichenko// (дата обращения 25.09.2021).
7. Абакумов О. Использование кластеризации в Text Mining // Новые информационные технологии в автоматизированных системах. 2010. №13. С.128-129.
8. Аралбаев т.з., Абрамова Т.В., Гетьман М.А. Кластерный анализ как инструмент построения и исследования пространственно-временных моделей угроз // Материалы Всероссийской научно-методической конференции (с международным участием). 2020. С. 1401-1405.
9. Куринных Д.Ю., Айдинян А.Р., Цветкова О.Л. Подход к кластеризации угроз информационной безопасности предприятий // Инженерный вестник Дона, №1 (2018) [Электронный ресурс]. URL: ivdon.ru/ru/magazine/archive/n1y2018/4803 (дата обращения 25.09.2021).

УДК 004.056.53

ЛЫОНГ ХА ЧА МИ, А. Р. ТАХАУТДИНОВ, И. Н. РЕЗЯПОВ
lhtrmi0212@gmail.com, aidartahautdinov@gmail.com, rezyapov101100@gmail.com
Науч. руководов. – канд. тех. наук, доц. В. Е. КЛАДОВ

Уфимский государственный авиационный технический университет

ПРИМЕНЕНИЕ НЕЙРОННЫХ СЕТЕЙ ДЛЯ ОБНАРУЖЕНИЯ СЕТЕВЫХ АТАК

***Аннотация*.** В данной статье проводится анализ существующих методов применения искусственных нейронных сетей для обнаружения сетевых атак, приведены достоинства и недостатки применения нейронных сетей и принцип их работы, а также рассмотрены системы, построенные на базе нейронных сетей, для выявления аномальной активности в сети.
***Ключевые слова*:** нейронные сети; нейросети; атаки; обнаружение атак; системы обнаружения атак; сетевые атаки; интернет; угрозы.

Стремительное развитие компьютерных сетей и Интернета породило за собой множество различных способов атак на них, соответственно вопрос об методах обнаружения аномалий в сети как никогда актуален. Безопасность компьютерной сети прежде всего зависит от своевременного и точного обнаружения вторжения и различного рода атак.

Большинство подходов к выявлению вторжений в компьютерную сеть базируются на основе набора правил, входящих в экспертную систему. Системы на основе правил не обладают достаточной гибкостью, что является их существенным недостатком. Экспертные системы требуют частого обновления, в противном случае ослабляются способности системы защиты, а пользователи вводятся в заблуждение относительно защищенности сети. Подобные системы не способны обнаруживать сценарии атак в течение продолжительных периодов времени.[1]

Вследствие чего за последние годы были созданы методы для обнаружения атак, например, на базе нейронных сетей, либо же их совместного применения с экспертными системами. Нейросеть позволяет построить систему, способную к самообучению и обнаружению ранее неизвестных типов сетевых атак.

Нейронная сеть состоит из группы элементов обработки (нейроны), которые сильно связаны между собой синапсами и преобразует набор входов к набору предпочтительных выходов. [2] Синапс — это связь между двумя нейронами. У синапсов есть 1 параметр — вес. Благодаря ему, входная информация изменяется, когда передается от одного нейрона к другому. Более подробно на рисунке 1 изображено то, как передается информация в нейронах на примере смешивания цветов.

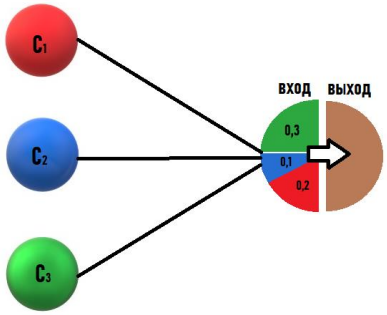


Рис. 1.

Основными преимуществами применения методов обнаружения атак, основанных на нейронных сетях, являются:

1) Гибкие алгоритмы, которые способны проанализировать данные из сети, даже при условии искажения и недостаточности информации. Это важные факторы, так как, например, информация очень часто подвергается случайным ошибкам системы.

2) Способность анализировать характеристики атак и идентифицировать аномальные активности, которые прежде не наблюдались в сети. Так, своевременное обнаружение подозрительной активности в сети позволяет отреагировать на атаку, прежде чем она нанесет непоправимый ущерб.

3) Высокая скорость обработки данных

Несмотря на вышеперечисленные преимущества применения методов обнаружения вторжения, построенные на нейронных сетях, они имеют и свои недостатки, такие как:

1) От правильного обучения нейронной системы зависит способность нейросети выявлять признаки атаки.

2) Требования к большим вычислительным мощностям.

3) Невозможность оперативного анализа больших объемов данных в условиях работы в качестве сетевого параметра обнаружения вторжений большой сети.

Существует множество различных методик применения нейронных сетей при обнаружении сетевых атак. Например южнокорейские исследователи предложили систему обнаружения вторжений с использованием искусственного интеллекта (AI) с использованием глубокой нейронной сети (DNN), которая была проанализирована и проверена с помощью набора данных KDD Cup 99.[4] Они использовали четыре скрытых слоя для построения нейронной сети, ReLU как функцию активации при пересылке и оптимизатор Adam при обучении обратному распространению. При использовании ReLU в качестве нелинейной функции активации в скрытом слое выходной слой состоит только из двух нейронов (атакующего и доброкачественного). Точность составила 93%.

Наиболее интересную методику предложили ученые из Вавилонского Университета в Ираке - Мухаммад Мейтем и доктор Гада Аль-Султани.[5] В своей работе для обнаружения пакетов вторжения в сеть они использовали глубокую нейронную сеть, а при ее обучении использовали ReLU в качестве нелинейной функции активации, оптимизатор Adam и кросс-энтропию в качестве функции потерь. Рассмотрим ее поподробнее

Данная система использует датасет KDD Cup 99. Этот датасет является достаточно большим - около 4,5 миллионов записей. Так же данный датасет имеет около 41 функции, которые могут быть классифицированы в три основные категории:

1.Функции TCP соединения

2.Функции содержимого

3.Функции траффика

Так же в составе KDD Cup 99 имеется 22 вида сетевых атак, которые в свою очередь могут быть подразделены на 4 группы:

1. Атака отказа в обслуживании (DoS)

2. Атака root пользователя.

3. Атака с удаленного на локальный (R2L).

4. Зондирование

В датасете KDD CUP 99 нет пропущенных значений, поэтому это чистый набор данных, который имеет числовые и текстовые значения, первые в свою очередь имеют большие числа, то есть имеют большое значение. Это задержит обучение и усложнит обработку. Также не стоит забывать о том, что в данном датасете есть и текстовые значения, которые не могут быть обработаны в операциях алгоритмов глубокой нейронной сети. Следовательно, набор данных должен быть предварительно обработан.

Предварительную обработку в этой модели можно разделить на два основных этапа: процесс нормализации и отображение текста. Ученые из Ирака определили нормализацию при помощи формулы 1, где Z - нормализация, x относится к значимости, μ - среднее значение выборки, σ - среднее отклонение выборки.

$$Z = \frac{x - \mu}{\sigma} \tag{1}$$

То есть, преобразование текстовых атрибутов в числовые значения было выполнено с использованием простого кодировщика унитарного кода с математическими уравнениями. Кодировщик показан на рисунке 2.

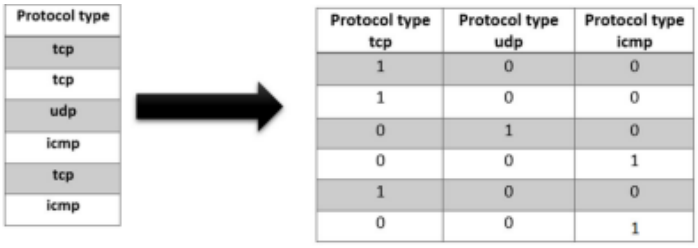


Рис. 2.

После выполнения данного действия, для KDD Cup 99 количество функций было увеличено с 41, до 125. Кроме увеличения функций в датасете ученые предложили свою модель глубокой нейронной сети для обнаружения сетевых атак состоящей из трехслойной топологии:

1.Вводный слой - инициализирует информацию для нейросети. Используемая система ввода основана на 125 узлах, которые представлены функциями предварительно обработанного датасета.

2.Скрытный слой - является промежуточным слоем между входным и выходными слоями, где выполняются все вычисления. Используемая система основана на двух скрытых слоях - первый скрытый слой с 50 нейронными узлами и второй скрытый слой с 30 нейронными слоями.

3. Выводящий слой - выводит результат работы. Все узлы входного слоя полностью связаны со всеми узлами следующего слоя и так далее. Более подробно эта модель представлена на рисунке 3.

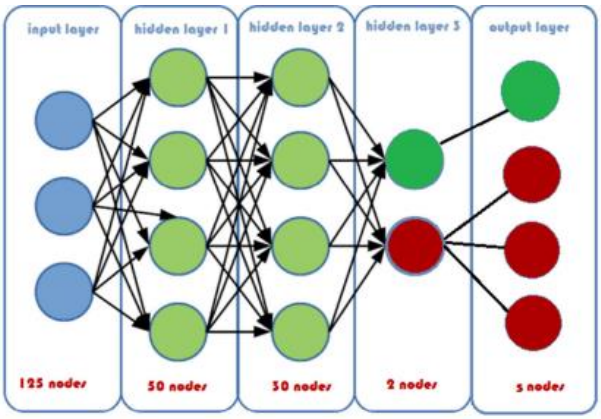


Рис. 3.

Кроме измененного датасета, авторы статей использовали прямое и обратное распространение.

Прямое распространение — это контролируемое обучение, состоящее из двух типов: однослойный персептрон и многослойный персептрон. Уравнение персептрона представлено в формуле 2

$$y = \sum_{i=1}^{n} XiWi + b \qquad (2)$$

В данной формуле n представляет собой количество узлов на слое, x является значениям этих узлов(значения набора данных), W относится к силе связи(вес), a b относится к смещению этих узлов. Результаты уравнения используются далее, в функциях активации. Данная модель использует две функции активации для разных слоев - функцию активации ReLU для Скрытого слоя и функцию активации Softmax для Выводящего слоя. Подробнее эти функции рассмотрены в формулах 3 и 4.

$$f(x) = 0 \text{ для } x \leq 0 \text{ и } f(x) = x \text{ для } x > 0 \quad (3)$$

$$\sigma(z)_i = \frac{e^{z_i}}{\sum_{k=1}^{k} e^{z_k}} \quad \textit{для } i=1,2,3 \ldots \ldots,k \quad (4)$$

Обратное распространение — это способ обучения глубокой нейросети с помощью модификации весов и смещения. В данной модели были использованы функции потерь кросс-энтропии. Функция потерь должна достичь оптимального значения параметра модели(веса и смещения). Оптимизатор — это способ получить наилучшее значение этого параметра. В данной модели был использован оптимизатор Adam.

Для оценки получившейся модели, Мухаммад Мейтем и доктор Гада Аль-Султани реализовали СОВ учитывая две классификации:

1)Бинарная классификация(Normal и Attack)

2)Мультиклассовая классификация (Normal, DoS, R2L,UM2R, и Probe).

Использовав такие оценки как Accuracy, Precision, Recall, F-score, Specificity, AUC для измерения бинарной классификации и Average Accuracy, Precision, Recall, F-score, Specificity для измерения мультиклассовой классификации, ученые получили матрицу, представленную на рисунке 4:

		Predicted		total
		Attacks	Normal	
actual	Attacks	TP	FN	TP+FN
	Normal	FP	TN	FP+TN
total		TP+FP	FN+TN	

Рис. 4.

После измерении бинарной классификации были получены результаты на рисунке 5:

		Predicted		total
		Attacks	Normal	
actual	Attacks	1 177 312	207	1 177 519
	Normal	108	291 903	292 011
total		1 177 420	292 110	

Рис. 5.

По итогу тестирования было выяснено, что предложенная модель из 292011 нормальных пакетов определила 291903 пакета как действительно нормальные, а на 108 пакетах получила ошибку. В случае атакующих же пакетов, из 1 177 519 пакетов 1 177 312 было обнаружено как атака, а 207 было определено как ошибка.

При измерении мультиклассовой классификации были получены следующие результаты:

		Predicted					total
		DOS	Probe	R2L	U2R	normal	
	DOS	1 165 359	1	0	0	13	1 165 373
	Probe	5	12293	1	0	100	12 399
actual	R2L	1	0	269	0	79	349
	U2R	0	0	0	0	9	9
	normal	42	7	50	0	291 391	291 490
total		1 165 407	12 301	320	0	291 592	

Рис. 6.

Как видно из данной таблицы, точность при определении DOS атак - 99.99%. В общем, точность мультиклассовой классификации составила 0.999789.

В данной статье были рассмотрены различные методы использования нейросетей для выявления сетевых атак, изучена модель, предложенная учеными из Вавилонского Университета. С использованием датасета KDD Cup 99 ученые добились 99.98% точности при определении атакующих пакетов трафика и 99.99% точности при определении атак типа DOS. Изучение иракской модели указывает на то, что проведение изучения работы нейросетей с СОВ на

основе бинарной и мультиклассовой классификаций является перспективным направлением для дальнейшего исследования и разработки.

СПИСОК ЛИТЕРАТУРЫ

1. Крыжановский Анатолий Владиславович Применение искусственных нейронных сетей в системах обнаружения атак // Доклады ТУСУР. 2008. №2-1 (18).
2. Aickelin U., Greensmith J., Twycross J. Immune system approaches to intrusion detection — a review // Proceedings ICARIS-2004, 3rd International Conference on Artificial Immune Systems, LNCS 3239. Pp. 316–329.
3. Кусакина Н. М. Методы анализа сетевого трафика как основа проектирования системы обнаружения сетевых атак // Труды XLI Междунар. науч.-прак. конф. “International Scientific Review of the Problems and Prospects of Modern Science and Education”. Boston: Problems of Science, 2018. С. 28—31.
4. Jin Kim, Nara Shin, Seung Yeon Jo and Sang Hyun Kim, "Method of Intrusion Detection using Deep Neural Network," IEEE, 2017.
5. Mohammed Maithem and Ghadaa A. Al-sultany “Network intrusion detection system using deep neural networks”, 2021 J. Phys.

УДК 004.056.5

А. Т. МАНСУРОВА, М. А. САЛМИН, Е. И. КОТОВ
mansurova.alisa@list.ru, kambr1g00@gmail.com, faf.fdfds@gmail.com
Науч. руководитель – доц. В. Е. КЛАДОВ

Уфимский государственный авиационный технический университет

ЗАЩИТА ИНФОРМАЦИИ С ПОМОЩЬЮ ТЕХНОЛОГИИ SRAM PUF НА БАЗЕ NXP SEMICONDUCTORS

Аннотация. Задачи данной статьи – рассмотреть процесс реализации технологии SRAM PUF, предназначенной для защиты информации технических средств, а так же рассмотреть преимущества и недостатки данной технологии.
Ключевые слова: SRAM PUF; физически неклонируемая функция; микросхемы; транзисторы; динамическая память.

В современном мире для защиты информации применяются различные технологические решения. Одно из них – PUF (физически неклонируемая функция). Технология базируется на особенностях характеристик каждой произведенной интегральной схемы (ИС), к примеру это могут быть уникальность транзисторов (их пороговых напряжений) внутри микросхемы, емкость конденсаторов, токопроводящая способность проводников и т.д., это связано с тем что в процессе производства ИС будут изготовлены с определенной погрешностью, пусть и совершенно незначительной, для работы самой ИС. [1]

В свою очередь технология PUF имеет различные способы реализации, одни из них – на базе SRAM. Статическая память с произвольным доступом (static random access memory) — это полупроводниковая оперативная память, в которой каждый двоичный или троичный разряд хранится в схеме с положительной обратной связью, позволяющей поддерживать состояние без регенерации, необходимой в динамической памяти. Тем не менее сохранять данные без перезаписи SRAM может, только пока есть питание, то есть SRAM остается энергозависимым типом памяти. При каждом включении устройства SRAM будет содержать неинициализированные значения. Эти первоначальные значения SRAM-ячеек будут случайными и уникальными для каждой микросхемы ввиду того, что транзисторы, из которых изготовлены эти ячейки, отличаются. [2]

При подачи питания ячейка принимает значение логического нуля или единицы. Совокупность этих ячеек формирует уникальное состояние памяти – SRAM Startup Data. При этом не все ячейки будут содержать одно и то же значение в зависимости от цикла, некоторые из них изменятся. Стабильность SRAM-ячейки при подаче питания обусловлена различием пороговых напряжений в ее «плечах». Чем меньше разность, тем большее влияние оказывает нестабильность таких показателей как: температура, питание, старение кремния. [3] Использовать такой отпечаток напрямую нельзя – необходимо обеспечить его воспроизводимость с помощью алгоритма коррекции ошибок. После пропускания зашумленного отпечатка через алгоритм, на выходе образуются воспроизводимый отпечаток Digital Fingerprint и вспомогательную информацию Helper Data.

Helper Data не содержит секретной информации, однако используется для того, чтобы восстанавливать точный отпечаток Digital Fingerprint из зашумленного отпечатка SRAM Startup Data. В процессе работы Digital Fingerpint остается в пределах PUF-блока и не сохраняется после выключения питания. Для его воспроизведения необходимо сохранить вспомогательную информацию (Helper Data). Таким образом, Digital Fingerprint может быть использован в качестве корневого ключа для защиты секретов – симметричных или асимметричных ключей и другой конфиденциальной информации. [2]

PUF-блок в контроллерах NXP Semiconductors реализован на основе IP-решения компании Intrinsic ID. На данный момент поддержка PUF-блока есть в контроллерах серий LPC5400 (Cortex-M4) и LPC5500 (Cortex-M33).

Существуют следующие основные методы SRAM PUF:

– Enroll – генерация кода активации (Activation Code);

– Start – воспроизведение отпечатка (Digital Fingerprint);

– SetKey – установка пользовательского ключа;

– GenerateKey – установка случайного пользовательского ключа;

– GetKey – получение пользовательского ключа.

Чтобы начать работать с SRAM PUF, необходимо выполнить команду Enroll. Эту операцию следует проделать единожды для каждого устройства. В результате выполнения Enroll мы получаем уникальный Digital Fingerprint и соответствующий ему Activation Code (Helper Data). [4]

Значение Digital Fingerprint не сохраняется и не покидает PUF-блок, а Activation Code можно сохранить в любую энергонезависимую память (NVM), т. к. он не содержит секрета. Digital Fingerprint представляет собой 256-битный ключ, а Activation Code – блок данных размером до 1192 байт (9536 бит).

При каждом вызове команды Enroll мы получаем другие значения Digital Fingerprint и Activation Code, поэтому при потере Activation Code невозможно восстановить оригинальный Digital Fingerprint, а следовательно, и все секреты, которые были защищены с помощью этого отпечатка. Поэтому существует возможность отключить команду Enroll с помощью специального Fuse (дополнительная настройка микроконтроллера).

Копирование Activation Code на другое устройство бессмысленно, так как малейшие изменения в SRAM Startup Data приведут к получению совершенно другого Digital Fingerprint, а следовательно, сведут на нет возможность прочитать ключи и данные, которые защищены оригинальным отпечатком.

После выполнения Enroll и получения Activation Code можно использовать SRAM PUF для защиты ключей и данных. Для этого необходимо сбросить питание в PUF, а затем вызвать команду Start.

Activation Code загружается в PUF, и на основе новых значений SRAM Startup Data с помощью алгоритма коррекции ошибок воспроизводится Digital Fingerprint. После этого можно использовать команды SetKey, GenerateKey и GetKey.

Команда SetKey выполняет преобразование User Key (пользовательского ключа / данных) в Key Code – безопасную последовательность, которую можно хранить где угодно. User Key может принимать значение от 64 бит до 4096 бит.

Перенос этой последовательности (Key Code) на другой микроконтроллер бессмыслен, так как Digital Fingerprint уникален.

Каждый Key Code имеет свой индекс. Key Code с индексом 0 после обратного преобразования будет недоступен из программной части. Он может быть напрямую определен для работы с AES-блоком, который можно использовать для защиты прошивки. Помимо этого имеется возможность генерации случайного ключа внутри PUF-блока с последующим преобразованием в Key Code. Метод GetKey выполняет обратное преобразование Key Code в пользовательские данные.

Помимо AES-блока, NXP Semiconductors предоставляет еще один симметричный алгоритм шифрования – PRINCE. Его особенность в том, что он очень быстрый и отлично подходит для того, чтобы разворачивать прошивку на лету. Это особенно актуально для серии LPC5400, в которой вообще нет энергонезависимой памяти внутри чипа. Эти контроллеры работают по принципу Execute-In-Place.

Поэтому у метода GetKey есть параметр KeySlot. Он позволяет определить, в какой из криптографических блоков (AES или PRINCE) будет отправлен ключ после обратного преобразования. [2]

На практике можно выделить три ключевые сферы применения SRAM PUF:

– персонализация устройств;

– безопасная загрузка;

– защита пользовательских ключей и данных.

При персонализации устройств выполняется подготовка PUF-блока посредством команды Enroll. Для этого подготавливается специальная прошивка – Enrollment Image. С ее помощью можно провести тестирование готового устройства, сгенерировать и защитить необходимые для работы ключи, а также составить базу аутентичных устройств. После этого происходит настройка

устройства на получение и работу с прошивкой, которая защищена уникальным для каждого устройства ключом.

Персонализация может проходить в доверенном и не доверенном сегменте. В доверенном сегменте с помощью штатных средств можно безопасно персонализировать устройства и подготовить их к работе. Но если работа происходит в недоверенном сегменте, то необходимо выстроить цепочку доверия с использованием асимметричного шифрования и отдельных модулей безопасности (Hardware Security Module, HSM). В таком случае возникает проблема проверки публичного ключа на подлинность. С целью предотвращения подмены ключа, его необходимо подписать доверенным сертификатом производителя. [5]

Для безопасной загрузки в контроллерах NXP Semiconductors есть поддержка Secure Boot. В NXP Semiconductors есть криптографические блоки AES и PRINCE, а Key Code с определенным индексом может быть сразу использован для работы с этими блоками по специальной шине.

Таким образом, разработчику достаточно сгенерировать и сохранить у себя симметричный ключ, закрыть прошивку этим ключом, а после этого обернуть ключ в Key Code с нулевым индексом. Тем самым разработчик запрещает PUF-блоку передавать явное представление ключа куда-либо, кроме криптографических блоков.

SRAM PUF может использоваться для защиты пользовательских ключей и данных во время работы устройства. Конфиденциальную информацию, которую необходимо сохранить, можно обернуть в Key Code, тем самым сделав его содержимое читаемым только на конкретном девайсе. То же самое касается и асимметричных ключей – мы можем хранить только публичный ключ, а приватный обернуть в Key Code, разворачивая его только в том случае, когда он требуется для работы криптографии. Для создания пар асимметричных ключей в NXP Semiconductors есть отдельный криптографический модуль – CASPER. Однако не стоит забывать, что максимальный размер User Key составляет всего 512 байт. [6]

Исходя из вышесказанного можно сделать вывод о том, что SRAM PUF по своей концепции является достаточно перспективной технологией для защиты ключей и данных. Однако в открытом доступе нет практического и задокументированного описание работы алгоритма коррекции ошибок и алгоритма получения Activation Code. Следовательно, нельзя быть уверенным в том, что данная технология и ее конкретная реализация безопасны и действительно работают так, как это описано в документах NXP Semiconductors и Intrinsic ID. То есть, приходится полагаться на безопасность через неясность (security through obscurity). Также у SRAM PUF есть свои недостатки. Срок жизни любого полупроводникового устройства ограничен, но сама технология накладывает дополнительные издержки. Нельзя исключать возможность криптографических атак, которые смогут пошатнуть стойкость SRAM PUF в будущем. А произведенные в не доверенном сегменте контроллеры должны проходить подготовительную стадию у производителя микросхем, что накладывает дополнительные издержки. Но в случае мелкосерийного производства у разработчика есть возможность выполнить персонализацию у себя.

СПИСОК ЛИТЕРАТУРЫ

1. Extend MCU Security Capabilities Beyond Trusted Execution with Hardware Crypto Acceleration and Protection [Электронный ресурс] URL: https://www.nxp.com/docs/en/white-paper/IOTSECWP.pdf
2. Защита секретов с помощью технологии SRAM PUF [Электронный ресурс] URL: https://habr.com/ru/company/ntc-vulkan/blog/563880/
3. White Paper - The reliability of SRAM PUF [Электронный ресурс] URL: https://www.intrinsic-id.com/wp-content/uploads/2017/08/White-Paper-The-reliability-of-SRAM-PUF.pdf
4. LPC55Sxx usage of the PUF and Hash Crypt to AES coding [Электронный ресурс] URL: https://www.nxp.com/docs/en/application-note/AN12324.pdf
5. Basics of SRAM PUF and how to deploy it for IoT security [Электронный ресурс] URL: https://www.embedded.com/basics-of-sram-puf-and-how-to-deploy-it-for-iot-security/
6. SRAM PUF Technology [Электронный ресурс] URL: https://www.intrinsic-id.com/sram-puf/

УДК 004.056

Е. В. МИХАЙЛОВА
katiana_2001@mail.ru
Науч. руководитель – канд. техн. наук, доц. А. М. ВУЛЬФИН

Уфимский государственный авиационный технический университет

АНАЛИЗ РЕКОМЕНДАЦИЙ КРЕДИТНО-ФИНАНСОВЫХ ОРГАНИЗАЦИЙ ПО ВЫЯВЛЕНИЮ МОШЕННИЧЕСКИХ ДЕЙСТВИЙ

***Аннотация*.** С учетом роста количества киберпреступлений и на фоне их низкой раскрываемости кредитно-финансовые организации стали выпускать разнообразные памятки и информационные блоки по кибербезопасности. В данной статье мы проанализировали их актуальность и составили иерархию с учетом полезности для пользователей разного уровня подготовленности к атакам мошенников.
***Ключевые слова*:** информационная безопасность; киберпреступность; банковские услуги; ДБО; фишинг; социальная инженерия; безопасность в сети.

Введение

На сегодняшний день в России очень активно действуют киберпреступники. Об этом заявил начальник главного организационно-аналитического управления Генпрокуратуры Андрей Некрасов в интервью ТАСС 24 мая 2021 года [1]. Он сообщил, что «за последние годы число преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, возросло до масштабов, позволяющих говорить о них как об угрозе национальной безопасности». Это тенденцию можно проследить, если обратиться к обзору отчетности об инцидентах информационной безопасности при переводе денежных средств за I и II кварталы 2019/2020 года Центрального Банка РФ [2]. В нем приведена статистка, говорящая о возрастании количества операций, проведенных без согласия клиента, при этом доля технологий социальной инженерии в действиях злоумышленников значительно возросла. В I квартале 2020 года объем операций без согласия клиента вырос на 38% по сравнению с аналогичным периодом 2019 года на фоне двукратного снижения общего объема операций с использованием электронного средства платежа. При этом согласно данным Генпрокуратуры, в России раскрывается меньше 25% киберпреступлений. Рассматривая сводные ста-

тистики Центробанка, можно сказать, что основной удар приходится именно на физические лица, нежели на юридические. Обосновывается это трудозатратностью организации атаки на какую-либо компанию. Поскольку такая схема требует оборудования, продуманности, большого количества усилий при том, что они могу не окупиться. А атака на физическое лицо реализуется намного проще с точки зрения экономических затрат.

Технологии социальной инженерии в действиях кибермошенников

Каждый человек сегодня имеет мобильный телефон с доступом к сети "Интернет", и большинство пользуется услугами интернет-банкинга, что значительно упрощает процесс перевода денег куда-либо. Этим и пользуются мошенники, применяя социальную инженерию и убеждая граждан самолично передать деньги злоумышленникам. Так, атаки с использованием вредоносного программного обеспечения в период с 2019 по 2020 год являются наиболее редкими, в то время как социальная инженерия занимает основную долю. Одной из наиболее вероятных причин такого роста атак — начало использования дистанционных способов оплаты товаров и услуг той частью населения, которая до введения ограничений в связи с пандемией COVID-19 приобретала и оплачивала их непосредственно в точках продаж. В силу отсутствия необходимого опыта противодействия злоумышленникам эта категория пользователей оказалась повышено уязвима к социальной инженерии.

Граждане были не готовы столкнуться с мошенниками напрямую, они не обладали достаточными знаниями, чтобы различить злоумышленников. Именно поэтому большинство кредитно-финансовых организаций стали размещать информацию о киберпреступниках, грамотном поведении в сети, а так же о наиболее распространенных способах мошенничества. Некоторые организации предоставили на своих официальных сайтах полную и понятную любому пользователю информацию, но другие ограничились памятками, содержащими ключевые данные. Поэтому цель данного исследования заключается в анализе и

классификации основных рекомендаций по выявлению мошеннических действий.

Классификация рекомендаций по выявлению кибермошенничества

Рассмотрим информацию о злоумышленниках, размещенную на официальных сайтах финансовых организаций, возглавляющих рейтинг российских банков по ключевым показателям деятельности, рассчитанный по методике сайта Banki.ru с использованием отчетности кредитных организаций РФ, публикуемой на сайте Банка России [3]. Все эти кредитно-финансовые организации на своих сайтах разместили информацию, посвященную кибербезопасности. Более того, они выделили под эти сведения минимум одну отдельную страницу, ссылку на которую большинство оставило на главной странице сайта. Подавляющее большинство представило информацию исключительно для частных лиц, хотя есть представители, которые сделали отдельные памятки и страницы специально для юридических лиц. Также на четвертом месте данного списка находится Национальный клиринговый центр, который тоже разместил на своем сайте советы по кибербезопасности. Он отличается своей спецификой и направленностью, однако общие подходы, которые буду рассматриваться далее, сохраняются и в этих рекомендациях.

Саму информацию можно разделить на несколько смысловых блоков, которые обозначим как «Кибербезопасность в повседневной жизни», «Поведение в сети «Интернет»» и «Атаки мошенников». В основном именно на такие тематические категории разделены большинство памяток. К «Кибербезопасности в повседневной жизни» можно отнести все действия, связанные с использованием банковских карт, банкоматов, а также хранение персональной информации. Вторая категория включает в себя использование мобильного приложения и сайта банка, получение сообщений на электронную почту, фишинг, покупки и продажи в интернете, в том числе CNP-операции (без присутствия карты). Последний смысловой блок подразумевает различные взаимодействия с мошенниками напрямую: звонки на мобильный телефон, СМС-сообщения, вредонос-

ные программы. Такая группировка позволяет собирать информацию в удобные разделы: например поведение мошенников при звонке или правила пользования банкоматом. Однако эффективность таких данных варьируются для пользователей с разным уровнем осведомленности в данной сфере. Это связано с тем, что разделение по смысловым блокам не подразумевает разную степень распространенности данных. Например, самая примитивная информация соседствует с такой, которую не все пользователи смогут понять. Поэтому разделим информацию на категории, которые показывают градацию эффективности рекомендаций для граждан с разными знаниями в этой сфере.

Первый уровень обозначим как базовый. Информация данной группы будет понятна всем. Она не требует какой-либо подготовки или обладания особыми знаниями. Все данные советы большинство людей выполняют интуитивно, основываясь на здравом смысле и внимательности. Такие советы могут быть полезны человеку, который только знакомится с миром банковских услуг, даже если он догадывался об этом подсознательно. В качестве примера можно привести следующие советы:

– Не сообщать никому пароли, ПИН-, CVV-коды и коды из СМС.

– ПИН необходимо запомнить или в случае, если это является затруднительным, хранить его отдельно от банковской карты в неявном виде, в месте недоступном для третьих лиц, в том числе родственников. Не хранить банковскую карту и ПИН в кошельке.

– Проверять реквизиты переводов и платежей, которые приходят в СМС от банка.

– Не оставлять карту без присмотра и не передавать ее никому.

– Прикрывать клавиатуру рукой во время введения ПИН-кода в банкомате.

– Если банкомат поврежден или находится в сомнительном месте, лучше перестраховаться и не пользоваться им.

Второй уровень – уровень настороженности. То есть данные советы заставляют человека задуматься о потенциальной враждебности вокруг себя. Вероятно, большинство людей, которые пользуются услугами дистанционного банковского обслуживания (ДБО) или длительное время активно используют банковские карты, знакомы с ними, однако иногда и они забывают их. Например:

– Не покупать ничего с общедоступных компьютеров или с использованием бесплатного Wi-fi.

– Использовать только официальные приложения банков в App Store, Google Play и Microsoft Store. Использовать только официальный сайт банка. Сохранить этот адрес в закладках браузера.

– Никому не сообщать пароли для входа в официальный сайт и пароль для входа в мобильное приложение. Даже близким и сотрудникам банка.

– Сохранять чеки после оплаты и картой, и наличными, если первоначально оплата по карте из-за сбоев не прошла.

– Не подключать уведомления об операциях на чужие телефоны, даже если об этом просят люди, которые представились сотрудниками банка.

Следующий уровень – продвинутый. Такие рекомендации можно отнести к применимым в повседневной жизни. Однако от базовых их отличает требование большей осведомленности пользователя, но и обеспечение более высокого уровня защиты данных. Для выполнения большинства таких рекомендаций необходимо умение пользоваться техническими устройствами на среднем уровне и повышенное внимание к мелочам. Однако начиная с данного разделы советы переходят на уровень защиты от мошенников. Примеры подобных рекомендаций:

– Использовать антивирус. Регулярно делать полную проверку компьютера программой-антивирусом. Установить автоматическое обновление антивирусных баз и операционной системы.

– Убедиться, что адресная строка начинается с префикса https:// . Это значит, что установлено защищенное соединение.

– Отключить в настройках iPhone голосовое управление Siri при заблокированном экране.

– Перед использованием банкомата осмотреть его внешний вид. Если обнаружено наличие каких–либо посторонних изделий, предметов, проводов, следов конструктивных изменений, воспользоваться другим банкоматом.

– Установить суточный лимит на сумму операций по банковской карте и одновременно подключить услугу оповещения о проведенных операциях (SMS-информирование или e-mail - информирование).

Последний раздел называется активная защита. Он содержит в себе самые действенные рекомендации по защите пользователей. Они требуют к себе больше внимательности и сосредоточенности, однако такие советы окажут наибольший эффект в борьбе с мошенничеством. Основные категории данного раздела:

– 3D-Secure. Подключение данной функции обеспечивает безопасность при совершении CNP-операций.

– Фишинговые сайты. Банки в основном раскрывают понятие фишинга при помощи иллюстрированных примеров, советов по распознаванию таких сайтов, объясняют схемы мошенничества и предоставляют ссылки на существующие копии официального сайта банка.

– Социальная инженерия. Это самый распространенный за последние годы метод воздействия на пользователей. Поэтому банки уделяют много времени на объяснение клиентам различных схем мошенников. Они объясняют, какими именами представляются мошенники и на какие человеческие качества и чувства давят во время звонков напрямую клиенту или посредствам СМС и электронных писем. Такая информация доносится и в формате перечисления основных предлогов для звонков, и рисованных историй, представляющих со-

бой ситуацию взаимодействия с мошенником, а так же описание таких случаев и грамотное поведение пользователей.

Если все эти советы суммировать, мы получим весьма подготовленного к встрече с мошенниками пользователя. Однако, к сожалению, данная информация собрана из разных памяток и информационных блоков, размещенных на сайтах семи банков. С одной стороны большинство организаций делают упор на базовую и интуитивную информацию, добавляя более углубленную в небольшом количестве или не особо акцентируя на ней. В то же время, так или иначе упоминание о фишинге и приемах социальной инженерии присутствует везде. В сегодняшних реалиях это наиболее актуальная информация. Поскольку основной упор мошенники делают именно на прямой контакт с жертвой, разные примеры схем мошенничества и наглядные иллюстрации разговоров со злоумышленниками становятся самыми необходимыми сведениями.

Базовые данные хоть и нельзя назвать особо эффективной информацией, но их присутствие в памятках является оправданным, поскольку в условиях пандемии и локдауна новым пользователям, не знакомым ранее с ДБО и использованием банковской карты на постоянной основе, будет полезно прочитать и усвоить пусть и довольно очевидные советы. К сожалению, более продвинутым клиентам может такая информация показаться неэффективной, и они не станут читать информационный блок до конца, пропуская важные сведения. В таком случае все зависит от подачи самой информации читателю, доступном языке изложения и формате кратких памяток или презентаций. А такой формат предоставления данных варьируется в зависимости от организации.

Заключение

Подводя итог, можно отметить, насколько за последние годы возросла актуальность задачи знакомства граждан с основами кибербезопасности. К довольно большому числу клиентов, использующих банковские карты и совершающих CNP-операции, прибавилось значительное количество новых пользователей, ранее с подобным не знакомых. В связи с чем действия кредитно-

финансовых организаций по размещению всевозможных памяток и информационных страниц о кибермошенничестве являются очень оперативными и верными. Самой эффективной и необходимой информацией можно назвать сведения о социальной инженерии и фишинге, установке антивирусных решений и подключении дополнительных средств проверки при платежах. Но стоит заметить, что и стандартная информация об использовании банкоматов и карт тоже присутствует не напрасно. Самыми слабыми местами остаются способы донесения и представления данных на сайтах, а также их количество, варьирующееся от банка к банку.

СПИСОК ЛИТЕРАТУРЫ

1. В Генпрокуратуре заявили, что киберпреступность стала представлять угрозу нацбезопасности // информационное агентство России ТАСС URL: https://tass.ru/obschestvo/11451173 (дата обращения: 25.08.2021).
2. Обзор отчетности об инцидентах информационной безопасности при переводе денежных средств // Центральный банк Российской Федерации URL: https://cbr.ru/analytics/ib/review_1q_2q_2020/ (дата обращения: 24.08.2021).
3. Рейтинги банков // banki.ru URL: https://www.banki.ru/banks/ratings/?source=submenu_banksratings (дата обращения: 27.06.2021).

УДК 004.056

Д. А. МИШНЕВ, Д. В. ЗОЛОТАРЕВ
danilzolotarev1980@gmail.com
Науч. руководв. – канд. тех. наук. доц. А. М. ВУЛЬФИН

Уфимский государственный авиационный технический университет

ВОЗМОЖНОСТИ XDR В ЛОКАЛЬНЫХ СЕТЯХ

Аннотация. В данной статье проведен анализ технологии XDR, исследованы ее структурная составляющая и сетевые возможности, а также ее основные проблематики. Представлены лидирующие предложения рынка и основные принципиальные особенности каждого из них. На основании выявленной информации выделены преимущества использования технологии и условия для ее внедрения.
Ключевые слова: XDR; вычислительные сети; EDR; облачные сети; централизация массивов данных.

В современном мире, неразрывно связанном с информационными технологиями, специалистам по информационной безопасности приходится реагировать на непрерывное совершенствование атак злоумышленников, совершенствуя текущие и создавая новые инструменты анализа и защиты. Вследствие высокого темпа развития средств защиты на рынке IT-решений появляется все большее количество компаний, представляющих широкий спектр современных решений в области защиты информации. В особенности остро актуальность применения средств обеспечения ИБ проявилась весной 2020 года в условиях введенных ограничений на территории большинства стран, нагрузка на глобальные информационно-телекоммуникационные сети возросла, что вызвало повышенный интерес к новым методам защиты информационных систем. Особое внимание привлекли технологии XDR.

XDR (Extended Detection and Response) – это расширенное обнаружение и реагирование на сложные угрозы и целевые атаки [1]. В нынешних реалях большинство атак направленны сразу по нескольким направлениям, поэтому компаниям необходимо обращать внимание не только на конечные системы, но и на другие, потенциальные точки проникновения в корпоративную инфраструктуру. Чтобы быстрее найти уязвимость в корпоративной сети,

мошенники используют многовекторные атаки, направленные сразу по нескольким направлениям, поэтому организации должны понимать, через какие лазейки хакеры могут проникнуть на их сервера. Имея полную карту атак, организация может быстро определить точку проникновения, проанализировать источники и организовать дальнейшие расследование инцидентов в пределах сразу всей сети, а не отдельных ее элементов. XDR включает в себя совокупность продуктов, направленных на контроль и обеспечение безопасности сразу всей сети, решение интегрируют в экосистему компании для мониторинга, безопасности, обнаружения имеющихся недостатков и контроля конечных точек, сети, серверов и облаков. Данный продукт обеспечивает аналитикам по безопасности дополнительные возможности просмотра и анализа данных, при этом облегчая командам работу, позволяя быстрее выполнять какие-либо этапы или автоматизируя их [2].

Основные составляющие XDR

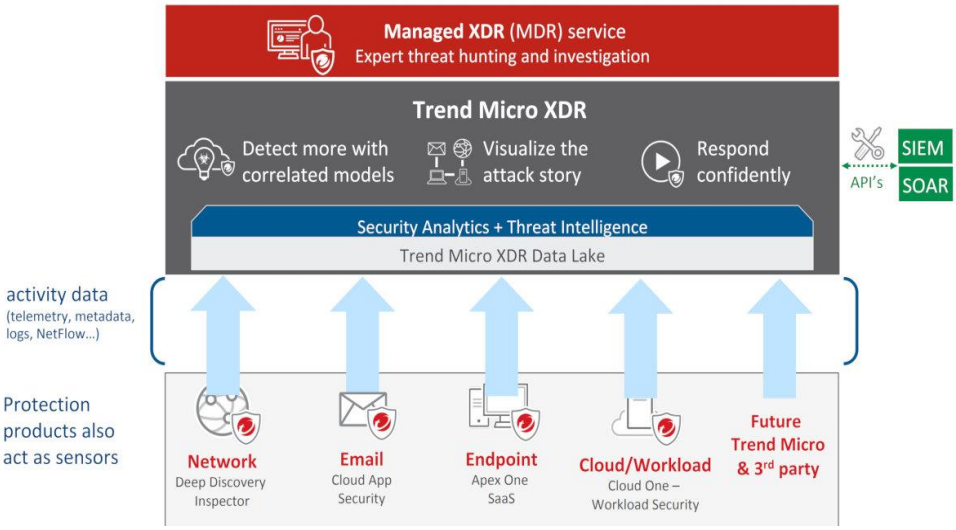


Рис. 1. Структурная схема взаимодействия компонентов XDR-решения на примере продукта Trend Micro

Описывая сильные стороны данной технологии, необходимо четко выявлять совокупность основных четырех систем, приносящих столь плодотворный синергетический эффект [3].

1. UBA

User Behavioral Analytics (анализ поведения пользователей) – это сеть объединенных систем, собирающих логи любых действий пользователей и анализирующих их с использованием технологии машиного обучения для построения общей модели поведения пользователя конечной системы.

User and Entity Behavioral (Analytics нализ поведения пользователей и ИТ-объектов) – представляет UBA с дополнением в виде инфомации о работе конченых точек, а также основных опорных пунктов локальной сети.

2. EDR — обнаружение и реагирование

Endpoint Detection and Response [4] (обнаружение и реагирование на конечных точках) – интегрированное решение для обеспечения безопасности конечных точек, которое сочетает непрерывный мониторинг и сбор данных конечных точек в режиме реального времени с возможностями автоматического реагирования и анализа на основе следующих решений:

- попытки сетевого соединения с вредоносными URL;
- попытки шифрования жесткого диска или файлов;
- установку недоверенного драйвера или службы;
- изменения параметров безопасности;
- внедрение в код «чужого» процесса;
- изменение ключей реестра, связанных с автозапуском;
- использование внутренних отладочных привилегий ОС;
- нелегитимное использование PowerShell.

3. SIEM — сбор и обработка событий

Программное обеспечение SIEM собирает и объединяет данные журналов, генерируемые всей технологической инфраструктурой организации, от хост-систем и приложений до сетевых устройств и устройств безопасности, таких как межсетевые экраны и антивирусные фильтры. Затем программное обеспечение идентифицирует и классифицирует инциденты и события для последующего анализа.

4. SOAR — оркестрация, анализ и реагирование

Платформы SOAR представляют собой набор программных решений и инструментов безопасности для просмотра и сбора данных из различных источников. Затем решения SOAR используют возможности экспертов-аналитиков и методов машинного обучения для анализа этих разнообразных данных, чтобы понять и определить приоритеты действий по реагированию на инциденты.

Таким образом, система, объединяющая данные технологические ответвления информационной безопасности, позволяет собирать и сопоставлять данные на уровне конечных устройств, серверов, электронной почты, облачных хранилищ, обеспечивая систематический сбор и мониторинг возможного контекста для последующего анализа сложных угроз. За счет данных действий происходит получения более полной картины угроз, что является непосредственным следствием анализа большего потока информации, в область анализа специалистов по безопасности попадают события, ранее ускользавшие от внимания.

Основные проблематики стэка

Решения, предлагаемые XDR, отвечают спектру нужд в области определения угроз и реагирования на них, представляя «SOC в коробке», нацеленный на интеграцию элементов управления, нормализации телеметрии, увеличении возможностей аналитики и постепенной автоматизации решений. Это оказывает сильное влияние на защищенность систем, значительно повышая ее. Однако, как и большинство молодых технологий, только вводимых в практику, она обладает несколькими проблемами [5].

1. Сложность развертки. Большинство сегодняшних инфраструктур, связанных с технологиями безопасности, состоит из множества разнообразных точечных инструментов. Организации практикуют использование нескольких программ для обеспечения защищенности систем, переплетая защиту контрольных точек с контролем утечек информации. Вследствие этого

возникает сложность перехода от набора инструментов к более долгосрочной технологий кибербезопасности.

2. Возможная конфронтация с SOC. Так как решение предполагает отсутствие элементов, представляющих анализирующий центр, крупные компании могут застопорить внедрение, вследствие издержек на обучение сотрудников.

3. Конкуренция с сервисами MDR / MSSP. Занятие ниши обеспечения организаций возможностями по обнаружению угроз и внедрению ответных мер для обеспечения безопасности системы, представляет сложность для использования XDR. Поэтому требуется постепенный ввод услуг от поставщиков технологии с оказанием услуг использования собственных продуктов, или интеграция системы в существую инфраструктуру сервисов MDR / MSSP.

Из-за "молодости" этого совершенно нового класса систем, на рынке присутствует не так много продуктов подобного рода. Но те разработки, которые сейчас доступны заказчикам, продолжают развиваться и обновляться, совершенствуясь и переходя из состояния наработок в готовые решения как для частных компаний, так и для государственных учреждений. Для сравнения возьмем для рассмотрения пару наиболее развитых предложений рынка - Cortex XDR и Cynet 360.

Cynet:

Cynet 360 – первая в мире платформа автономной защиты от взломов, которая изначально объединяет возможности предотвращения и обнаружения XDR с автоматическим расследованием и исправлением с помощью одного легкого агента с нулевыми операционными усилиями. Платформа Cynet XDR дополняется круглосуточной службой MDR, которая обеспечивает отслеживание угроз, реагирование на инциденты, отчеты об атаках и анализ вредоносных программ, делая сквозную защиту от взломов доступной для любой организации, независимо от размера и навыков ее группы безопасности.

Как только угрозы обнаружены, удобная система управления угрозами инициирует процесс исправления и исправления, также называемый исправлением [6]. Cynet чрезвычайно гибок, поскольку процесс, начинающийся со сканирования конечных точек, пользователей и сетей для устранения угроз, автоматизирован и не требует использования агентов.

Рис. 2. Платформа Cynet

Так Cynet предоставляет единую платформу для защиты организации за счет автоматизации мониторинга и контроля, предотвращения и обнаружения атак, а также оркестровки ответов. Это единственная платформа, которая объединила возможности NGAV, EDR, сетевой аналитики, UBA и Deception.

Palo Alto Networks:

Cortex XD представляет собой первую в мире платформу расширенного обнаружения и реагирования на угрозы благодаря полной интеграции данных сетей, конечных точек и облаков для блокирования самых сложных атак. Он обеспечивает защиту конечных устройств от вредоносных программ, эксплойтов и безфайловых атак благодаря инструментам на базе ИИ для локального анализа и защиты на основе анализа поведения [7].

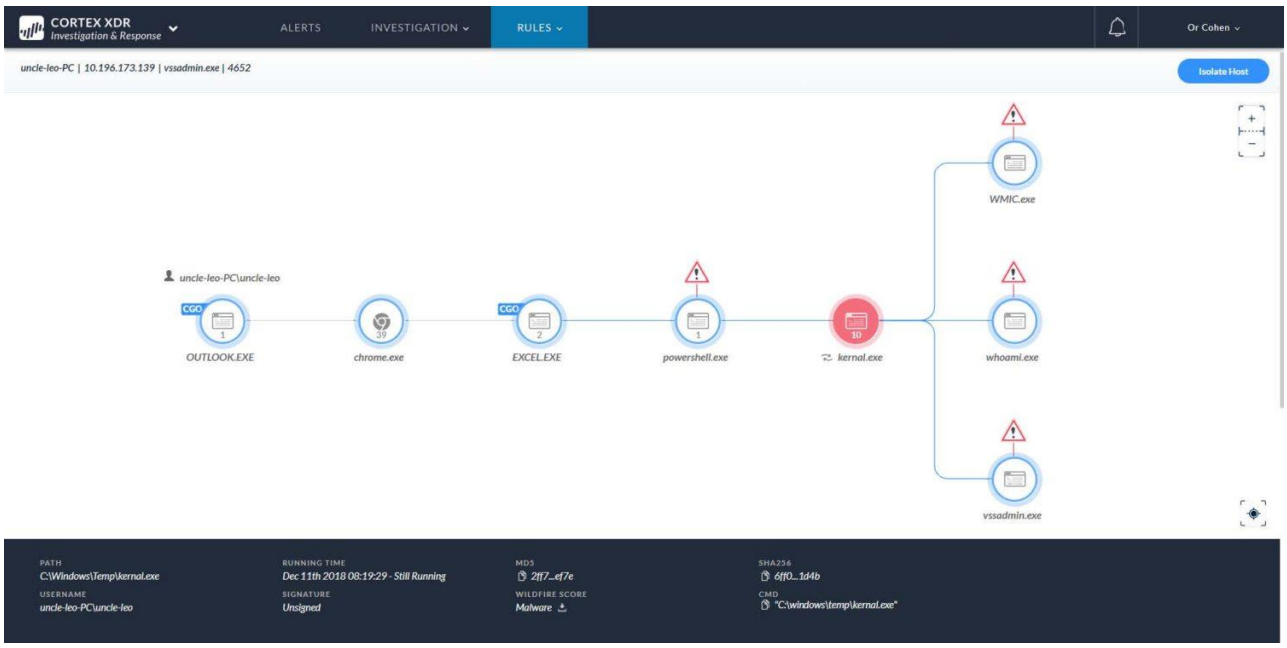


Рис. 3. Функции интеллектуального группирования

Функции интеллектуального группирования и дедупликации оповещений упрощают их обработку и сокращают объем операций, необходимых на каждом этапе обеспечения безопасности. Так же он включает в себя широчайший набор модулей защиты от эксплойтов, который позволяет блокировать эксплойты, ведущие к заражению вирусами. Каждый файл изучается адаптивной системой локального анализа на базе ИИ, которая непрерывно обучается, чтобы эффективно противостоять новым атакам. Система защиты на основе анализа поведения изучает поведение нескольких взаимосвязанных процессов, чтобы эффективно выявлять атаки по мере их появления

Проанализировав данные проблемы внедрения технологий XDR, а также опираясь на особенности предложений основных компаний данного направления, выделим основные премущества XDR на момент осени 2021 года.

Способность обнаруживать и анализировать угрозы

XDR способен анализировать как внутренние, так и внешние угрозы. Это гарантирует, что любая вредоносная атака будет обнаружена как внутри, так и во внешней среде. Он может легко идентифицировать угрозу, которая могла обойти проверку конечной точки [8].

Он обладает интеллектом для сопоставления информации об известных угрозах и атаках и внимательно анализирует стратегии и инструменты, используемые при атаке, для обнаружения любых аналогичных действий в расширенной среде. Эта функция также дает преимущество над традиционными методами безопасности, которые могут обойти эти расширенные угрозы.

Определение первопричины атаки и помощь в реагировании на нее.

Как только угроза или атака обнаружены, инструменты определяют основную причину атаки, а также измеряют ее серьезность. XDR, будучи способным анализировать внешние угрозы, также опережает следующий шаг злоумышленника.

Поскольку анализ данных является централизованным, группы безопасности могут быстро анализировать события и реагировать на них, что ускоряет и упрощает процесс. Ответные действия также инициируются через интерфейс XDR. Процесс расследования также централизован, что дает лучшее представление обо всех атаках / событиях в сети.

Технологическая ценность получаемого от внедрения инструментария

Решения XDR зарекомендовали себя как отличный актив с точки зрения защиты от вредоносных угроз, и с течением времени обеспечили возросшие и дополнительные преимущества [9].

Собранные данные могут быть полезны для обнаружения и анализа продвинутых угроз как внутри, так и снаружи, и могут быть сохранены и доступны в любое время, поскольку XDR использует облачные ресурсы. Это делает процесс расследования угрозы более тщательным.

Решения XDR могут эффективно сочетаться с существующими мерами безопасности, чтобы упорядочить и систематизировать ответы.

Вывод

XDR позволяет объединять множество продуктов от одного производителя в одну структуру, которая предоставляет возможность

отслеживать обмен информации внутри системы. Благодаря центральному консольному управлению специалисты по кибербезопасности компаний могут гораздо эффективнее реагировать и расследовать инциденты. Объединение множества задач в единую экосистему позволит вывести на новый, гораздо более высокий уровень, реагирование на происшествия, благодаря чему специалисты в области информационной безопасности могут проводить многоуровневый анализ данных, а также заранее выявлять и устранять недостатки. XDR – технология, которая позволяет сократить время на распознание, сдерживание и реагирование, что в свою очередь значительно уменьшает последствие происшествия.

СПИСОК ЛИТЕРАТУРЫ

1. Cisco, [В Интернете]. Available: https://www.cisco.com/c/ru_ru/products/security/what-is-xdr.html.
2. trendmicro, [В Интернете]. Available: https://www.trendmicro.com/ru_ru/what-is/xdr.html.
3. anti-malware.ru, [В Интернете]. Available: https://www.anti-malware.ru/compare/Managed-Detection-and-Response-MDR-services.
4. xakep.ru, [В Интернете]. Available: https://xakep.ru/2020/09/10/trend-micro-xdr/.
5. ZXWN. [В Интернете]. Available: https://habr.com/ru/post/551128/.
6. Cynet, [В Интернете]. Available: https://www.cynet.com/.
7. Paloaltonetworks, [В Интернете]. Available: https://www.paloaltonetworks.com/.
8. fortinet, [В Интернете]. Available: https://www.fortinet.com/ru/resources/cyberglossary/what-is-XDR.
9. Лаборатория касперского, [В Интернете]. Available: https://encyclopedia.kaspersky.ru/glossary/xdr-extended-detection-and-response/.
10. Tiger-optics, [В Интернете]. Available: https://blog.tiger-optics.ru/2021/03/xdr/.

УДК 004.8

А. В. МУЛИНА, А. И. ДЕНМУХАММАДИЕВА
alina.mulina297@gmail.com alan.lichtenberg@yandex.ru
Науч. руководов. – доц. В. Е. КЛАДОВ

Уфимский государственный авиационный технический университет

АНАЛИЗ МЕТОДОВ ЗАЩИТЫ ОТ АТАК НА СИСТЕМЫ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Аннотация. В данной статье рассматриваются модели искусственного интеллекта, возможные реализации угроз на данные модели, а также способы защиты от таких угроз.
Ключевые слова: искусственный интеллект$ информационная безопасность$ информационные технологии; машинное обучение.

Технологии искусственного интеллекта прочно вошли в современную жизнь. Технологии машинного обучения применяются в бизнесе, медицине, научных исследованиях и на производстве. Множество организаций во время пандемии осознали все плюсы искусственного интеллекта и начали активно развивать данные технологии. 57% компаний начали разработку в области ИИ, а 42% компаний создали специальные подразделения внутри организации. [1]

Искусственный интеллект - это наука и технология создания интеллектуальных машин. Наиболее популярными методами ИИ сегодня является машинное обучения (ML) и глубокое обучение (DL). В основе машинного обучения лежат методы анализа на основе данных. Наборы алгоритмов используют предоставленные данные для обучения и прогнозирования. В отличие от обычных алгоритмов, система машинного обучения на выходе предоставляет “правильный результат” на основе предыдущих данных. Глубокое обучение основано на алгоритмах машинного обучения для моделирования высокоуровневых абстракций с применением многочисленных нелинейных преобразований. [2]

Несмотря на популярность и широкое применение технологий искусственного интеллекта, алгоритмы машинного обучения в реальных

условиях могут выдавать ошибки и сбоить. К тому же такие ошибки можно вызвать намеренно, чем могут воспользоваться преступники.

Основная цель преступника - это нарушение свойств информации: конфиденциальности, целостности и доступности.

Чтобы обезопасить систему искусственного интеллекта, нужно принять во внимание следующие проблемы, с которыми можно столкнуться:

– Программная и аппаратная безопасность:

Код и микросхемы модели ИИ могут содержать уязвимости и бэкдоры. Из-за сложной структуры, в таких моделях обнаружить бэкдоры проблематично, поэтому программной и аппаратной безопасности должно быть уделено достаточно внимания.

– Целостность данных:

На этапе обучения злоумышленники могут вводить вредоносные данные в модель ИИ. Также они могут добавить искажающие данные к входным выборкам, что может изменить результат вывода.

– Конфиденциальность модели:

Злоумышленники могут попытаться создать клон модели, с помощью атаки оракула.

– Устойчивость модели:

Обучающие образцы могут не покрывать всех угловых случаев, что может привести к неустойчивости модели. Следовательно, модель может выдавать неверные результаты.

– Конфиденциальность данных:

Если в системе обрабатываются данные, предоставленные пользователями, то злоумышленники могут попытаться украсть персональные данные, многократно посылая запросы модели.

Из всего вышесказанного можно построить схему паттернов атак на модели ИИ:

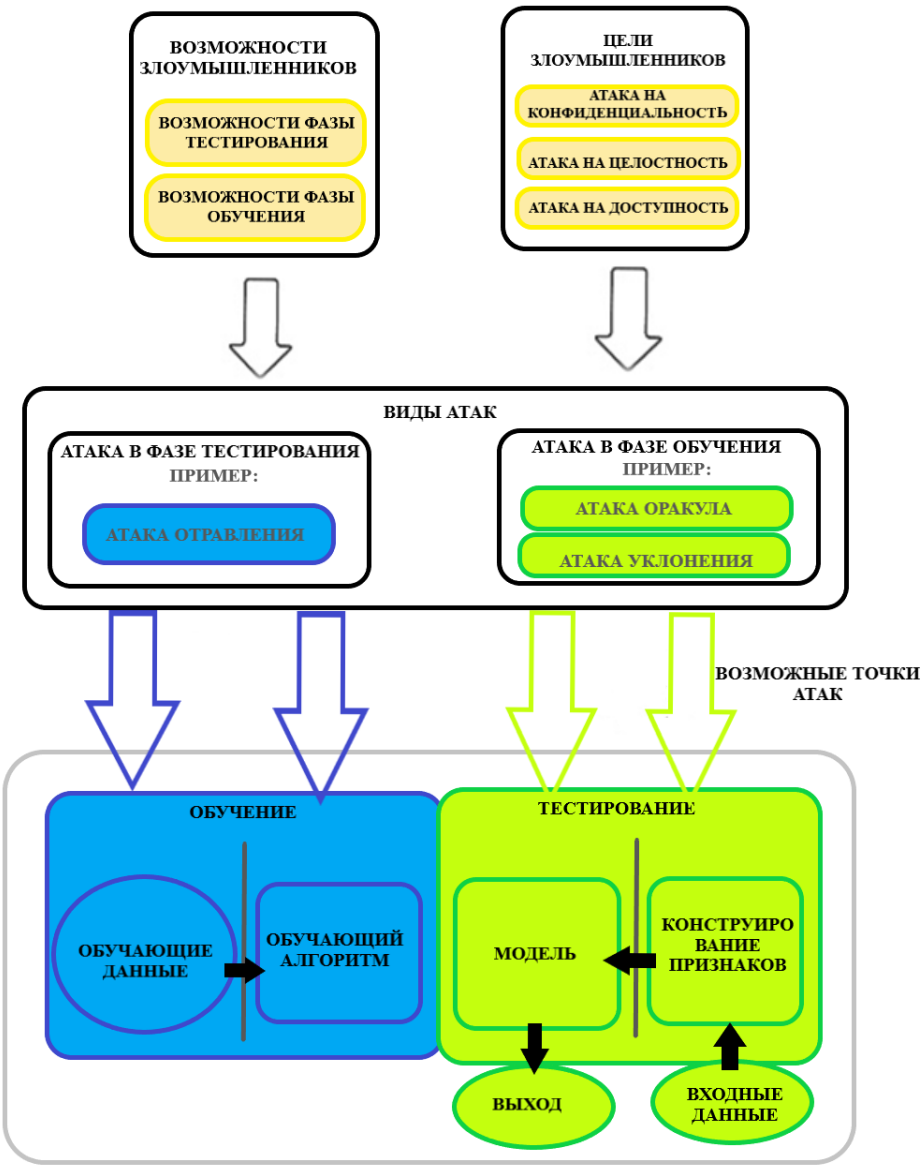


Рис. 1. Схема возможных состязательных атак на ИИ модели

На этапе тестирования входные данные обрабатываются моделью машинного обучения, чтобы создать вероятностный классификатор, который далее станет основой для внешней системы. [3]

Рассмотрим основные виды атак против систем искусственного интеллекта.

“Отравляющие” атаки. Системы искусственного интеллекта обычно переобучаются, получая новые данные после установки. Так как модели глубокого обучения требуют огромное множество образцов, трудно гарантировать их качество. В исследование [4] обнаружили, что смешивание

обучающих образцов с измененными образцами, значительно влияют на результат. Всего 8% искаженных образцов могут вызвать 75-ти процентное изменение результатов. [4]

Атака оракула. Это атаки, при которых злоумышленник использует образцы ввода-вывода для сбора и вывода информации о модели или о ее обучающих данных. [5] Таким атакам могут быть подвержены системы, которые работают с введенными пользователем данными. Злоумышленник может вводить входные данные и наблюдать за выходными значениями. Такие пары ввода-вывода используются для обучения суррогатной модели, которая работает также как обучающая модель. [6] Схема атаки оракула представлена на рис. 2.

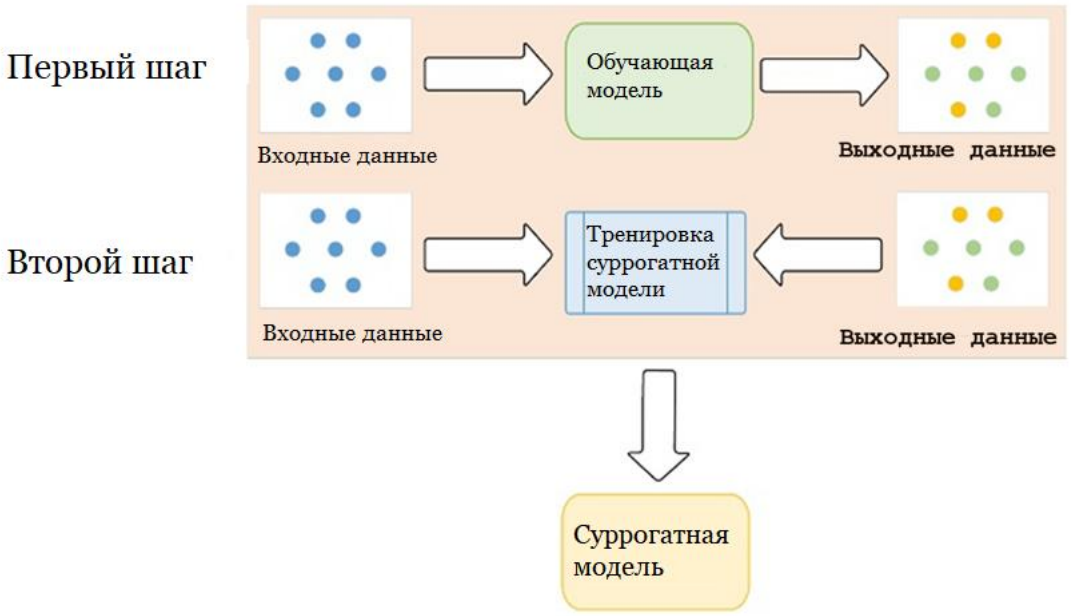


Рис. 2. Шаги атаки оракула

Атаки уклонения. При данном типе атак злоумышленник напрямую манипулирует входными выборками, чтобы избежать обнаружения. Это наиболее распространенный тип атак на системы ИИ. Однако модели глубокого обучения могут противостоять таким атакам, так как в них могут содержаться функции, которые могут сопротивляться враждебным данным. Атаки

уклонения не изменяют поведение системы, а используют ее уязвимости, чтобы привести к желаемым ошибкам.

Для защиты систем искусственного интеллекта от рассмотренных выше атак были разработаны определенные методы обеспечения безопасности.

Фильтрация данных. Это метод защиты от “отравляющих” атак, который отсеивает зараженные образцы перед использованием модели. [7] Данный метод может быть реализован путем определения возможных зараженных образцов с помощью меток, которые фильтруются во время переобучения. Также возможно реализовать данный метод сравнения моделей, позволяющего снизить зараженные образцы и отфильтровать их.

Обучение состязательности. Это метод защиты от атак уклонения, который используется во время обучения системы. На данном этапе в системе генерируется состязательные примеры, добавляющиеся к обучающим данным. Этот метод повышает надежность системы, но из-за количества итерационных вычислений он может занимать много времени. [8]

Метод дистилляции. Это метод, основанный на передачи знаний от совокупности моделей или отрегулированных моделей, другим моделям. Такая передача знаний способна снизить чувствительность системы к небольшим возмущениям и улучшить ее надежность. [9]

Реконструкция входных данных. Этот метод основан на деформации входных данных на этапе вывода модели. Реконструкция входа может быть реализована путем добавления шума, устранения шумов или использования автоматического кодировщика (автокодировщика) для изменения входной выборки. [10]

Регрессионный анализ. Данный анализ использует статистические методы для обнаружения шума и аномальных значений данных. Такая технология может реализоваться разными способами, например, для модели могут быть определены различные функции потерь для проверки аномальных значений или могут использоваться характеристики распределения данных.

Анализ ансамблем. Эта технология основана на использовании нескольких подмоделей для улучшения способности системы машинного обучения защищаться от атак отравления. Анализ ансамблем снижает риск реализации “отравляющей” атаки, благодаря тому, что несколько независимых моделей используют разные наборы обучающих данных. [11]

Дифференциально конфиденциальная защита. Метод, позволяющий сохранить конфиденциальность частной информации, внесением случайности в обучающие данные. Дифференциальная конфиденциальность помогает защитить обучающие данные от инверсионных атак, направленных на восстановление обучающих данных из параметров модели. [12]

Таким образом, системы искусственного интеллекта активно применяются в бизнесе и на производстве. Область состязательного машинного обучения привлекает большое внимание исследователей и продолжает развиваться. Для того чтобы системы ИИ развивались и дальше, нужно обратить внимание на их безопасность. Особое внимание нужно уделить целостности данных и устойчивости модели.

Основные атаки злоумышленников направлены на вызывание ошибок в результатах работы систем и краже конфиденциальной информации. Несмотря на существующие методы защиты от данных атак, все еще существует вероятность реализации угрозы. Поэтому компаниям и предприятиям стоит уделять безопасности используемых систем искусственного интеллекта больше внимания.

СПИСОК ЛИТЕРАТУРЫ

1. Latest IDG Research Explores Artificial Intelligence & Machine Learning Trends Amid the Pandemic. [Электронный ресурс] URL: https://www.idg.com/news/latest-idg-research-explores-artificial-intelligence-machine-learning-trends-amid-the-pandemic/
2. *Deng, L.; Yu, D.* Deep Learning: Methods and Applications (неопр.) // Foundations and Trends in Signal Processing. — 2014. — Т. 7, № 3—4. — С. 1—199. — doi:10.1561/2000000039. [Электронный ресурс] URL: http://research.microsoft.com/pubs/209355/DeepLearning-NowPublishing-Vol7-SIG-039.pdf
3.Ayodeji Oseni, Nour Moustafa, Helge Janicke, Peng Liu, Zahir Tari, and Athanasios Vasilakos. 2020. Security and Privacy for Artificial Intelligence: Opportunities and Challenges. J. ACM 37, 4, Article 111 (August 2020), 35 pages.

4. M. Jagielski, A. Oprea, B. Biggio, C. Liu, C. Nita-Rotaru and B. Li, "Manipulating machine learning: Poisoning attacks and countermeasures for regression learning," in IEEE Symposium on Security and Privacy (S&P) , 2018.
5. Elham Tabassi, Kevin J Burns, Michael Hadjimichael, Andres D Molina-Markham, and Julian T Sexton. 2019. A Taxonomy and Terminology of Adversarial Machine Learning
6. Yi Shi and Yalin E Sagduyu. 2017. Evasion and causative attacks with adversarial deep learning. In MILCOM 2017-2017 IEEE Military Communications Conference (MILCOM). IEEE, 243–248.
7. Patrick PK Chan, Zhi-Min He, Hongjiang Li, and Chien-Chang Hsu. 2018. Data sanitization against adversarial label contamination based on data complexity. International Journal of Machine Learning and Cybernetics 9, 6 (2018), 1039–1052
8. Florian Tramèr, Alexey Kurakin, Nicolas Papernot, Ian Goodfellow, Dan Boneh, and Patrick Drew McDaniel. 2018. Ensemble adversarial training: Attacks and defenses. In 6th International Conference on Learning Representations, ICLR 2018
9. Nicolas Papernot, Patrick McDaniel, Arunesh Sinha, and Michael P Wellman. 2018. SoK: Security and privacy in machine learning. In 2018 IEEE European Symposium on Security and Privacy (EuroS&P). IEEE, 399–414
10. S. Gu and L. Rigazio, "Towards deep neural network architectures robust to adversarial examples," in International Conference on Learning Representations (ICLR) , 2015.
11.Thomas G Dietterich. 2000. Ensemble methods in machine learning. In International workshop on multiple classifier systems. Springer, 1–15
12. Mathias Lecuyer, Vaggelis Atlidakis, Roxana Geambasu, Daniel Hsu, and Suman Jana. 2018. On the connection between differential privacy and adversarial robustness in machine learning. stat 1050 (2018), 9.

УДК 004.056.5

Т. И. МУХАМАТУЛЛИН, Д. В. ЗОЛОТАРЕВ, Д. А. МИШНЕВ
danilzolotarev1980@gmail.com
Науч. руководитель – канд. юр. наук. доц. Н. Д. АНДРЕЕВ

Уфимский государственный авиационный технический университет

ТЕХНОЛОГИЧЕСКИЕ ВОЗМОЖНОСТИ SD-WAN

Аннотация. В статье представлены анализ структуры использования SD-WAN предложений на наличие мест слабой защищенности. Объяснен основной принцип действия технологии, а также каждой ее составляющей. На основании выявленной информации предложены средства обеспечения безопасности трафика.
Ключевые слова: SD-WAN; проблематика топологии сети; vSmart Controllers; информационная безопасность; WAN.

С начала цифровой революции, кардинально повлиявшей на развитие человечества, прошло всего полвека, однако за столь короткий промежуток времени, нам удалось совершить поистине грандиозный скачок в сфере информационных технологий и вывести процесс глобализации на совершенно иной уровень, чем имевшийся когда-либо до этого. При этом стоит понимать, прогрессия не замедляется, а лишь ускоряется с течением времени. Так за последние несколько лет в глобальных сетях произошли значительные изменения в устройстве локальных сетей, одним из которых, выделяется технологическое решение по созданию программно определяемых сетей типа SD-WAN, полностью меняющих представление сетевых специалистов об оптимизации и использовании возможностей многопротокольной коммутации меток, ретрансляции кадров, а также Digital Subscriber Line.

Основным преимуществом SD-WAN по сравнению с традиционными WAN является уровень видимости сети, которую обеспечивает он обеспечивает. Сетевые администраторы могут централизованно управлять сетью, отслеживая несоответствия трафика. Благодаря этой функции стало возможно обеспечивать бесперебойную работу приложений, устранять неполадки в сети и обеспечивать правильную работу элементов безопасности и политик. Так, благодаря появлению больших возможностей по перенаправлению трафика, перед

специалистами в области информационной безопасности открылся новый огромный стек решений по обеспечению защиты данных сети. А соответственно необходимость в изучение возможных технологических решений.

Устройство SD-WAN

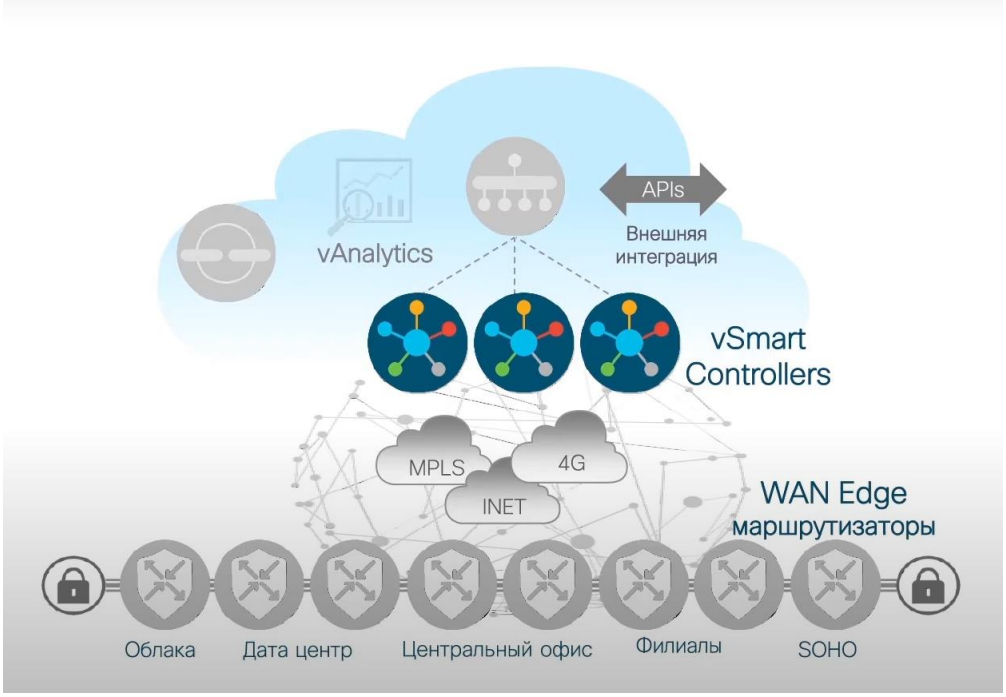


Рис. 1. Схема устройства SD-WAN от Cisco

Основным отличием технологии SD-WAN от стандартного WAN соединения является виртуальный блок позволяющий програмно определить созданную сеть, и в случае необходимости, легко и быстро адаптировать LAN к меняющимся потребностям [1]. За данную функцию отвечают специально выделенные vSmart Controllers. Фактически, это так главные обработчики данных всей сети. Они определяют маршруты поступающих и отправляеммых пакетов, балансируют нагрузку и контролируют качество каналов сети, перенаправляя запрашиваемы данные в vManage, интерфейс доступа администратора. Так основные возможности сетки распределяются на следующие характеристики.

1. *Централизованное управление*

Основное средство управления в SD-WAN - централизованное. Он часто находится в приложении SaaS, запущенном в общедоступном облаке.

Управление отделено от оборудования, чтобы упростить управление сетью и улучшить предоставление услуг [2]. Данные устройства (и виртуальные устройства) следуют принимаемым правилам сети, передаваемым от центрального контроллера SD-WAN. Это значительно снижает или устраняет необходимость в индивидуальном управлении шлюзами и маршрутизаторам.

2. Множественное соединение

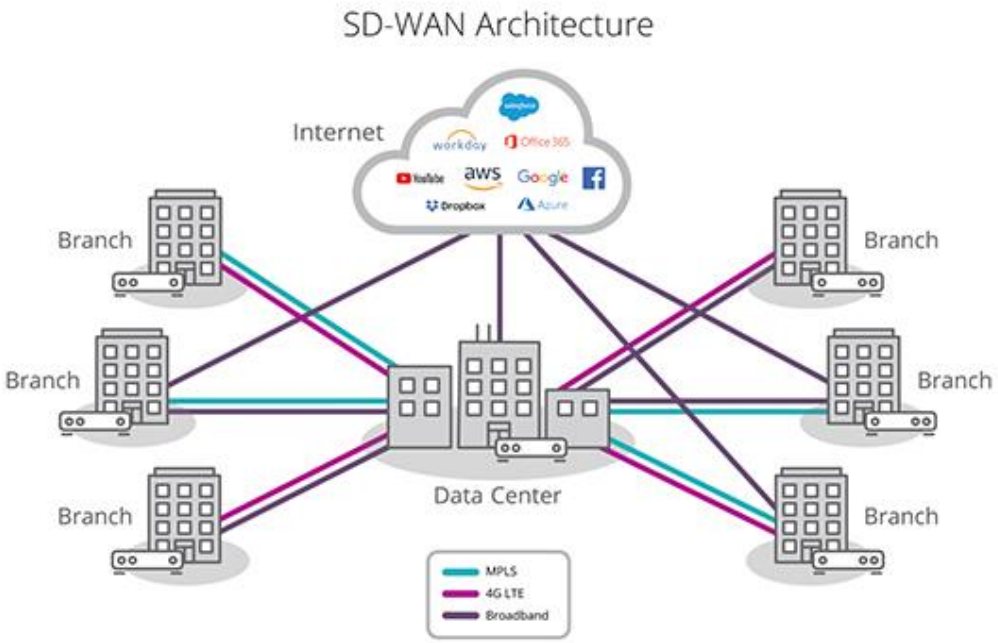


Рис. 2. Демонстрация принципа множественного соединения

Шлюзы поддерживают гибридный соединение, которое подразумевает , что каждый шлюз может иметь несколько подключений с использованием различных транспортов-MPLS, широкополосный доступ в Интернет, LTE и виртуальная частная сеть (VPN) , которую обычно устанавливают до для каждого WAN-соединение, в целях безопасности. Следовательно, технология может быть перекрытием, охватывающим разнообразную инфраструктуру связи [3].

3. Динамический выбор пути

Другой особенностью является динамический выбор пути - возможность автоматически и выборочно направлять трафик по одному или другому каналу

в зависимости от состояния сети или характеристик трафика. Пакеты могут направляться на конкретный канал, потому что другой канал не работает или работает не очень хорошо, или для балансировки сетевого трафика по всем доступным каналам. SD-WAN также может идентифицировать пакеты по приложению, пользователю, источнику / получателю и т. Д. И отправлять их по тому или иному пути на основе этих характеристик [4].

4. Управление на основе правил

Технология поддерживает политику качества обслуживания (QoS) и определяет, куда динамический выбор пути будет направлять трафик. Правила сети также определяют, какой уровень приоритета предоставляется. Решнеия для управления стэком могут быть реализованы в виде правил через центральную консоль управления. Новые и обновленные политики преобразуются в рабочие правила и загружаются на все подконтрольные шлюзы и маршрутизаторы SD-WAN. Политика может быть создана, например, для обеспечения наилучшей производительности для VoIP и интерактивных веб-конференций путем присвоения их пакетам приоритета передачи и маршрутизации их по путям с малой задержкой. Также можно достичь снижение затрат за счет отправки резервных копий файлов через широкополосное Интернет-соединение [5]. Трафик WAN, требующий высокого уровня безопасности, может быть ограничен частными соединениями (например, MPLS) между сайтами и должен проходить через надежный стек безопасности при входе на предприятие.

Проанализировав данные возможности технологии, можно вывести основной движущий принцип использования sd-wan. Он состоит в том, чтобы упростить способ создания крупными компаниями новых каналов связи с филиалами, лучше управлять способами использования этих каналов - для передачи данных, голоса или видео - и потенциально сэкономить при этом деньги. Данная возможность активно принимается рынком, как одно из наиболее удачных решений.

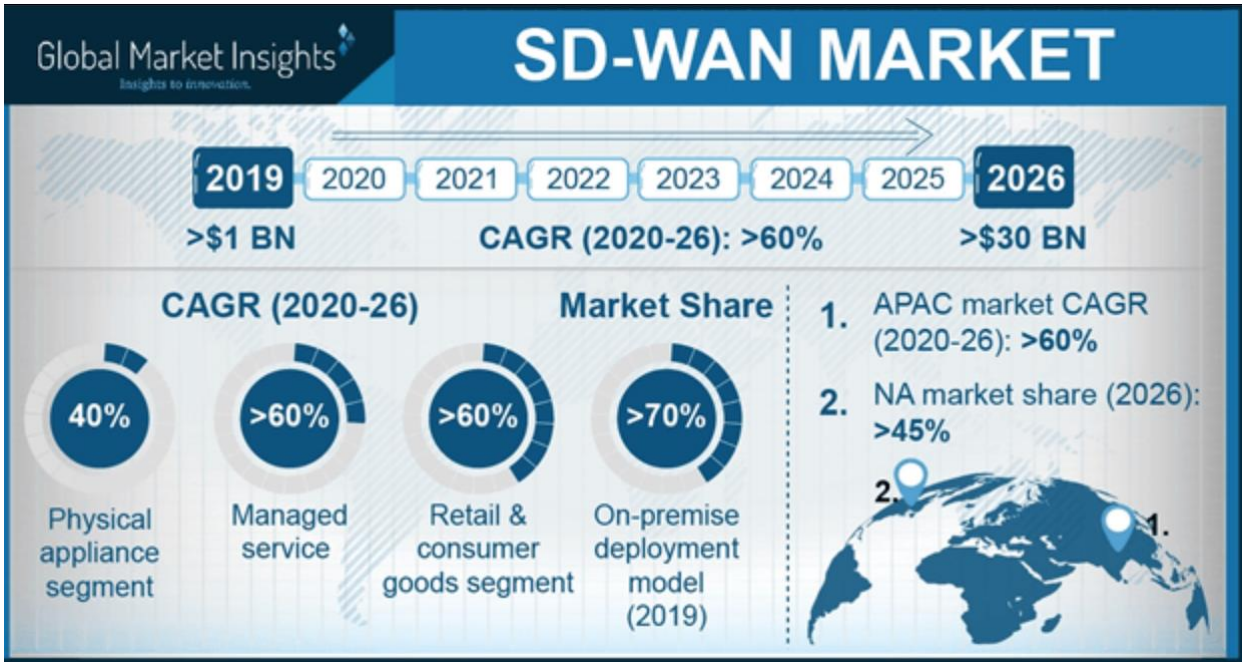


Рис. 3. Анализ рынка развития SD-WAN

Так в своем исследовании VNI Cisco сообщает, что в глобальном масштабе трафик SD-WAN составлял 9 процентов бизнес-трафика IP WAN в 2017 году и к 2022 году составит 29 процентов бизнес-трафика IP WAN. Кроме того, трафик SD-WAN вырастет в пять раз по сравнению с С 2017 по 2022 год, совокупный годовой темп роста составит 37 процентов. «SD-WAN продолжает оставаться одним из самых быстрорастущих сегментов рынка сетевой инфраструктуры, чему способствует множество факторов. Во-первых, традиционные корпоративные глобальные сети все больше не удовлетворяют потребности современного цифрового бизнеса [6]. Во-вторых, предприятия заинтересованы в более простом управлении несколькими типами соединений в своей глобальной сети для повышения производительности приложений и удобства работы конечных пользователей ", - сказал Рохит Мехра, вице-президент IDC по сетевой инфраструктуре." В сочетании с быстрым внедрением SD-WAN ведущими коммуникациями поставщики услуг во всем мире, эти тенденции продолжают стимулировать внедрение SD-WAN.

Основные средства обеспечения безопасности трафика

Сетевые функции безопасности необходимо виртуализировать, чтобы не отставать от возникающих угроз безопасности, также стоит контролировать стоимость обновления и обновления элементов безопасности. Использование же виртуальных машин для обеспечения безопасности SD-WAN означает, что обновления программного обеспечения можно устанавливать на существующее оборудование, вместо того, чтобы устанавливать новое оборудование при каждом обновлении, что экономит время и деньги [7]. Однако это не первостпенная возможность преодоставляемая технолгией. Как мы заявляли в начале статьи, основным преимуществом SD-WAN по сравнению с традиционными WAN является уровень видимости сети, которую обеспечивает SD-WAN. Сетевые администраторы могут централизованно управлять сетью и управлять ею, отслеживая несоответствия трафика. Видимость на уровне устройства выходит за рамки простого отображения данных о приложениях, создающих трафик, отображая информацию об устройстве, использующем приложение, и об человеке, использующем устройство, - если есть идентификаторы, связывающие пользователя с устройством [8]. Возможность получения информации на уровне устройства обеспечивает большую детализацию политик безопасности, которые могут применяться к сети. Система самостоятельно может группировать пользователей и определять их уровень доступа к сети и то, что они делают в сети. Используя данную возможность можно создать адаптивную СУБД, способную выдать любую необходимую информацию для администрации сети.

Также В SD-WAN можно сегментировать трафик от различных приложений на основе его характеристик и сетевых политик, установленных для SD-WAN администраторами сети. Сегментация позволяет отделить трафик от разных приложений или групп приложений друг от друга, что устраняет вектор атаки и позволяет применять политику безопасности и качество обслуживания гораздо более детально. К отдельным сегментам могут применяться разные политики.

Технология SD-WAN предоставляет специалистам иформационной безопастности возможность работать с общим потоком информации всей сети, оптимизируя ее и переводя в единое центрелизванное облако. Чем обеспечивает высокую видимость сети, возможность для шифрования как отдельных частей Lan, так и глобального шифрования трафика. . Трафик из разных приложений проходит через отдельные микросегменты SD-WAN, поэтому атака не может скомпрометировать весь трафик приложений, а соотвественно нам проще определить проблемную часть сети. Это позволяет быстрее выявлять слабые места стека, а также обеспечить его быструю адаптацию под новые правила.

СПИСОК ЛИТЕРАТУРЫ

1. Cisco. (б.д.). Получено из https://www.cisco.com/c/ru_ru/solutions/enterprise-networks/sd-wan/what-is-sd-wan.html
2. fortinet. (б.д.). Получено из https://www.fortinet.com/ru/products/sd-wan
3. huawei. (б.д.). Получено из https://e.huawei.com/ru/solutions/business-needs/enterprise-network/sd-wan
4. itel. (б.д.). Получено из https://itel.ua/ru/articles/prosto-pro-skladne-shho-take-sd-
5. wan-i-jak-vin-pracjuye
6. networkcomputing. (б.д.). Получено из https://www.networkcomputing.com/networking/software-defined-wan-primer
7. sdxcentral. (б.д.). Получено из https://www.sdxcentral.com/articles/analysis/gartner-report-highlights/2018/11/
8. tadviser. (б.д.). Получено из https://www.tadviser.ru/
9. vmware. (б.д.). Получено из https://www.vmware.com/ru/solutions/sd-wan.html

УДК 004.056.5

А. А. НАБИУЛЛИН, С. Д. ЗАХАРОВ, М. Р. ЮСУПОВ
Anvar-1398@ya.ru, zambarolz@gmail.com, i.omnishai@gmail.com
Науч. руководитель – канд. техн. наук, доц. Т. А. ИВАНОВА

Уфимский государственный авиационный технический университет

ПРИМЕНЕНИЕ ТЕХНОЛОГИИ THREAT INTELLIGENCE В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация. В данной статье рассматривается необходимость внедрения Threat Intelligence для повышения уровня информационной безопасности в организациях. Также представлено описание основных факторов, оказывающих влияние на эффективность Threat Intelligence, преимущества использования данной технологии и возможный сценарий ее использования.
Ключевые слова: threat intelligence; информационная безопасность; инцидент; индикатор компрометации.

Введение

Во всем мире аналитики и специалисты по информационной безопасности (ИБ) борются с различного рода угрозами, но разрозненно. Крупные компании не торопятся делиться информацией о совершенных атаках на их систему безопасности и держат в тайне новые методы противодействия. Киберпреступники, наоборот, тщательно и сообща планируют свои атаки и активно делятся уязвимостями и вредоносным ПО.

Проблема неосведомленности о новых угрозах присутствует даже в пределах одной компании, например, в крупных или территориально разрозненных. Ключевым фактором минимизации ущерба является быстрое обнаружение атаки, так как чем дольше она остается незамеченной, тем дороже она обойдется. Традиционные методы обмена информацией об инцидентах, такие как электронная почта, мессенджеры не масштабируемы и с незначительным ростом числа инцидентов перестают справляться со своей задачей. Растет нагрузка на специалистов, занимающихся мониторингом, а их эффективность снижается, что влечет за собой угрозу ИБ. Для решения этих проблем внедряется Threat Intelligence, или процесс киберразведки.

Данные, полученные в процессе, осведомляют об угрозах, атаках, о новых методах злоумышленников еще до того, как компании будет причинен какой-либо ущерб. Источниками данных могут быть антивирусные базы, центры мониторинга, закрытые сообщества хакеров, объединения по борьбе с киберпреступностью, ФинЦерт (центр мониторинга Банка России), НКЦКИ (Национальный координационный центр по компьютерным инцидентам).

Ведущая исследовательская и консалтинговая компания Gartner Inc. определяет Threat Intelligence как «совокупность знаний, построенных на наблюдениях, включающая в себя контекст, механизмы, индикаторы, последствия и практические рекомендации о существующей или возможной угрозе». Это информация, которую организация использует для определения угроз, которые были, будут или в настоящее время нацелены на организацию. Данная информация используется для предотвращения и обнаружения атак, направленных на информационные ресурсы.

Threat Intelligence может помочь организациям получить ценные знания об угрозах, создать эффективные механизмы защиты и снизить риски, которые могут нанести ущерб их прибыли и репутации. В конце концов, целенаправленные угрозы требуют целенаправленной защиты, а Threat Intelligence обеспечивает возможность предотвратить потери.

Полученные данные — это актуальные сведения об атаках, тактике и технике злоумышленников, а также индикаторах компрометации (англ. Indicator of Compromise, IoC). Они позволяют быстро выявить вредоносную активность и свести к минимуму финансовые и репутационные потери.

Наиболее распространенные индикаторы включают в себя:

– IP-адреса, URL-адреса и доменные имена;

– адреса электронной почты, темы письма, ссылки и вложения;

– ключи реестра, имена файлов и хеши файлов и DLL библиотеки.

Преимущества использования Threat Intelligence

Внедрение Threat Intelligence дает ряд преимуществ, в том числе:

– позволяет организации разработать политику безопасности, которая является прогнозирующей, а не просто реактивной, и укрепить общую политику управления рисками;

– позволяет облегчить обнаружение угроз;

– информирует о более эффективном принятии решений во время и после обнаружения атак.

В качестве программного средства, предоставляющего актуальную информацию об угрозах безопасности информации, часто используется платформа Threat Intelligence «MISP»[1], с набольшим размером сообщества среди всех платформ с открытым исходным кодом.

Преимуществом применения «MISP» является предоставление полной информации об инциденте информационной безопасности:

– описание угрозы;

– индикаторы компрометации;

– информацию о нейтрализации;

– описание злоумышленника;

– описание используемого инструмента;

– TTP (Tactics, Techniques, and Procedures).

Возможный сценарий

Обнаружение инцидентов информационной без-опасности является трудоемкой задачей: среднее время обнаружения нарушений информационной безопасности может составлять недели и месяцы Таким образом, в рамках разработки системы менеджмента инцидентов информационной безопасности стоит уделить должное внимание выбираемым программно-техническим средствам обнаружения нарушений и каналам обновления информации о нарушениях информационной безопасности (применимость, достоверность, качество поступающей информации, оперативность поступления информации и т. д.).

В качестве демонстрации предлагаемого подхода была выбрана система обнаружения и предотвращения вторжений (IDS). Свободно распространяемые

правила IDS, предоставляемые на сайте разработчика, бывают двух видов: общие правила и правила для зарегистрированных пользователей. Список общих правил часто обновляется, но не учитывает специфику угроз, характерных для данной организации. Список правил для зарегистрированных пользователей разбит на различные классы угроз, но не содержит информацию об атаках нулевого дня.

Таким образом, появляется необходимость в дополнительном источнике информации о нарушениях информационной безопасности, имеющем постоянное обновление правил и учитывающем специфику угроз, характерных для организации. Здесь и пригодится решение класса Threat Intelligence, предоставляющее актуальную информацию об угрозах безопасности информации.

Внедрение процесса кибербразведки оказывает влияние на все стадии жизненного цикла инцидента:

– обнаружение инцидента – с более полной информацией о существующих атаках легче найти инцидент;

– регистрация инцидента – в этот момент можно указать, где уже замечалась атака данного типа с данными индикаторами, что поможет в определении уровня важности;

– расследование инцидента;

– предупреждение инцидентов в будущем.

При реагировании на инциденты информационной безопасности необходимо установить факт реализации инцидента информационной безопасности и собрать информацию об инциденте информационной безопасности с использованием журналов средств защиты информации. После сбора информации об инциденте информационной безопасности специалист имеет большое количество данных об инциденте и ограниченное время на анализ данных и последующее реагирование на инцидент информационной безопасности.

С целью сокращения времени на анализ журнала системы обнаружения и предотвращения вторжений и выбора сценария по реагированию на инцидент

информационной безопасности используются скрипты, автоматизирующие фиксацию событий, обнаруженных IDS, в платформе «MISP».

На вход скрипта подается alert-файл, зафиксированный в IDS. Поле правила «msg» содержит информацию об индикаторах компрометации, информация о которых хранится в платформе «MISP». Скрипт выделяет обнаруженный индикатор компрометации, необходимый для дальнейшего распознавания конкретного, связанного с данным индикатором инцидента, информация о котором хранится в платформе Threat Intelligence. Далее осуществляется подключение к базе данных «MISP», в которой находится соответствующий порядковый номер индикатора компрометации. После этого порядковый номер передается на вход POST-запроса, позволяющего зафиксировать в рамках платформы Threat Intelligence нарушение, выявленное в рамках информационной системы.

Скрипт позволит специалисту при возникновении инцидента информационной безопасности уменьшить время на анализ и реагирование на инцидент информационной безопасности. Фиксация инцидентов информационной безопасности в рамках платформы Threat Intelligence «MISP» также позволит отслеживать реализованные в рамках организации угрозы информационной безопасности, что даст возможность анализировать недостатки существующей системы защиты информации организации с целью ее дальнейшего совершенствования.

Факторы, влияющие на эффективность Threat Intelligence

На эффективность Threat Intelligence влияют следующие факторы: источники данных (feeds), платформа, API и используемые стандарты.

Feeds – это данные об угрозах, например, IP и DNS-адреса, URL, CVE-записи, ключи реестра и т. д. Данные об угрозах могут быть общими (информация о вредоносном ПО, DNS, спаме и т. д.) и узкоспециальными (информация предназначена для конкретной отрасли).

Существует множество внешних источников такой информации. Среди российских поставщиков выделяются: Group-IB, Kaspersky, Cisco, среди зару-

бежных – Check Point, Arbor ATLAS и др. Именно выбор источника данных об угрозах является одной из самых первых задач, которые необходимо решить на этапе планирования внедрения Threat Intelligence в существующую систему защиты информации.

При поиске поставщика данных для нужд организации возникает множество вопросов, таких как: насколько предоставляемые ими данные полны? Насколько оперативно они обновляются? Насколько они учитывают отраслевую специфику? Для решения данной проблемы при выборе источника данных рекомендуется оценить следующие параметры: число записей, доверие к источнику пользователей, частота предоставления информации, формализованность представления информации, возможность автоматизации, количество ложноположительных индикаторов.

Автоматизировать процесс Threat Intelligence и интегрировать его с существующей системой защиты позволит API (application programming interface) – на средства защиты информации (IDS, SIEM, межсетевые экраны и т. д.) будут поступать правила, позволяющие защитить информацию от актуальных угроз.

Выбор того или иного API будет напрямую зависеть от того, какие средства защиты информации применяются в организации [5].

Использование данных об угрозах

Threat Intelligence бывает разных форматов, но обычно его можно классифицировать как:

– Сетевой: веб-классификация, веб-репутация, репутация IP, антифишинг.

– Файловый: репутация файла (исполняемые файлы, потенциальное вредоносное ПО).

– Мобильный: репутация приложения, безопасность мобильных устройств.

Сегодня на рынке предлагается аналитика угроз в следующих категориях, которые могут быть использованы вместе или по отдельности. Службы безопасности включают:

– Веб-классификация – обеспечивает классификацию контента для миллиардов веб-страниц, чтобы защитить пользователей от сетевых угроз.

– Web Reputation – прогнозирует риск для безопасности посещения веб-сайта и позволяет администраторам точно настраивать параметры безопасности.

– IP Reputation – публикует динамический анализ IP-адресов высокого риска и анализ входящих и исходящих сообщений.

– Антифишинг в режиме реального времени – ловит сложные фишинговые атаки, обеспечивая своевременную защиту с помощью сканирования в режиме реального времени перед посещением сайтов.

– Репутация файлов – обеспечивает динамический анализ репутации известных вредоносных файлов и файлов из белого списка, чтобы остановить распространение вредоносных программ.

– Репутация мобильного приложения – классифицирует и оценивает приложения с помощью многоэтапного анализа и передовых алгоритмов, чтобы убедиться, что они безопасны и соответствуют требованиям.

На данном этапе развития Threat Intelligence существует большое количество стандартов, применимых для описания угроз и осуществления информационного обмена, однако, единого общепризнанного стандарта для Threat Intelligence не существует. Российские поставщики Threat Intelligence используют стандарты STIX (Structured Threat Information eXpression) и TAXII (Trusted Automated eXchange of Indicator Information). Стандарт STIX является стандартом описания различных угроз, индикаторов атаки, информации об инциденте, рекомендаций о реагировании на инцидент и т. д. Стандартом обмена информации об угрозах, описанных с помощью STIX, является стандарт TAXII. Эксперт по информационной безопасности Алексей Лукацкий [5] в качестве стандарта рекомендует использовать CIF (Collective Intelligence Framework). Обосновано это тем, что в России существует опыт эксплуатации данного стандарта, а также возможность интеграции CIF под нужды организации (генерация пра-

вил для IDS и других средств защиты информации). Таким образом, внедрение и эксплуатация Threat Intelligence позволяет организациям получать знания об угрозах и рисках в реальном времени, что позволит поддерживать систему защиты информации в актуальном состоянии, и, соответственно, обеспечивать высокий уровень безопасности информации в организации. Так, например, согласно исследованию SANS Institute организации-потребители Threat Intelligence отметили следующие положительные изменения, полученные после внедрения: 63 % опрошенных считают, что улучшилось пони-мание методов и тактик атакующих; 51 % организаций утверждают, что обнаружение и реагирование на инциденты информационной безопасности стали быстрее и точнее; 48 % говорят о снижении количества зафиксированных инцидентов за счет уменьшения количества ложных срабатываний средств защиты информации; 28 % опрошенных отметили увеличение точности и скорости мониторинга и управления инцидентами. [19]

Выводы

Рынок Threat Intelligence появился относительно недавно, но уже стал важным компонентом кибербезопасности для многих организаций. Запросы на эти услуги будут расти в ближайшее время, так как традиционные решения кибербезопасности не всегда успевают за постоянно изменяющимися методами атак и за растущей профессионализацией хакеров. Прогнозирование потенциальных атак позволяет компаниям подготавливаться к ним и таким образом смягчать их последствия.

Данных из бесплатных источников данных кибер-разведки зачастую будет недостаточно, организации скорее всего придется использовать платные подписки на данные от ведущих Центров безопасности

В любом случае, успех применения Threat Intelligence в процессе мониторинга инцидентов ИБ зависит от выбора источников, правильной настройки взаимодействия с другими средствами защиты и работы аналитиков над полученной информацией.

СПИСОК ЛИТЕРАТУРЫ

1. Дрянных Ю.Ю., Жуков В.Г. «Структурный подход к расследованию инцидентов информационной безопасности на базе платформы threat intelligence». 2018 г.
2. Дрянных Ю.Ю., Жуков В.Г. «О необходимости внедрения threat intelligence.» 2017 г.
3. Webroot «Threat Intelligence: What is it, and How Can it Protect You from Today's Advanced Cyber-Attacks? »
4. АО «Лаборатория Касперского» «Сервисы Kaspersky Security intelligence». 2016 г.
5. Алексей Лукацкий «Новое решение Cisco по кибербезопасности – Cisco Threat Intelligence Director». 2017 г.
6. Dave Shackleford «Who's Using Cyberthreat Intelligence and How? » 2015 г.
7. Н.С. Исаков, В.Г. Жуков «Потребители информации об угрозах безопасности информации Threat Intelligence процесса». 2018 г.
8. Алексей Лукацкий «А что, если завтра нас отключат от CVE? Или как создать собственную систему Threat Intelligence?». 2015 г.
9. Greg Farnham «Tools and Standards for Cyber Threat Intelligence Projects». 2013 г.
10. Robert D. Stelle «The Importance of Open Source Intelligence for Military». 2004 г.
11. Семиков В.С., Команов П. А. «Применение технологии распределенного реестра в системах threat intelligence» 2020 г.
12. Manfred Vielberth «Human-as-a-security-sensor for harvesting threat intelligence» 2019 г.
13. Robert Luh & Sebastian Schrittwieser «Advanced threat intelligence: detection and classification of anomalous behavior in system processes» 2019 г.
14. Fabian Böhm, Florian Menges & Günther Pernul « Graph-based visual analytics for cyber threat intelligence » 2018 г.
15. Hamad Al-Mohannadi, Irfan Awan & Jassim Al Hamar « Analysis of adversary activities using cloud-based web services to enhance cyber threat intelligence » 2020 г.
16. Owen Redwood, Joshua Lawrence, Mike Burmester «A Symbolic Honeynet Framework for SCADA System Threat Intelligence» 2015 г.
17. Daniel Schlette, Fabian Böhm, Marco Caselli & Günther Pernul «Measuring and visualizing cyber threat intelligence quality» 2020 г.
18. Sagar Samtani, Maggie Abate, Victor Benjamin «Cybersecurity as an Industry: A Cyber Threat Intelligence Perspective» 2019 г.
19. SANS Institute InfoSec Reading Room Who's Using Cyberthreat Intelligence and How? Available at: https://www.sans.org/reading-room/whitepapers/analyst/cyberthreat-intelligence-how-35767.

УДК 004.057.4

А. Р. НАСЫРОВА
nasirova.alia14@gmail.com
Науч. руководитель – канд. техн. наук, доц. Т. А. ИВАНОВА

Уфимский государственный авиационный технический университет

ПРОБЛЕМЫ ПРОТОКОЛА SS7

Аннотация. В данном материале рассматриваются основы и уязвимости протокола SS7, служащего для передачи данных в телефонных сетях. В статье уделяется внимание двухфакторной аутентификации и возможности несанкционированным доступом получить любые конфиденциальные данные пользователя. Изучение данного материала позволит читателям позволит узнать об угрозах и возможных атаках при использовании данной технологии, а также защитить себя и свои данные от злоумышленников.
***Ключевые слова*:** Signaling System №7; SS7; ОКС-7; Система сигнализации №7; протокол; информационная безопасность; несанкционированный доступ; двухфакторная аутентификация.

Введение

В современном мире очень востребована двухфакторная аутентификация как способ защиты платежных данных. Покупки, совершаемые с помощью банковских карт через Интернет, подтверждаются отправкой шестизначного кода, который знает только авторизованный пользователь. Поскольку код приходит в СМС, перехватить сообщения можно, например, с помощью протокола SS7. В таком случае мошенник будет знать и номер карты, и код, присланный на телефон, а значит сможет воспользоваться этими данными и перевести деньги на свой счет; сможет украсть пароль от социальных сетей, а затем и личные данные, или терроризировать близких, которые наивно ведутся и помогают в случаях займа, например. И деньги возвращать некому. Я думаю отклик найдется в каждом и многие с этим встречались. Это очень неприятные ситуации, и в этой статье освещены некоторые проблемы данного протокола и информация о том, как пользователь может себя защитить.

Суть протокола SS7

Эти сигнальные протоколы являются основой всей современной системы телефонной связи — они служат для передачи всей служебной информации в

телефонных сетях. Их разрабатывали еще в 1970-х, впервые использовали в 1980-х, и с тех пор они успели стать общепринятым стандартом. [1]

Изначально протоколы ОКС-7 разрабатывались для стационарной связи. Нужно было разделить голосовой трафик и служебные сигналы физически, поместив их в разные каналы. Это было сделано для борьбы с телефонными взломщиками — они использовали специальные коробочки для имитации тоновых сигналов, с помощью которых тогда передавалась служебная информация в телефонных сетях.

Позже тот же набор протоколов был использован и в мобильных сетях. Попутно телефонисты прикрутили к нему еще кучу функций — в частности, именно через ОКС-7 на самом деле передаются SMS. [2]

Разработка и развитие

Надо сказать, что эта система была разработана, опираясь именно на доверие. В 80-х годах об информационной безопасности (по крайней мере, гражданской) думали мало, важнее была эффективность, поэтому Система сигнализации №7 получилась удобной, но уязвимой. Предполагалось, что к ней будут иметь доступ только операторы связи, которые подразумеваются как честные сотрудники. Это недостаток для системы в настоящее время. И на тот момент времени авторы не задумывались о дальнейшем масштабировании проекта. Проблема в том, что сейчас SS7 используют как проверенный временем протокол, а это не гарант безопасности.

Уровень защищенности системы в целом определяется наименьшим уровнем защищенности среди ее участников. То есть если какого-то из входящих в нее операторов взломали, то всю систему можно считать скомпрометированной. Или если кто-то из администраторов сети какого-либо оператора решил несколько превысить служебные полномочия и использовать SS7 в своих целях — результат будет тот же.

К сожалению, несанкционированным доступом к SS7 могут пользоваться как спецслужбы разных стран, так и злоумышленники, ведь имея к ней доступ,

можно подслушивать разговоры, определять местоположение абонента и перехватывать текстовые сообщения.

Первой систему SS7 внедрила американская компания AT&T, через несколько лет подтянулась Европа с Великобританией и к концу 80-х SS7 вытеснила все предыдущие поколения. Кроме очевидных преимуществ, повсеместное принятие этого протокола — обеспечило унификацию и совместимость телефонных сетей по всему миру, многие привычные услуги, такие как: АОН, удержание вызова, черные списки, переадресация, и даже СМС — стали возможны как раз благодаря новой версии. Но проблемы все же появились. [3]

Уязвимости протокола

Поскольку никто из создателей протокола не предполагал, что сигнальная линия будет использоваться для передачи чего-то кроме служебных сигналов, так как ее канал был отделен от голосовых и недоступен пользователям, то разработчики решили не расходовать понапрасну вычислительные ресурсы и передачу данных не шифровали. В наше время о таком и подумать страшно.

Но современным пользователям доступна самая изощренная криптография: повсеместное внедрение SSL на сайтах, активная популяризация шифрования всего и вся, VPN и мессенджеры с end-to-end шифрованием. Сайт, работающий по протоколу «http» сегодня вызывает подозрение и недоумение, суды всего мира бьются над доступом к переписке пользователей в мессенджерах. А в середине 70-х никто и не предполагал, каких невиданных масштабов достигнет сеть Интернет.

Однако, интернет начал свое победное шествие по планете, и в начале 2000-х был разработан протокол SIGTRAN, который поддерживал все функции SS7, но еще мог выполнять адресацию по протоколу IP и передавать данные через SCTP, одному из транспортных протоколов типа TCP и UDP (старые протоколы возраста SS7), но имеющий свои преимущества, такие как многопоточность и защиту от DDoS, например. Все это позволило получить доступ в служебный канал SS7, который раньше был недоступен.

Благодаря тому, что шифрования в этом канале изначально не было, а оборудование для ускорения и упрощения работы проектировалось таким образом, что источник управляющего пакета не проверялся, потому что это очень серьезно замедлило бы работу всей сети — то злоумышленник получал полный контроль над ним, без особого труда, потому что его команды было не отличить от операторских. Достаточно было только иметь компьютер с необходимым набором программного обеспечения и доступом в интернет. Особо неприятно то, что злоумышленнику абсолютно не требуется находиться близко к взламываемому абоненту, он может атаковать из любой точки планеты. Ситуация осложняется еще и тем, что работа с протоколом SS7 у подавляющего большинства провайдеров — зашита “в железе”, а поменять аппаратную прошивку далеко не так просто, как установить обновления обычной программы. Ко всему прочему — это весьма дорого и требует большего количества времени, потому организаторы связи не торопятся менять свое оборудование и переводить его на другие протоколы.

Угрозы при использовании протокола

К сожалению, с помощью атаки через этот протокол можно сделать почти все, что угодно, потому что злоумышленник организует классический перехват по принципу ататки Man In The Middle. Можно читать чужие сообщения, подделывать USSD-запросы, определять местонахождение абонента и даже слушать его телефонные разговоры или вовсе отключить ему телефонную связь. Причем, взлом сообщений сейчас стал намного опаснее, чем прямое прослушивание, потому как перехваченные сообщения позволяют получить доступ к интернет-банкингу, украсть пароли для авторизации в социальных и мессенджерах, и даже к «непробиваемому» Telegram. Двухфакторная авторизация не спасает, потому что хакеру будут доступны все коды, передаваемые в сообщениях.

Как осуществляются такие атаки?

Злоумышленник подключается к сигнальной сети SS7 и отправляет служебную команду Send Routing Info для SM (SRI4SM) в сетевой канал, указывая номер телефона атакуемого абонента в качестве параметра. Домашняя або-

нентская сеть отправляет в ответ следующую техническую информацию: IMSI (International Mobile Subscriber Identity) и адрес MSC, по которому в настоящее время предоставляет услуги подписчику. [4]

После этого злоумышленник изменяет адрес биллинговой системы в профиле подписчика на адрес своей собственной псевдобиллинговой системы (например, сообщает, что абонент прилетел на отдых и в роуминге зарегистрировался на новой биллинговой системе). Как известно, никакую проверку такая процедура не проходит. Далее атакующий вводит обновленный профиль в базу данных VLR через сообщение «Insert Subscriber Data» (ISD).

Когда атакуемый абонент совершает исходящий звонок, его коммутатор обращается к системе злоумышленника вместо фактической биллинговой системы. Система злоумышленника отправляет коммутатору команду, позволяющую перенаправить вызов третьей стороне, контролируемой злоумышленником.

В стороннем месте устанавливается конференц-связь с тремя подписчиками, две из них являются реальными (вызывающий абонент А и вызываемый В), а третий вводится злоумышленником незаконно и способен прослушивать и записывать разговор.

Соответствующим образом получаем и SMS атакуемого. Имея доступ к псевдобиллинговой системе, на которую уже зарегистрировался наш абонент, можно получить любую информацию, которая приходит или уходит с его телефона.

Что касается воровства денег с банковских карт, схема работает так: сначала киберпреступники выясняют логин и пароль жертвы для онлайн-банкинга — например, с помощью фишинга, клавиатурных шпионов или банковских троянов. Войдя в онлайн-банк, они отправляют запрос на перевод денег. Большинство современных банков требуют дополнительное подтверждение для перевода и отправляют код, чтобы убедиться, что операцию выполняет именно владелец счета.

Если банк отправляет код в SMS, то злоумышленники, пользуясь уязвимостью SS7, перехватывают сообщение и вводят код, как будто получили его на телефон жертвы. Банк переводит деньги, считая операцию абсолютно легитимной, потому что она авторизована дважды: сначала паролем, а потом — разовым кодом. В результате довольные кибермошенники получают чужие деньги без препятствий.

Истории успешных атак

Первую атаку на протокол осуществили всеми известные Стив Джобс и Стив Возняк. [5] Они взломали телефонную сеть с помощью свистка из коробки с хлопьями и устройством Blue Box. Это была атака на предыдущую версию протокола под названием SS6, до смешного примитивная, но эффективная. Седьмая версия исключала взлом с помощью таких простых способов. Но есть способы и посложнее.

Специалисты по информационной безопасности уже давно предупреждали о теоретической возможности подобного взлома, и пару лет назад это произошло на практике: в Германии была зафиксирована массовая атака на клиентов банков по данному сценарию. А совсем недавно это случилось снова, на этот раз в Великобритании: по сообщению издания Motherboard, мишенями стали некоторые клиенты банка Metro Bank.

В случае недавней атаки в Германии [1] последовательность действий злоумышленников выглядела так:

1. Компьютер жертвы заражали банковским троянцем. Троянцев довольно легко подцепить, если у вас нет защитного решения, а многие из них ведут себя так, что обнаружить их без антивируса невозможно, поэтому пользователи ничего не замечали.

С помощью такого троянца злоумышленники воровали у жертв логины и пароли для доступа в интернет-банк. Но украсть только платежную информацию в большинстве случаев недостаточно — надо еще получить тот самый код подтверждения транзакции, который банк присылает на телефон в виде сообщения.

2. С помощью того же банковского троянца воровали и номера телефонов — его часто требуется указывать при покупке в интернет-магазине, как раз перед тем как вводить номер карты. На этом моменте у мошенников были и доступ к интернет-банку, где они могли видеть, сколько денег есть у жертвы на счетах, и ее номер мобильника. Оставалось вывести деньги.

3. Далее злоумышленники, используя украденные логин и пароль интернет-банка, инициировали перевод денег с карты на свой счет. После этого, получив доступ к SS7 от лица некого оператора связи из другой страны, они переадресовывали SMS, отправленные на номер абонента немецкого оператора, на свой номер. Таким образом они получали коды подтверждения транзакций, вводили их в интернет-банке и успешно переводили на свой счет все деньги — так, что у банка даже подозрение не закрадывалось о возможной нелегитимности операции.

Атаку подтвердил и немецкий оператор, абоненты которого оказались пострадавшими в этой истории. Иностранного мобильного оператора, чей доступ в систему был использован для атаки, заблокировали, а пострадавших уведомили об атаке. Правда, нам не известно, помогло ли им это вернуть деньги.

Самые известные атаки были продемонстрированы на хакерских конгрессахю Хотя специалисты давно знали о проблемах этого протокола, одно из первых публичных обсуждений состоялось на CCC в 2008 году, немецкий эксперт по безопасности Тобиас Энгель, рассказал о способах слежки за абонентами сотовых сетей на основе этих уязвимостей, для которого достаточно знать только мобильный номер человека.

Очередной всплеск интереса к SS7 произошел после откровений Сноудена в 2013 году [3], который рассказал о проекте SkyLock, в котором американские спецслужбы эксплуатировали описываемые уязвимости для слежки за людьми.

Карстен Нол, в 2016 году поставил публичный эксперимент в эфире телепрограммы 60 Minutes телеканала CBS. Через уязвимость в SS7 он взломал телефон специально приглашенного для этого американского конгрессмена Теда

Лье. Последнего это настолько впечатлило, что он официально потребовал провести расследование этой проблемы. [3]

В данный момент операторы медленно закрывают многочисленные дыры в SS7, несмотря на то, что некоторые даже не признают их наличие. Кто-то обвиняет в разжигании паники вокруг этой проблемы, кто-то воздерживается от комментариев, кто-то говорит обтекаемые фразы, типа: «Безопасность наших клиентов стоит у нас в приоритете». Тем не менее, на сегодняшний день этому вопросу не уделяется должного внимания со стороны операторов, а доступность эксплуатации этой уязвимости существует, а это значит, что ей будут пользоваться в случае необходимости. Нет разницы, насколько она велика.

Методы защиты

Теперь рассмотрим, как пользователь может себя защитить. Для двухфакторной аутентификации можно пользоваться не только SMS. Если есть возможность, стоит использовать другие варианты — например, приложение Google Authenticator или криптографические USB-ключи. К сожалению, банки альтернативных видов двухфакторной аутентификации не приемлют, отправляя для подтверждения исключительно SMS. Но у нас есть выбор, чьи услуги использовать.

Компания Apple готовит новый механизм двухфакторной авторизации для защиты Apple ID [6]. Напомним, что завладев учетными данными Apple ID можно ни много ни мало заблокировать и полностью стереть все ваши Apple устройства удаленно. К сожалению, на данный момент пароль можно восстановить через SMS, которое в свою очередь, как мы уже знаем, можно перехватить.

Учитывая, что псевдобиллинговые системы злоумышленников в большинстве случаев представляются иностранными операторами (сообщают, что вы в международном роуминге), то достаточно просто отключить на телефоне возможность международного роуминга. Это можно сделать у оператора сотовой связи бесплатно. Если нет острой необходимости именно с этого телефона общаться в роуминге, то это решение сильно обезопасит от тех неприятностей, которые были описаны в этой статье.

Используйте надежное защитное решение на каждом устройстве. В случае описанной атаки в Германии хороший антивирус не позволил бы банковскому троянцу заразить компьютер и украсть логин и пароль от интернет-банка. И было бы уже не так важно, могут злоумышленники получить доступ к вашим SMS, или нет — до этого этапа просто не дошло бы.

Заключение

Рассмотренный в статье протокол SS7 был создан много лет тому назад. Его безопасности не уделяли должного внимания на протяжении всего этого времени, однако его все еще используют. Этот протокол использует авторизацию через SMS, что является неэффективным способом защиты от кибератак. Злоумышленники используют сетевые коммуникации для отслеживания абонентов, перехвата вызовов, отказа в обслуживании и для совершения мошеннических операций. В статье представлен обзор угроз и уязвимостей SS7. Поэтому сейчас очень важно поддерживать инструменты массового использования на актуальном уровне безопасности, регулярно проводить анализ защищенности сигнальной сети с целью выявления существующих уязвимостей и разработки мер по снижению рисков реализации угроз, а после — поддерживать параметры безопасности в актуальном состоянии.

СПИСОК ЛИТЕРАТУРЫ

1. АО «Лаборатория Касперского», 2021, .https://www.kaspersky.ru/blog/ss7-attack-intercepts-sms/17673/
2. Signaling System No. 7 (SS7/C7): Protocol, Architecture, and Applications Lee Dryburgh, Jeff Hewett
3. https://3-info.ru/post/23526
4. https://networkguru.ru/ataka-na-protokol-ss7/
5. Даниил Турковский, Москва https://meduza.io/feature/2016/06/07/my-vas-vnimatelno-slushaem
6. Apple Inc., 2021, https://support.apple.com/ru-ru/guide/iphone/iphd709a3c46/ios

УДК 004.056

Е. С. НИКОЛИНА
enikolina99@inbox.ru
Науч. руководитель – канд. техн. наук, проф. Т. А. ИВАНОВА

Уфимский государственный авиационный технический университет

СОБЛЮДЕНИЕ ТРЕБОВАНИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ОСОБЕННОСТИ ПЕРЕВОДА СОТРУДНИКОВ НА УДАЛЕННУЮ РАБОТУ

Аннотация. Данная статья посвящена проблемам удаленного доступа сотрудников в период пандемии. В статье рассматриваются основные способы организации удаленного доступа, их преимущества и недостатки. Разбираются проблемы контроля рабочего времени сотрудников и предотвращение утечек информации в условиях дистанционной работы.
***Ключевые слова*:** удаленная работа; удаленный доступ, VPN, BYOD, системы контроля рабочего времени.

Введение

Пандемия коронавируса COVID-19 заставила государственные организации и частный бизнес массово переводить сотрудников на удаленный режим работы. Дистанционный режим работы уменьшает вероятность заражения благодаря исключению значительной части контактов.

Коммерческие предприятия переводят на удаленную работу целые отделы и управления. В некоторых странах ЕС правительства официально порекомендовали предприятиям максимально широко вводить технологию удаленной работы для их сотрудников, чтобы минимизировать физические контакты между ними. Такой метод работы имеет свои плюсы и минусы как для сотрудников, так и для работодателей.

Однако стоит учитывать и минусы подобного режима работы. Существенные для работодателя недостатки удаленной работы —возрастающая сложность контроля работников, соблюдения сотрудниками режима работы, а также предотвращения утечек информации.

Основные сценарии, активно использующиеся при организации удаленной работы:

1. Концепция Bring Your Own Device (BYOD)

2. Удаленное подключение к рабочему столу

3. Использование виртуальных частных сетей (VPN).

Рассмотрим эти сценарии подробнее.

BYOD

Концепция Bring Your Own Device — глобальная тенденция в сфере информационных технологий, описывающая феномен применения личных устройств на рабочем месте для использования и подключения к корпоративной сети. В качестве таких устройств могут использоваться мобильные телефоны, планшеты, ноутбуки, жесткие диски или USB-накопители.

Концепция достигла популярности в 2009 году после того, как ее внедрила компания Intel. По их данным, количество мобильных устройств, используемых на работе, в 2009-2010 годах выросла с 10 000 до 30 000.

В сфере организации удаленной работы BYOD используется следующим образом. Сотрудники работают из дома, но на своих личных домашних компьютерах, которые используются исключительно как терминалы удаленного доступа: вся работа проходит на сервере терминалов, который организуется в серверной группировке компании.

Преимущества такого подхода заключаются в следующем:

− есть единый центр управления и мониторинга;

− на личном домашнем компьютере сотрудника не сохраняется никакая служебная информация, домашний компьютер используется исключительно как терминал удаленного доступа;

− вся информация, собранная агентом, не передается через сеть «Интернет», а остается внутри локальной сети компании — охраняемого периметра.

Главный минус работы по данному сценарию — сервер терминалов при большом числе сотрудников потребует значительных аппаратных ресурсов. Кроме того, на сервере должны быть установлены все приложения, необходимые пользователям. Еще один недостаток систем с централизованным управлением состоит в том, что при выходе из строя главного сервера теряется доступ к офису, и работа становится невозможной.

Удаленное подключение к рабочему столу.

В этом случае вся офисная техника остается на месте во включенном состоянии. Сотрудники подключаются к своим рабочим станциям либо с помощью стандартных RDP-средств, встроенных в ОС Windows, либо используя программное обеспечение от сторонних разработчиков.

Наиболее популярные приложения для подключения к рабочему месту:

- AMMYY Admin;
- TeamViewer;
- Anydesk;

Основное преимущество этого сценария состоит в отсутствии необходимости вносить изменения в инфраструктуру.

Однако при использовании данного подхода возрастает нагрузка на работников службы информационных технологий и информационной безопасности. Они вынуждены обеспечивать функционирование рабочих станций в офисе и контролировать бесперебойную связь между домашними компьютерами сотрудников и офисными рабочими станциями. В некоторых случаях приходится поддерживать работоспособность домашних компьютеров сотрудников.

Второй серьезный минус сценария состоит в том, что все подключения к рабочим станциям при использовании TeamViewer, AnyDesk и похожих продуктов третьих сторон происходят через серверы этих приложений. Следовательно, эти подключения находятся вне контроля служб информационных технологий и информационной безопасности компании и могут оказаться небезопасными. Да, можно создать свой собственный сервер TeamViewer, что заманчиво; но, во-первых, быстро это не сделаешь, а во-вторых, при ближайшем рассмотрении это приводит к весьма большим расходам.

Третий недостаток – необходимость следить за тем, чтобы были включены рабочие места в офисе. Функция Wake-on-LAN решает эту проблему, но она поддерживается далеко не всеми устройствами.

По вышеприведенным причинам, данный способ подключения является не самым надежным.

VPN

Virtual Private Network – виртуальная частная сеть - совокупность технологий, позволяющих обеспечить одно или несколько сетевых соединений поверх другой сети.

Виды VPN-подключений:

- Узел-Узел. Соединение двух внешних устройств.
- Узел-Сеть. VPN-подключение удаленного доступа типа «узел-сеть» («клиент-сервер», «клиент-маршрутизатор») связывает с VPN-сервером (внутренней сетью организации) любое внешнее устройство, прошедшее авторизацию, и дает пользователям возможность работать дома или в дороге, получая доступ к серверу частной сети с помощью инфраструктуры публичной сети
- Сеть-Сеть. VPN-подключения типа «сеть-сеть» («сервер-сервер», «маршрутизатор-маршрутизатор») связывает два сегмента частной сети, позволяя организациям устанавливать маршрутизируемые подключения между отдельными структурами (или между другими организациями) обеспечивая безопасность связи.

В концепции удаленной работы сотрудников, очевидно, используется VPN вида «Узел-Сеть»

Наиболее распространенные сервисы:

- PPTP – Point-to-Point Tunneling Protocol. Поддерживается абсолютным большинством современных операционных систем. Не требует много вычислительных мощностей. К недостаткам можно отнести устаревшие методы шифрования, плохую архитектуру, ошибки в реализации протокола от Microsoft. Нет шифрования по умолчанию, на взлом требуется менее суток. Используется, когда защита данных не очень важна или когда нет других вариантов.
- L2TP – Layer 2 Tunneling Protocol. Не смотря на название, является протоколом пятого уровня модели OSI. По сравнению с PPTP более эффективен для построения виртуальных сетей, но также более требователен к вычис-

лительным ресурсам. Работает совместно с другими протоколами, чаще всего с IPSec. Используется интернет-провайдерами и корпоративными пользователями.

− IPSec – Internet Protocol Security – группа протоколов и стандартов для безопасных соединений. Обладает высокой надежностью алгоритмов. Сложен в настройке (следовательно, снижение защиты, если настроить неправильно) Требует много вычислительных ресурсов; этот недостаток компенсируется путем аппаратного ускорения алгоритма шифрования AEC. Часто используется совместно с другими технологиями (GRE over IPsec, Cisco DMVPN) в VPN типа «сеть-сеть».

− OpenVPN. Имеет открытый код, реализован практически для всех платформ, считается очень надежным. Не совместим с подавляющим большинством продуктов от известных сетевых поставщиков.

Преимущества данного подхода:

− сотрудник работает так, как будто находится в офисе. Службы информационных технологий и информационной безопасности имеют удаленный доступ к рабочим станциям сотрудников точно так же, как это было в офисе (естественно, за исключением того, что для подключенных по VPN рабочих станций сетевые администраторы, как правило, выделяют другой пул адресов; но при стабильно работающих доменных службах DNS это не должно вызывать проблем — рабочая станция корректно «находится» в сети по своему имени);

− нет необходимости использовать личный компьютер для выполнения работы;

− отсутствует необходимость дополнительной настройки приложений.

Минусы:

− Низкая скорость интернета. На дополнительное шифрование требуется время. Также часто трафик проходит большее расстояние, что связано с удаленностью расположения VPN-сервера.

− Периодический разрыв VPN-подключения, внезапный выход трафика в публичную сеть. Часто можно не заметить разрыв подключения и утеч-

ку данных, также VPN-соединение может не восстанавливаться автоматически, что не удобно. Во современных ОС на базе Windows предусмотрена функция VPN Reconnect. Если ее нет, то придется использовать особые программы или специальные настройки маршрутизации, которые контролируют VPN-соединение и в случае его разрыва сначала блокируют передаваемую информацию, закрывают приложения, потом обновляют VPN-подключение.

− IPv6 почти никогда не поддерживается VPN. Следовательно, когда в публичной сети используется IPv6, и в интернет-ресурсе он также поддерживается, трафик пойдет по умолчанию по открытой IPv6 сети. Чтобы такого не произошло можно просто отключить IPv6 в ОС.

− На практике часто DNS-запросы обрабатываются DNS-серверами публичной сети (а не виртуальной, защищенной). В случае их некорректного ответа можно получить поддельный адрес запрашиваемого домена. Так, ничего не подозревающие пользователи могут быть перенаправлены, например, на сайты мошеннических онлайн-банков. Также по DNS-серверам можно определить примерную геолокацию и интернет-провайдера пользователя.

− Присутствуют также разнообразные юридические аспекты. Во-первых, это отличия в законодательстве разных государств. VPN-клиент и VPN-сервер часто находятся в разных странах. Также трафик может проходить через третью страну транзитом. Таким образом существует возможность сохранить себе копию передаваемых данных для дальнейшей расшифровки и изучения.

Контроль рабочего времени сотрудников

Очевидно, что контроль удаленных сотрудников необходим. Однако нельзя забывать про индивидуальный подход, основанный на размере штата, особенностях трудовой деятельности и отношениях руководства с подчиненными. Благодаря этому осуществляется контроль и учет рабочего времени территориально удаленных от офиса сотрудников с максимальной пользой для бизнес-процесса.

В зависимости от этих условий используются следующие методы контроля занятости удаленного персонала:

1. Метод контрольных точек.

Для мониторинга малочисленного штата, который занимается преимущественно творческим трудом или разработкой, подойдет методика контрольных точек, заключающийся в проверке выполнения основных этапов поставленной задачи. Руководитель с помощью коммуникаций через различные каналы связи, онлайн-совещаний и отметок о выполнении подзадач в общедоступной информационной системе получает представление об общем ходе проекта или о возможных проблемах. В результате такого подхода он может принять своевременные управленческие решения и, при необходимости, спасти ситуацию. Контроль со стороны руководства удаленной работы переведенных на нее сотрудников скорее качественный, а не количественный: важно не когда делал, а сделал ли в полном объеме к определенному сроку.

Рабочий процесс персонала свободен от отслеживания их действий на компьютере и посекундного учета рабочего времени, а работодатель избавлен от необходимости анализа логов учетной системы. Проект движется, сроки соблюдаются — значит, все отлично (не важно, когда именно специалист выполняет свои задачи: в регламентированные рабочие интервалы или авралом по ночам и в выходные).

Такой способ нацелен на конечный результат с контролем промежуточных этапов.

Он дает более широкую свободу для исполнителей, но трудно применим к значительному штату с ежедневной документальной работой.

Его минусом является невозможность вести контроль действий удаленных территориально сотрудников на домашнем ПК по отношению к корпоративной информации: несанкционированный доступ, порча или распространение могут быть своевременно не обнаружены.

Контроль значительного по численности штата, занятого разнородными обязанностями (менеджеры, бухгалтеры, разработчики), непросто осуществлять по методу контрольных точек.

Во-первых, руководитель может быть не в курсе ежедневных обязанностей отдельных. Чтобы удостовериться, что человек решает именно нужную в данный момент задачу, ему потребуется потратить время, чтобы вникнуть в нюансы работы каждого подчиненного

Во-вторых, такой контроль работников на удаленке при значительном и неоднородном штате будет занимать много времени, даже если эту задачу делегировать начальникам отделов.

В-третьих, метод контрольных точек не спасает от нежелательных форм обращения с конфиденциальной информацией в условиях, когда все сотрудники имеют удаленный доступ к корпоративной системе.

Наконец, рабочий регламент для некоторых должностей очень важен (решающим становится сам процесс, а не результат). Например, специалист техподдержки или менеджер-консультант не имеет права отвлекаться и пропадать из зоны доступа в определенные рабочие часы. Его заместительная работа в другое время никому не интересна. В этом случае было бы более полезным слежение за сотрудниками на ПК на протяжение рабочей смены

2. Метод непрерывного мониторинга

Организуется с помощью специализированного ПО и автоматического учета рабочего времени. В результате применения программы-шпиона, о деятельности которой сотрудник не догадываться, руководитель получает на выходе подробные отчеты о занятости и эффективности каждой единицы штата.

Такой мониторинг сотрудников может стать несколько более затратным по начальным вложениям на внедрение системы контроля, настройку прав доступа к программам или интернет-ресурсам для пользователей, должностей и отделов, однако впоследствии окупается полностью автономной работой программы.

Руководителю достаточно периодически просматривать отчеты системы мониторинга и делать соответствующие выводы на основе рассчитанных данных о продуктивности в различных разрезах.

Служба безопасности, которая часто имеется на крупных предприятиях, будет получать от системы уведомления о нарушениях со стороны персонала, сведения о запускаемых ими программах или посещаемых ресурсах, сохраненные фотографии рабочих экранов, логи нажатий клавиш для более точного анализа.

Используя подходящие методы для контроля действий удаленных от офиса сотрудников, можно организовать дистанционную работу в условиях масштабной организации, понимая, что четкое выполнение служебных обязанностей непрерывно отслеживается, а нежелательное обращение с корпоративными данными может быть своевременно зафиксировано и предотвращено.

Предотвращение утечек информации

Очевидно, что при дистанционной работе сотрудников компании число потенциальных каналов утечки информации увеличится. Поэтому можно выделить следующие особенности работы ИБ-отделов компаний при организации удаленной работы сотрудников: Отдел информационной безопасности должен убедиться в том, что все подключения по протоколам удаленного доступа выполняются безопасно, с использованием соответствующих непросроченных сертификатов, шифрования, сложных паролей и т. д. По возможности следует применять системы одноразовых паролей или регулярно менять многоразовые, при этом используя технологии генерации сложных паролей.

Необходимо убедиться в том, что офисные рабочие станции и носители, передаваемые сотрудникам, не содержат сведений, подпадающих под регламенты коммерческой тайны и конфиденциальной информации (включая персональные данные сотрудников). Необходимо убедиться в том, что конфигурации агентов обеспечивают сбор необходимой информации о работе пользователей, а также блокировку нежелательных приложений и доступа к запрещенным сайтам.

При работе в офисе сотрудник отдела ИБ имеет возможность под любым предлогом пройти по офису и посмотреть на мониторы сотрудников. Очевидно, что при работе на «удаленке» это невозможно, поэтому необходимо удостовериться, что дистанционный просмотр рабочих столов пользователей включен.

Вывод

При переводе сотрудников на удаленную работу возникает целый комплекс проблем, связанных как с соблюдением режима работы сотрудников, так и с соответствием требованиям информационной безопасности.

Перечисленные в данной статье методы описывают возможности организации удаленной работы сотрудников, а также возможности учета и контроля выполнения заданий.

Необходимо учитывать, что при решении данной проблемы возникает дополнительная нагрузка на сотрудников ИТ-отдела и специалистов по информационной безопасности. Переход на удаленный режим работы потребует дополнительных финансовых и человеческих ресурсов и высокую квалификацию сотрудников.

В целом, задача перехода на дистанционный режим работы решаема и сводится к выбору методов организации удаленного доступа в зависимости от конкретных требований компании.

СПИСОК ЛИТЕРАТУРЫ

1. Кейсы для применения средств анализа сетевых аномалий: контроль удаленного доступа// https://habr.com/ru/company/cisco/blog/493786/
2. VPN: еще раз просто о сложном// https://habr.com/ru/post/534250/

УДК 004.056

И. Н. РЕЗЯПОВ, А. Р. ТАХАУТДИНОВ, ЛЫОНГ ХА ЧА МИ
rezyapov101100@gmail.com, aidartahautdinov@gmail.com, lhtrmi0212@gmail.com
Науч. руководв. – доц. В. Е. КЛАДОВ

Уфимский государственный авиационный технический университет

ТЕХНОЛОГИИ ОБНАРУЖЕНИЯ МАТЕРИАЛОВ, СВЯЗАННЫХ С ЖЕСТОКИМ ОБРАЩЕНИЕМ С ДЕТЬМИ В СЕТИ ИНТЕРНЕТ

Аннотация. В статье рассмотрены технологии защиты детей в сети Интернет, в частности системы обнаружения материалов, связанных с насилием над детьми и их эксплуатацией. Отмечена важность совместной работы организаций по защите детей, правоохранительных органов и крупных ИТ-компаний.
Ключевые слова: информационные технологии; защита детей; CSAM; PhotoDNA; CSAM Detection.

Влияние новых информационно-коммуникационных технологий на ситуацию с насилием над детьми и их эксплуатацией вызывает все большую озабоченность в силу целого ряда факторов. За последние несколько десятилетий бурное развитие таких технологий привело к масштабным общественным трансформациям во всем мире. Развитие инновационных технологий привело также к резкому повышению доступности компьютерной техники, увеличению скорости передачи данных и распространению мобильных устройств.

В таких условиях использование информационно-коммуникационных технологий позволяет сократить издержки и упростить работу на всех этапах преступного действия. Цифровая техника превратилась в дешевое и доступное средство, облегчающее производство и широкое распространение материалов запрещенного характера.

По данным организации Internet Watch Foundation, в 2020 году было обработано 299,616 сообщений о жестоком обращении с детьми, из которых 153,383 были подтверждены, что на 16% больше по сравнению с 2019 годом. [1]

Тем не менее в данной области начинает вырисовываться ряд многообещающих подходов. В частности, крупными ИТ-компаниями прилагаются уси-

лия для разработки и применения новых технологий, позволяющих осуществлять обмен большими объемами данных между правоохранительными органами, а также организациями по защите детей в рамках расследования дел о сексуальном насилии над детьми и их эксплуатацией с целью противодействия созданию и распространения таких материалов.

Одним из способов эффективного обнаружения изображений с подобным контентом является вычисление их хэша и сравнение с базой данных с набором хэшей изображений, которые уже определены как незаконные. Поддерживанием подобных баз данных занимаются специальные контролирующие организации, сотрудничающие с правоохранительными органами. К таким организациям можно отнести вышеупомянутую Internet Watch Foundation (IWF) созданную в Великобритании для надзора за Интернетом, Национальный центр пропавших без вести и эксплуатируемых детей (NCMEC), основанный в 1984 году Конгрессом США. В России разработкой подобной базы данных занималась Лига безопасного интернета - неправительственная организация, созданная с целью цензурирования Интернета в 2011 году. [2]

По этому принципу работает технология PhotoDNA, разработанная и поддерживающаяся компанией Microsoft с 2009 года, которая вычисляет цифровую сигнатуру изображения на основе визуального содержимого. Суть метода заключается в том, что сначала исходное изображение конвертируется в черно-белый формат, затем сегментируется и для каждого сегмента находится значение интенсивности градиента, которые, в совокупности, образуют уникальный паттерн для изображения. Благодаря этому возможно идентифицировать даже модифицированное изображение, подвергнутое изменению размера или сохраненное в другом формате. Эта технология используется такими онлайн-платформами как OneDrive, Google Gmail, Twitter, Facebook, Adobe Systems. [3]

В августе 2021 года подобную технологию так же анонсировала компания Apple в своем пакете мер по защите детей, который будет введен на устрой-

ствах с операционной системой iOS 15, iPadOS 15, watchOS 8 и macOS Monterey. [4]

Согласно опубликованному техническому документу, технология называется CSAM Detection. Ее работа заключается в сравнении изображений на устройствах пользователей с базой данных заранее хэшированных изображений при их выгрузке на облачный сервис iCloud. Базы данных разработаны совместно с NCMEC и другими организациями по защите детей. [5]

Механизм, по которому изображения преобразуются в хэш-сумму, называется NeuralHash. Он устойчив к различным преобразованиям, например, к таким как изменение размера или перекодирование. Это добивается при помощи сверточной нейронной сети и самоконтролируемого контрастного обучения. Нейросеть обучена так, чтобы при вводе почти одинаковых изображений, их результирующие векторы также были очень похожи. Близкие друг к другу векторы определяются с помощью технологии locality sensitive hashing (LSH).

Процесс сравнения происходит через криптографический протокол «private set intersection», который позволяет определять наличие совпадения, не раскрывая сам результат. Впоследствии зашифрованный результат, хэш-сумма, а также визуальная репрезентация изображения помещаются в так называемый «safety voucher» (ваучер безопасности), который загружается в iCloud вместе с изображением.

Только при преодолении определенного порога совпадений хэш-сумм появляется возможность раскрыть содержание ваучеров безопасности. За это отвечает механизм «threshold secret sharing». Пороговое разделение секрета происходит таким образом, что, если секрет разделен на тысячу частей, а порог равен, например, десяти, то при наличии одиннадцати любых частей появляется возможность восстановить секрет. Секретом в данном случае являются сами ваучеры безопасности.

С целью исключения ложного срабатывания системы, последним этапом является ручная проверка отчета системы о совпадении сотрудником компании.

В случае подтверждения наличия запрещенного контента учетная запись пользователя будет заблокирована, а информация доведена до NCMEC и правоохранительных органов.

Однако, 3 сентября 2021 года компания Apple объявила о намерении отложить запуск этой и других функций по защите детей с целью их улучшения после критики, связанной с нарушением конфиденциальности пользователей. [4]

Как известно, практически любая хэш-функция имеет коллизии, и в данном случае это означает, что два абсолютно разных изображения могут иметь одинаковый хэш. Такая проблема присутствует в скрытом в операционной системе iOS 14.3 алгоритме NeuralHash, найденном пользователем веб-сервиса GitHub. [6] Уже во время первых проверок этого алгоритма было обнаружено, что, зная находящийся в базе данных алгоритма хэш, можно получить ложноположительный результат, при котором разные изображения идентифицируются как одинаковые. [7]

Следующим недостатком является тот факт, что работа подобной системы напрямую связана с содержанием базы данных, с элементами которой сравниваются файлы на клиентских устройствах. Это означает, что систему можно перепрофилировать для обнаружения любого контента, не связанного с CSAM, изменив содержание базы данных. С подобной проблемой столкнулись ученые из Принстонского университета, которые несколько лет работали над аналогичной системой. После аналитического изучения системы и создания рабочего прототипа, они пришли к выводу, что на техническом уровне система ни при каких обстоятельствах не может ограничиваться поиском только одного типа контента. [8]

Таким образом, рассмотренные в статье технологии наряду с совместной работой органов по защите детей являются эффективным инструментом противодействия созданию, распространению и хранению материалов, связанных с насилием над детьми и их эксплуатацией. При этом подобные технологии необходимо развивать таким образом, чтобы они не нарушали принципы кон-

фиденциальности пользователей, но, безусловно, это не должно происходить за счет безопасности детей.

СПИСОК ЛИТЕРАТУРЫ

1. Face the facts The annual report 2020. [Электронный ресурс] URL: https://annualreport2020.iwf.org.uk
2. Лига безопасного интернета подготовила базу образов детской порнографии [Электронный ресурс] URL: http://www.ligainternet.ru/news/news-detail.php?ID=5068
3. PHOTODNA – ROBUST HASHING THAT FINDS ONLINE CHILD SEXUAL ABUSE MATERIAL [Электронный ресурс] URL: https://www.netclean.com/technical-model-national-response/photodna/
4. Expanded Protections for Children [Электронный ресурс] URL: https://www.apple.com/child-safety/#footnote-1
5. CSAM Detection Technical Summary August 2021. [Электронный ресурс] URL: https://www.apple.com/child-safety/pdf/CSAM_Detection_Technical_Summary.pdf
6. Исследователь обнаружил, что код проверки изображений NeuralHash в iOS присутствует еще с версии 14.3 [Электронный ресурс] URL: https://habr.com/ru/news/t/573592/
7. Working Collision? [Электронный ресурс] URL: https://github.com/AsuharietYgvar/AppleNeuralHash2ONNX/issues/1
8. Ученые Принстонского университета рассказали о создании аналогичной Apple системы детской безопасности [Электронный ресурс] URL: https://rb.ru/news/researchers-system-apple/?utm_source=yxnews&utm_medium=desktop

УДК 05.04

Р. О. САЙПУШЕВ
r.saipusheff@yandex.ru
Науч. руководитель – канд. техн. наук, доц. Т. А. ИВАНОВА

Уфимский государственный авиационный технический университет

ЗАЩИТА WEB-РЕСУРСОВ ОТ КИБЕРАТАК И УДАЛЕННОГО ДОСТУПА

Аннотация. В данной статье рассматривается проблема защиты веб-сайтов, а в частности возможные типы защиты от удаленного доступа к веб-приложениям.
Ключевые слова: WAF; песочница; сетевые шпионы; вирусы.

В настоящее время невозможно представить себе практически любую сферу человеческой жизнедеятельности без участия (и интеграции) в ней информационных систем, которые занимаются обеспечением различных функций, начиная от операций, связанных с торговлей, и заканчивая поддержкой электронного правительства. Информационные системы поддерживаются миллиардами веб-серверов, расположенных по всему миру.

Во всем этом множестве информационных ресурсов (систем) хранятся не только данные персонального характера, но и финансовая информация, как никто постоянно нуждающаяся в защите в процессе своего хранения, передачи и модификации.

Выход финансовых потоков за пределы банковской сферы, появление различных платежных систем и торговых операций, заключающихся удаленно, стали причиной расширения круга потенциальных злоумышленников, имеющих возможность посягнуть на эти объекты.

Средства защиты веб-приложений

Средства защиты веб-сайтов (приложений) — программные или аппаратно-программные комплексы, предназначенные для обеспечения защиты веб-приложений и различных веб-сервисов.К средствам защиты веб-сайтов можно отнести следующие:

- Web Application Firewall (WAF).

- Средства анализа веб-сайтов на наличие вирусов.
- Балансировщики нагрузки на веб-приложения.
- Средства защиты от DDoS.
- Сканеры защищенности веб-приложений (WASS).

WAF - средства фильтрации трафика прикладного уровня, специально ориентированные на веб-приложения. Применение Web Application Firewall традиционно считается наиболее эффективным подходом к защите веб-ресурсов. WAF может быть реализован как облачный сервис, агент на веб-сервере или специализированное железное или виртуальное устройство.

Традиционно считается, что прикладной уровень — это последний уровень модели и выше него располагаются только данные конечных приложений, которые не могут быть формализованы и сгруппированы. Однако с развитием стандартов представления информации прикладными сервисами уже можно говорить о том, что, частично, данные, которыми оперируют определенные группы приложений, хорошо формализуются, и правила их представления, по сути, являются некими проприетарными протоколами или, упрощенно говоря, закономерностями.

Классическое размещение WAF в сети — в режиме обратного прокси-сервера, перед защищаемыми веб-серверами. В зависимости от производителя могут поддерживаться и другие режимы работы — например, прозрачный прокси-сервер, мост или даже пассивный режим, когда продукт работает с репликацией трафика.

После установки WAF и пуска продуктивного трафика сразу же начинает работу основной компонент защиты — машинное обучение, в ходе которого составляется эталонная модель коммуникации с объектом защиты, и таким образом формируется «белый» список допустимых идентификаторов доступа. На данный момент в веб-приложениях используются три типа идентификатора доступа: HTTP-параметры (в представлениях типа: Raw, XML, JSON), идентификатор ресурса (URL, URN), идентификатор сессии (cookie). Задача WAF состо-

ит в определении допустимых значений идентификаторов для веб-приложения. Из определенных значений впоследствии будет состоять эталонная (позитивная) модель.

Угроза внедрения вредоносных программ. В результате такой атаки пользователи и владельцы сайта могут не сразу заметить какие-либо изменения. Тем не менее вредоносная программа сможет производить зловредные действия, включая переадресацию на вредоносный или мошеннический сайт, кражу персональных данных пользователей, заражение посетителей веб-сайта вирусами и так далее.

Угроза заключается в стремлении запустить на хосте ИСПДн различные предварительно внедренные вредоносные программы: программы-закладки, вирусы, «сетевые шпионы», основная цель которых - нарушение конфиденциальности, целостности, доступности информации и полный контроль за работой хоста. Кроме того, возможен несанкционированный запуск прикладных программ пользователей для несанкционированного получения необходимых нарушителю данных, для запуска управляемых прикладной программой процессов и др.

Выделяют три подкласса данных угроз:

- распространение файлов, содержащих несанкционированный исполняемый код;
- удаленный запуск приложения путем переполнения буфера приложений-серверов;
- удаленный запуск приложения путем использования возможностей удаленного управления системой, предоставляемых скрытыми программными и аппаратными закладками, либо используемыми штатными средствами.

Типовые угрозы первого из указанных подклассов основываются на активизации распространяемых файлов при случайном обращении к ним. Примерами таких файлов могут служить: файлы, содержащие исполняемый код в вид документы, содержащие исполняемый код в виде элементов ActiveX, Java-

апплетов, интерпретируемых скриптов (например, тексты на JavaScript); файлы, содержащие исполняемые коды программ. Для распространения файлов могут использоваться службы электронной почты, передачи файлов, сетевой файловой системы.

При угрозах второго подкласса используются недостатки программ, реализующих сетевые сервисы (в частности, отсутствие контроля за переполнением буфера). Настройкой системных регистров иногда удается переключить процессор после прерывания, вызванного переполнением буфера, на исполнение кода, содержащегося за границей буфера. Примером реализации такой угрозы может служить внедрение широко известного «вируса Морриса».

При угрозах третьего подкласса нарушитель использует возможности удаленного управления системой, предоставляемые скрытыми компонентами (например, «троянскими» программами типа Back. Orifice, Net Bus), либо штатными средствами управления и администрирования компьютерных сетей (Landesk Management Suite, Managewise, Back Orifice и т. п.). В результате их использования удается добиться удаленного контроля над станцией в сети.

Решение проблемы с удаленным доступом

1. «Песочницы» - системы для изолированного запуска программ

MBOX – ее задача, сделать так, чтобы приложение не смогло ничего записать в файловую систему. Для этого он создает специальную виртуальную ФС, на которую перенаправляет все запросы ввода/вывода. В результате под управлением Mbox приложение работает как ни в чем не бывало, однако в ходе его работы ты получаешь возможность применить или отвергнуть те или иные изменения виртуальной файловой системы к файловой системе реальной.

Sandbox полностью отрезает приложение от внешнего мира, позволяя читать только stdin (то есть на вход запущенного в песочнице приложения можно передать данные другого приложения), а писать только в stdout (выводить данные на экран или перенаправлять другому приложению). Все остальное, включая доступ к файловой системе, сигналам, другим процессам и сети, запрещено.

2. Комплексные антивирусные средства - Internet Security комплекс включает в себя антивирус, фаервол, антишпион, антиспам, антифишинг, а также функции, осуществляющие эффективную защиту при посещении интернет-ресурсов, во время выполнения платежей, перевода денежных средств через сеть. Антивирусное программное обеспечение может контролировать сетевой трафик, блокировать посещения опасных сайтов и защищать ящик электронной почты от спама. Программы Internet Security надежно защищают компьютер от вирусных атак, восстанавливают поврежденные файлы. В комплексных антивирусных продуктах, как правило, используются облачные технологии, песочница. Среди наиболее популярных в России: Kaspersky Internet Security, ESET NOD32 Smart Security, Dr.Web Security Space, Comodo Internet Security и Norton Security Deluxe. Комплексные антивирусные программы Internet Security могут быть платными и бесплатными. Главное преимущество платных антивирусников состоит в том, что они надежно защищают компьютеры во время активного пользования интернетом, тогда как не во всех бесплатных продуктах присутствует веб-антивирус.

СПИСОК ЛИТЕРАТУРЫ

1. https://www.anti-malware.ru/security/web-application-firewall
2. https://totrdlo.ru/ugroz-vnedreniya-po-seti-vredonosnyh-programm-ugrozy-udalennogo.html
3. https://www.anti-malware.ru/threats/unwanted-content
4. https://zoo-mania.ru/internet/pesochnica-dlya-zapuska-programm-v-izolirovannoi-srede-obzor-programm/
5. https://www.anti-malware.ru/security/internet-security

УДК 004.056

М. А. САЛМИН, А. В. МУЛИНА, Е. И. КОТОВ
kambr1g00@gmail.com alina.mulina297@gmail.com faf.fdfds@gmail.com
Науч. руководов. – доц. В. Е. КЛАДОВ

Уфимский государственный авиационный технический университет

АНАЛИЗ УГРОЗ ПРИ РЕАЛИЗАЦИИ ПРОТОКОЛА MQTT ДЛЯ ИНТЕРНЕТА ВЕЩЕЙ

Аннотация. Задачи данной статьи – акцентировать внимание на безопасности реализации передачи данных при использовании протокола MQTT для IoT. Рассмотреть основные принципы работы протокола, его уязвимости и методы защиты от них.
Ключевые слова: интернет-вещей; протокол MQTT; информационная безопасность; информационные технологии.

На сегодняшний день стремительными темпами развивается технология интернета вещей (Internet of Things, IoT). Это концепция сети передачи данных между физическими объектами оснащенными встроенными средствами и технологиями для взаимодействия друг с другом или с внешней средой. IoT-технологии - одна из самых популярных технологий настоящего времени. Из 21.7 миллиарда активных соединений, более половины (54%) - соединения IoT. К 2025 году ожидается рост IoT-соединений до 30 миллиардов. [1]

Чтобы обеспечить беспрерывную работу всей сети устройств, учитывая их ограниченные вычислительные и энергетические мощности, разрабатываются “легкие” протоколы передачи данных, охватывающих весь стек OSI. Из-за этого возможностей угроз безопасности становится больше. Так, проект OWASP в 2018 году создали рейтинг 10 самых уязвимых направлений для технологии IoT, 2 место в рейтинге занимают небезопасные сетевые службы. [2]

Рассматривая архитектурную модель IoT-систем, сетевой уровень представлен универсальной сетевой моделью TCP/IP. Модель описывает различные протоколы и технологии, которые организуют сеть, а также обеспечивают ее функционирование. Основными протоколами,

представляющими прикладной уровень сетевой модели являются: MQTT , HTTP , CoAP, AMQP, DDS, XMPP, OPC UA [3].

Одним из наиболее применяемых протоколов является MQTT. С точки зрения использования сетей «Интернет вещей» протокол MQTT очень удобен при массовой рассылке информации одновременно большому числу устройств.

Структура сообщений MQTT сообщение состоит из нескольких частей:

- Фиксированный заголовок (присутствует по всех сообщениях)
- Переменный заголовок (присутствует только в определенных сообщениях)
- Данные (присутствует только в определенных сообщениях) [4]

Структура фиксированного заголовка представлена на рис. 1. Фиксированный заголовок состоит из:

- *Message Type* – тип сообщения
- *Flags specific to each MQTT packet* – вспомогательные флаги. Их наличие и состояние зависит от типа сообщения.
- *Remaining Length* – длина текущего сообщения (переменный заголовок + данные). Занимает от 1 до 4 байта.

Рис. 1. Фиксированный заголовок

Четыре старших бита первого байта фиксированного заголовка отведены под специальные флаги (рис.2).

Рис. 2. Четыре старших бита первого байта фиксированного заголовка

Применяемые флаги:

– *DUP* – флаг дубликата. Используется в типах PUBLISH, SUBSCRIBE, UNSUBSCRIBE, PUBREL. Он устанавливается, когда клиент или MQTT шлюз совершает повторную отправку пакета. Если установлен данный флаг, переменный заголовок должен содержать Message ID

– *QoS* – флаг качества обслуживания (0,1,2)

– *RETAIN* – используется в сообщениях с типом PUBLISH. Если установлен флаг, шлюз сохраняет опубликованные данные. При следующей подписке на данный топик, шлюзом будет отправлено сообщение с этим флагом.

Переменный заголовок помещается лишь в некоторые заголовки. В нем содержится такая информация, как:

– *Packet identifier* – идентификатор пакета, присутствует во всех типах сообщений, кроме: CONNECT, CONNACK, PUBLISH(с QoS <1), PINGREQ, PINGRESP, DISCONNECT

– *Protocol name* – название протокола (только в сообщениях типа CONNECT)

– *Protocol version* – версия протокола (только в сообщениях типа CONNECT)

– *Connect flags* – флаги указывающие на поведение клиента при подключении

Bit	7	6	5	4	3	2	1	0
Byte 8	User name	Password	Will Retain	Will QoS		Will Flag	Clean Session	Reserved

Рис. 3. Структура переменного заголовка

Флаги, используемые в переменном заголовке:

– *User name* – используется для аутентификации клиента (указывается имя пользователя)

– *Password* – используется для аутентификации клиента (указывается пароль)

– *Will Retain* – при установке в 1, шлюз хранит у себя Will Message.

– *Will QoS*– является обязательным, если установлены флаги Will Flag, Will QoS и Will retain .

– *Will Flag* - если установлен флаг и клиент отключается от шлюза без отправки сообщения DISCONNECT (например при обрыве связи), шлюз оповещает об этом всех подключенных клиентов через Will Message.

– *Clean Session* – Если установлен «0» шлюз сохраняет сессию, подписки клиента, а так же при повторном подключении передаст ему все сообщения с QoS1 и QoS2, которые были получены шлюзом во время отключения клиента. Если установлен «1», при повторном подключении клиент вынужден заново подписываться на топики. [5]

Данные сообщений, их содержание и формат в MQTT определяются в приложении. Размер данных может быть вычислен путем вычитания длины переменного заголовка из Remaining Length.

Протокол MQTT работает поверх TCP/IP. Пример организации обмена сообщениями по протоколу MQTT представлен на рис. 3.

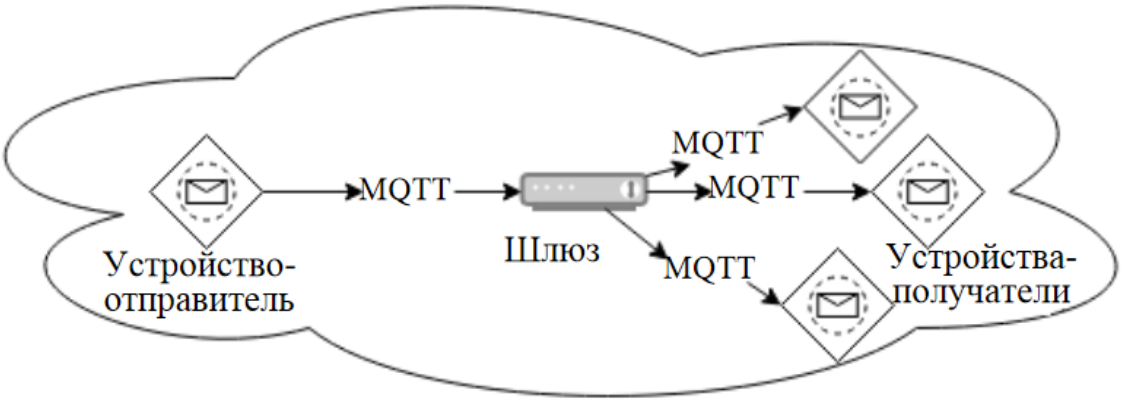


Рис. 4. Процесс обмена сообщениями по протоколу MQTT

Рис. 5. Процесс обмена сообщениями по протоколу MQTT

Сначала сообщение отправляется на шлюз, затем перенаправляется получателю или группе получателей. Тем самым, протокол MQTT позволяет снизить энергопотребление при передаче группе других устройств, за счет того, что маршрутизацию сообщений обеспечивает устройство-шлюз. В такой схеме, издатель - устройство отправляющее сообщение (например исполнительное устройство или датчик), подписчик - устройство, получающее и обрабатывающее сообщения, и шлюз (или брокер) - устройство, обеспечивающее логистику сообщений от издателей к подписчикам. Именно шлюх отвечает за аутентификацию и управление доступом, а также может хранить сообщения при необходимости.

В протоколе MQTT поддерживаются уровни качества передачи QoS (Quality of Service):

— доставка без подтверждения (QoS 0);

— доставка один раз (QoS 1);

— доставка гарантированно только один раз (QoS 2).

По умолчанию в протоколе MQTT (Message Queuing Telemetry Transport) используется порт 1883 для соединения по открытому каналу, для соединения по закрытому каналу (TSL/SSL-соединение) используется порт 8883. На транспортном и сетевом уровне используется TCP/IP. Следовательно, уязвимости перечисленных протоколов могут быть реализованы для IoT-сети, которая использует протокол MQTT. [6]

С точки зрения безопасности, в протоколе MQTT возможна реализация следующих угроз:

− атака «человек посередине» при передаче информации, в том числе для аутентификации, по открытому каналу;

− получение несанкционированного доступа к информационным потокам;

− атаки «отказ в обслуживании», например, с помощью переполнения очереди буфера на порту.

Из документации протокола MQTT Version 3.1.1 OASIS Standard. 2014, следует, что этот протокол предназначен для взаимодействия M2M (машина-машина). Однако существует угроза безопасности обмена данных. [7] Один из вариантов угрозы представлен на рис. 6. Один пользователь, имеющий уникальную пару «логин–пароль», может иметь неограниченное число устройств, каждое из которых имеет уникальный в данной сети идентификатор clientId. Таким образом, для каждого устройства одного пользователя пара «логин–пароль» одинакова. В случае компрометации, например, при соединении без криптографической защиты по протоколу TLS или успешной атаки на перебор паролей, злоумышленник сможет «прослушивать» всю информацию, циркулирующую в сети путем подписок на всевозможные темы. [8]

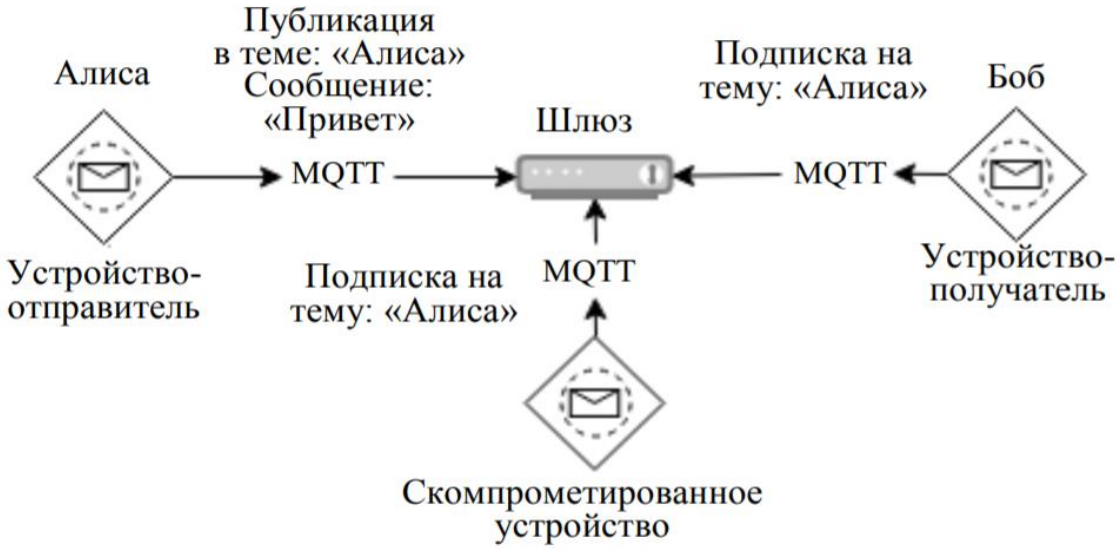


Рис. 6. Схема утечки информации при использовании протокола MQTT

На текущий момент существуют следующие решения безопасности в MQTT. Основные направления безопасности IoT - конфиденциальность и управление доступом.

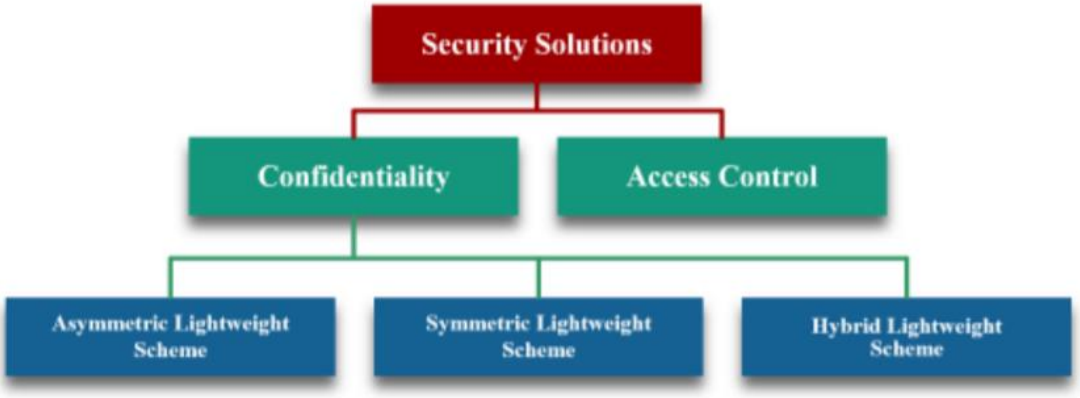


Рис. 7. Схема текущих решений безопасности

Конфиденциальность данных считается одной из фундаментальных проблем для IoT-сетей, особенно в индустрии бизнеса. Основными сложностями в защите конфиденциальности является размер генерируемых данных и эффективность контроля доступа динамичных потоков данных. Для конфиденциальности каналов связи используются методы криптографии. В основном применяются асимметричные, симметричные и гибридные схемы шифрования.

Одним из решений, основанных на асимметричном шифровании, стало шифрование на основе атрибутов (ABE), используя эллиптические кривые [9], так как использование TLS/SSL с сеансовыми ключами и сертификатами неэффективно [10].

Среди симметричных методов, рассматривается шифрование на операциях XOR, а также облегченный алгоритм шифрования SIT (Secure IoT) [11].

В протоколе MQTT защита может осуществляться на различных уровнях. На физическом уровне безопасность достигается разделением физических единиц. Это эффективно лишь в некоторых сценариях. На сетевом уровне применяется IPSec, однако из-за дополнительных заголовков он может

вызывать перегрузку. Помимо этого применяется Протокол идентификации хоста (The Host Identity Protocol), но несмотря на такие преимущества как мобильность и многозадачность, существуют трудности с криптографическими методами и распространением открытого ключа. На транспортном уровне неэффективно применять TLS из-за ограничений по пропускной способности канала IoT. Данную проблему можно решить аппаратной реализацией TLS, что значительно повысит стоимость и энергопотребление. Тем не менее, в MQTT для подключения к шлюзу используется TLS и его сертификаты, для обеспечения конфиденциальности. На прикладном уровне используются такие аутентификационные системы, как OAuth или LDAP. [12]

Традиционные механизмы, которые используются для защиты сообщений в MQTT, истощают энергетические ресурсы узлов интернета вещей. Поэтому нецелесообразно использовать такие механизмы на устройствах с низкими вычислительными ресурсами. Кроме того, угрозы безопасности канала связи MQTT, такие как подделка, могут вызвать DDoS-атаки на брокера MQTT. Однако, когда ресурсы IoT-устройств не имеют ограничения по пропускной способности канала, TLS протокол является хорошим выбором для защиты.

Текущие решения безопасности для протокола MQTT нуждаются в доработке, особенно для устройств с ограниченными ресурсами.

Несмотря на то, что протокол MQTT имеет свои достоинства - легкость и простоту, подвержен угрозам безопасности. Основными атаками являются: атака «человек посередине»; получение несанкционированного доступа к информационным потокам; атака «отказ в обслуживании». Также на шлюз MQTT может быть совершена DDoS-атака.

Для обеспечения защиты в протоколе MQTT используются следующие методы защиты: аутентификация клиентов; контроль доступа клиентов через Client ID; подключение к брокеру через TLS/SSL.

Текущие решения безопасности для протокола MQTT требуют доработки, особенно для устройств с ограниченными ресурсами.

СПИСОК ЛИТЕРАТУРЫ

1. Knud L. L. “State of the IoT 2020: 12 billion IoT connections, surpassing non-IoT for the first time”. [Электронный ресурс] URL: https://iot-analytics.com/state-of-the-iot-2020-12-billion-iot-connections-surpassing-non-iot-for-the-first-time/
2. OWASP Internet of Things Project. [Электронный ресурс] URL: https://wiki.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=Main
3. Носов А. В. АНАЛИЗ ПРИКЛАДНЫХ ПРОТОКОЛОВ ПЕРЕДАЧИ ДАННЫХ ДЛЯ СИСТЕМ ИНТЕРНЕТА ВЕЩЕЙ. [Электронный ресурс] URL: https://cyberleninka.ru/article/n/analiz-prikladnyh-protokolov-peredachi-dannyh-dlya-sistem-interneta-veschey/viewer
4. Что такое MQTT и для чего он нужен в IIoT? Описание протокола MQTT. [Электронный ресурс] URL: https://ipc2u.ru/articles/prostye-resheniya/chto-takoe-mqtt/
5. Дикий Д.И. Анализ протокола MQTT на атаки «отказ в обслуживании» // Научно-технический вестник информационных технологий, механики и оптики. 2020. Т. 20. № 2. С. 223–232 doi: 10.17586/2226-1494-2020-20-2-223-232 [Электронный ресурс] URL: https://cyberleninka.ru/article/n/analiz-protokola-mqtt-na-ataki-otkaz-v-obsluzhivanii/viewer
6. MQTT Version 3.1.1 OASIS Standard. 2014.
7. Дикий Д.И., Артемьева В.Д. Протокол передачи данных MQTT в модели удаленного управления правами доступа для сетей Интернета // Научно-технический вестник информационных технологий, механики и оптики. 2019. Т. 19. No 1. С. 109–117. doi: 10.17586/2226-1494-2019-19-1-109-117 [Электронный ресурс] URL: https://ntv.ifmo.ru/file/article/18416.pdf
8. Ahmed J. Hintaw. A Brief Review on MQTT’s Security Issues within the Internet of Things (IoT) [Электронный ресурс] URL: jocm.us/uploadfile/2019/0509/20190509033506594.pdf
9. B. S. Adiga, P. Balamuralidhar, M. A. Rajan, R. Shastry, and V. L. Shivraj, “An identity based encryption using elliptic curve cryptography for secure M2M communication,” in Proc. First Int. Conf. Secur. Internet Things - Secur. ’12, pp. 68–74, 2012.
10. V. Goyal, O. Pandey, A. Sahai, and B. Waters, “Attribute-based encryption for fine-grained access control of encrypted data,” in Proc. 13th ACM Conf. Comput.Commun. Secur. - CCS ’06, 2006, p. 89.
11. M. Usman, I. Ahmed, M. I. Aslam, S. Khan, and U. A. Shah, “Sit: A lightweight encryption algorithm for secure internet of things,” arXiv Prepr. arXiv1704.08688, 2017.
12.Ahmed J. Hintaw, Selvakumar Manickam, Shankar Karuppayah, and Mohammed Faiz Aboalmaaly, "A Brief Review on MQTT’s Security Issues within the Internet of Things (IoT)," Journal of Communications, vol. 14, no. 6, pp. 463-469, 2019. Doi: 10.12720/jcm.14.6.463-469.

УДК 004.056

М. А. САЛМИН, Е. И. КОТОВ
kambr1g00@gmail.com faf.fdfds@gmail.com
Науч. руководов. – доц. В. Е. КЛАДОВ

Уфимский государственный авиационный технический университет

ПРИНЦИПЫ ЗАЩИТЫ ИНФОРМАЦИИ ПРИ ИСПОЛЬЗОВАНИИ ФИЗИЧЕСКИ НЕКЛОНИРУЕМЫХ ФУНКЦИЙ

Аннотация. Задачи данной статьи – акцентировать внимание на теоретической и практической стороне применения технологии физически неклонируемых функций (Physical Unclonable Functions, PUF), которые используются в защите информации, и борьбе с контрафактными электротоварами. Проанализировать физический принцип работы технологии PUF, плюсы и минусы использования, а также перспективы развития.
Ключевые слова: PUF; физически неклонируемые функции; интегральные схемы; информационная безопасность; контрафактные электротовары; информационные технологии.

В современном мире распространение контрафактных товаров является серьезной и постоянно растущей проблемой во всем мире. Контрафакт существует практически во всех отраслях промышленности. Большая часть контрафакта приходится на Китай (56 %) и Гонконг (36%). [1] По оценкам Организации экономического сотрудничества и развития, 3,3 % всех проданных товаров, которые пересекали границу в 2019 году, были контрафактными. В денежном выражении это составляет огромную сумму — 427 миллиардов евро или 509 миллиардов долларов США. [2]

Контрафакт в общем смысле понимают, как фальсификацию оригинального объекта интеллектуальной собственности. Согласно гражданскому законодательству товары, этикетки, упаковки товаров, на которых незаконно размещены товарный знак или сходное с ним до степени смешения обозначение, являются контрафактными. [3] Основные категории контрафактных товаров: одежда, текстиль, игрушки, обувь, электронные товары. [4]

Существуют различные методы защиты цифровой электроники от нелегального копирования, модификации и обратного проектирования: внедрение цифровых водяных знаков и отпечатков пальцев в проектное описание, лексическая и функциональная обфускация, формальная верификация и другие. Не-

достатком большинства перечисленных методов являются аппаратные затраты и, как следствие, высокое энергопотребление. С возникновением концепции интернета вещей (Internet of Things, IoT) требования к площади, занимаемой цифровым устройством на кристалле интегральной схемы (ИС), а также к энергопотреблению становятся более жесткими, поскольку из года в год размер устройств значительно уменьшается.

Один из самых экономичных методов защиты с точки зрения аппаратных затрат — физически неклонируемые функции (Physical Unclonable Functions, PUF).

Из-за глубоких субмикронных вариаций производственного процесса каждый транзистор в ИС имеет немного разные физические свойства. Эти изменения приводят к небольшим, но измеримым различиям в электронных свойствах, таких как пороговые напряжения транзисторов и коэффициент усиления. Поскольку эти изменения процесса нельзя полностью контролировать во время производства, эти физические свойства устройства не могут быть скопированы или клонированы.

Было обнаружено, что за счет использования этих присущих вариаций PUF очень ценны для использования в качестве уникального идентификатора для любой данной ИС. Они делают это с помощью схемы внутри ИС, которая преобразует крошечные вариации в цифровую комбинацию нулей и единиц, которая уникальна для этого конкретного чипа и воспроизводится с течением времени. Этот образец представляет собой «силиконовый отпечаток пальца», который сопоставим с его биометрическим аналогом человека. [5]

Таким образом PUF для защиты электроники основаны на использовании вариаций технологического процесса изготовления интегральных схем: точных значений пороговых напряжений, задержек распространения сигналов, частоты работы компонентов и т.д. В стандартном процессе проектирования разработчики цифровых устройств стремятся уменьшить влияние вариаций на конечный

продукт. В случае PUF, напротив, данное неконтролируемое явление используется для извлечения случайности и уникальности цифрового устройства.

Используя определенные алгоритмы, кремниевый отпечаток пальца превращается в криптографический ключ, который является уникальным для этого отдельного чипа и используется в качестве его корневого ключа. Этот корневой ключ надежно восстанавливается из PUF всякий раз, когда это необходимо системе, без необходимости хранить ключ в какой-либо форме памяти. Таким образом, когда устройство выключено, секретный ключ отсутствует в любой форме памяти; в действительности корневой ключ «невидим» для злоумышленников, что делает хранение ключей с PUF очень безопасным.

PUF похожи на аппаратные реализации хеш функций, разница заключается в том, что уникальность выходного значения PUF основана на уникальности конкретной интегральной схемы. Входной аргумент PUF принято называть запрос (Challenge, CH), а выходное значение — ответом (Response, R). Таким образом, для некоторой интегральной схемы IC_k множество запросов $\{CH_0, \ldots, CH_{n-1}\}$ будет уникально отображено в множество ответов $\{R_0, \ldots, R_{n-1}\}$ с помощью физически неклонируемой функции: $R_i = PUF(CH_i)$.

Множество пар запрос — ответ уникально характеризует интегральную схему IC_k и не может быть скопировано даже при условии использования абсолютно идентичного проектного описания.

При реализации идентичного проектного описания PUF на различных интегральных схемах (ИС) ответы R_i на одинаковый запрос CH_i будут уникальны (значительно отличаться друг от друга) для каждой копии. Данное явление называется межкристальной уникальностью, т.е. способностью отличить ИС друг от друга, используя PUF. В случае использования идентичных реализаций PUF на одном кристалле для идентификации, например, различных компонентов интеллектуальной собственности, наблюдается явление внутрикристальной уникальности. Поскольку реализации PUF внутри кристалла различны как ми-

нимум по взаимному расположению, внутри кристальная уникальность, как правило, более выражена, чем межкристальная.

В настоящее время существует множество реализаций PUF на основе: задержек распространения сигналов, частоты работы компонентов, состояние памяти, изображения на светочувствительной матрице, порогового напряжения транзистора, токового зеркала, силы давления пользователя на экран смартфона, структуры бумаги и т.д.

Самый известный вариант использования технологии PUF — это создание и хранение криптографического корневого ключа для устройства. Криптографический корневой ключ, созданный с помощью PUF, не требует внедрения ключа и не может быть скопирован с одного устройства на другое. Это связано с тем, что он никогда не сохраняется, а воссоздается по кремниевому отпечатку пальца устройства каждый раз, когда это необходимо. Поскольку этот отпечаток отличается для каждого чипа, злоумышленник не может скопировать ключ с одного устройства на другое.

Для сохранения конфиденциальной информации необходимо использовать безопасные хранилища, в которых данные можно надежно разместить и физически привязать к оборудованию устройства. Этого можно легко достичь с помощью PUF, зашифровав все конфиденциальные данные с помощью ключа, полученного из корневого ключа PUF.

PUF можно применять для настройки безопасного канала между устройством IoT и облаком на основе инфраструктуры открытого ключа (например, соединение безопасности транспортного уровня (TLS) с облачной службой), сертификатов устройства и обмена облаком. Эти сертификаты аутентифицируют объекты друг для друга. Чтобы создать сертификат для аутентификации устройства, пара открытого/закрытого ключей создается из отпечатка PUF. [5]

Первой коммерческой реализацией PUF в 2008 были радиочастотные идентификаторы, изготовленные компанией Verayo. Также в настоящее время многие производители FPGA — например, Xilinx и Altera (Intel) — используют

PUF в качестве встроенного неклонируемого идентификатора ПЛИС. Поскольку PUF используются в качестве криптографических примитивов (генераторов случайных чисел, уникальных идентификаторов, аппаратных хеш функций), многие производители не раскрывают факт использования PUF, чтобы хранить в тайне детали реализации их протоколов безопасности от злоумышленников. [1]

Реализации PUF требуют алгоритмов обработки, чтобы превратить кремниевый отпечаток пальца в криптографический корневой ключ. Это связано с тем, что кремниевый отпечаток пальца будет слегка зашумлен между различными измерениями, так как помимо внутренних изменений процесса на электронные свойства также будут влиять условия окружающей среды, такие как температура и источник питания. Следовательно, хорошая реализация PUF должна превратить этот зашумленный отпечаток пальца в полностью стабильную и полностью случайную строку из нулей и единиц, чтобы ее можно было квалифицировать как криптографический ключ. Для этого в большинстве реализаций PUF используются два процесса:

− Коррекция ошибок, чтобы гарантировать, что полученный ключ остается одним и тем же каждый раз, когда измеряется PUF.

− Усиление конфиденциальности, чтобы превратить отпечаток пальца в полностью случайную строку.

Хоть PUF и действительно являются сильными якорями доверия для устройств, но каждый поставщик микросхем и OEM не развертывают свои собственные реализации PUF, потому что нелегко открывать и производить новые типы PUF. Большое количество исследований направлено на поиск элементов микросхемы, которые обладают типом поведения, необходимым для создания отпечатка пальца устройства, и в этот момент фактическое производство еще даже не началось. Для определения параметров, необходимых для алгоритмов исправления ошибок и усиления конфиденциальности, требуются миллионы измерений при различных обстоятельствах и с возрастающим старением крем-

ния. Процесс создания новой реализации PUF обычно занимает годы исследований и разработок. [5]

Физическая неклонируемая функция является очень ценным строительным блоком безопасности для поставщиков микросхем и OEM-производителей. Криптографический ключ, который создается и надежно «хранится» с помощью PUF, обеспечивает основу доверия для устройства. Это краеугольный камень успешного использования для защиты ключей, данных, IP-адресов и установки безопасных соединений с облаком или другими устройствами. [5]

Одной из основных проблем, PUF является нестабильность некоторых из значений, что, в свою очередь, вынуждает разработчика прибегать к кодам коррекции ошибок и более надежным архитектурам PUF. С другой стороны, наличие очень высокой стабильности подвергает PUF риску криптографической атаки с помощью методов машинного обучения, т.е. построения достаточно точной — более 95% — математической модели PUF, что изначально (до 2010 года) считалось невозможным в научном сообществе. Тем не менее, использование PUF в современных коммерческих приложениях в качестве криптографического примитива доказывает перспективность исследований в области поиска новых архитектур PUF, а также усовершенствования характеристик существующих реализаций. [1]

СПИСОК ЛИТЕРАТУРЫ

1. Физически неклонируемые функции: защита электроники от нелегального копирования. [Электронный ресурс] URL: https://habr.com/ru/post/343386/
2. «Приобретение оригинальной продукции важно для всех». Технический журнал EVOLUTION. 2021 г. [Электронный ресурс] URL: https://evolution.skf.com/ru/sourcing-genuine-products-concerns-everyone-everywhere/#related-articles
3. Гражданский кодекс Российской Федерации. п. 1 ст. 1515. [Электронный ресурс] URL: http://base.garant.ru/10164072/5c3bdd3bf68f494e586ff7c968087033/#block_415151
4. «По контрафакту в Сети наносят удар». Статья 2019 г. [Электронный ресурс] URL: https://rspectr.com/articles/580/po-kontrafaktu-v-seti-nanosyat-udar
5. What is a Physical Unclonable Function? [Электронный ресурс] URL: https://www.intrinsic-id.com/physical-unclonable-function/

УДК 004.056

С. О. САФИН
salavat01021999@gmail.com
Науч. руководв. – канд. техн. наук, доц. Т. А. ИВАНОВА

Уфимский государственный авиационный технический университет

КИБЕРАТАКИ, КИБЕРУГРОЗЫ В ГЛОБАЛЬНОЙ СЕТИ ИНТЕРНЕТ И ПРОТИВОДЕЙСТВИЕ

***Аннотация*.** Данная тема актуальна потому что, растет количество кибератак, совершаемых с использованием Интернет технологий и наносящих огромный ущерб компаниям по всему миру. В данной статье я рассмотрел меры по предупреждению кибератак и эффективные средство защиты от мошенников.
***Ключевые слова*:** информационная безопасность; защита информации; кибератака; киберпреступления; киберзащита.

Internet — находка для мошенника. Злоумышленнику созданы все условия: анонимность, скрытие сведений о себе, доверчивые пользователи. Актуальность разработки политик безопасности для компаний и организаций объясняется необходимостью формирования основ планирования информационной безопасности и управления ею на современном этапе.

Эпоха высоких технологий, характерной чертой которой является глобальный сдвиг от традиционной индустрии к компьютеризованной, предоставила обществу широкие возможности свободно передавать и принимать информацию, а также иметь мгновенный доступ к любой информации. Однако указанные возможности быстрых глобальных коммуникаций и информационных сетей не только легли в основу концепций цифрового века и привели к началу цифровой революции, но и дали массу возможностей преступным элементам для совершения противоправных деяний в Интернет-пространстве, обеспечивающем злоумышленникам максимальную анонимность и безопасность, оперативность, доступность, трансграничность и многие другие преимущества.

Каждый день киберпреступники взламывают тысячи сайтов. Злоумышленники используют взломанные сайты для широкого спектра задач, от созда-

ния фишинговых страниц до рассылки SEO-спама. Владельцы небольших веб-сайтов наивно полагают, что находятся в безопасности, так как их сайты хакерам не интересны. К сожалению, обычно это не так.

1. Киберугрозы в интернете

Новые технологии порождают и новые преступления. Согласно унификации Комитета министров Европейского Совета определены криминальные направления компьютерной деятельности. К ним относятся

– *Фрод (мошенничество).* Когда юзер оплачивает покупки или услуги банковской картой на вредоносном сайте, создатели ресурса могут получить доступ к реквизитам пользователя.

– *Взлом аккаунтов.* Тот случай, когда злоумышленники получают логины и пароли от почты, онлайн-банкинга или социальной сети.

– *Утечка данных.* Сбор личной информации человека для передачи третьим лицам. В такой скандал попадал Facebook. Социальная сеть допустила массовую передачу данных 50 миллионов пользователей, которым потом показывалась политическая таргетированная реклама.

– *Проникновение*. Обеспечение удаленного доступа для мошенников на персональный компьютер через вредоносное ПО.

– *Фишинг*. Сайты-подделки под популярные сервисы: социальные сети, платежные ресурсы, онлайн-банки. Рассылки, которые маскируются под рассылку от авторитетных сайтов (Google, Mail.ru, Facebook, VK). Они рассчитаны на невнимательность человека и пытаются заполучить доступ к конфиденциальным данным — логинам и паролям.

– *Обман.* Предложение в соцсетях, интернет-магазинах, досках объявлений, где продавец готов отдать товар за низкую цену. Оплата принимается онлайн или переводом на карту. После злоумышленник пропадает и не выходит на связь.

2. Почему киберпреступники взламывают сайты?

Мотивы взлома веб-сайта столь же разнообразны, как и методы, используемые для таких целей. Отсюда следует, что целью киберпреступников может

стать практически любой сайт. В статье я приведу 10 возможных причин, по которым злоумышленники могут взломать ваш сайт.

1. Платежные реквизиты

Веб-сайт, на котором что-либо продается - самая очевидная цель для киберпреступников. Хакеры могут украсть платежные реквизиты, а затем использовать их самостоятельно или кому-то продать.

Существуют различные методы взлома, позволяющие украсть платежные реквизиты при их вводе на веб-сайте. Даже если вы лично не храните платежную информацию, ваш сайт все равно интересен злоумышленникам, похищающим платежные реквизиты.

2. Информация любого рода

Веб-сайты часто собирают личную информацию посетителей, например адреса электронной почты. На веб-сайте, используемом для ведения бизнеса, может храниться информация о сотрудниках компании или предстоящих выпусках продуктов.

Любая подобная информация может оказаться полезной для хакера. Киберпреступники либо продадут информацию в даркнете, либо предложат ее приобрести владельцу пострадавшего сайта в обмен на безопасный возврат данных.

3. Фишинговые страницы

Фишинговая страница - веб-страница, предназначенная для кражи конфиденциальной информации. Фишинговые страницы выглядят точно также как обычные веб-страницы, полностью повторяя их оригинальный дизайн. Киберпреступники создают фальшивые страницы, имитирующие веб-сайт банка, заманивая пользователей в свои сети. Ничего не подозревающий пользователь вводит на фишинговой странице данные для входа в банк, и конфиденциальная информация оказывается в руках злоумышленников.

Google борется с фишинговыми страницами и заранее предупреждает пользователей об опасности. Однако, если Google уже доверяет вашему сайту, его можно взломать и использовать для обхода такой защиты. Кроме того, фи-

шинговые страницы являются незаконными. Использование взломанного веб-сайта для их размещения позволяет вору сохранить анонимность.

4. SEO-спам

Большинство владельцев веб-сайтов понимают важность SEO. Многие методы SEO включают создание обратных ссылок. Когда создается обратная ссылка с сайта A на сайт B, фактически подразумевается, что сайт A рекомендует сайт B.

Ежедневно киберпреступники взламывают множество веб-сайтов с целью создания SEO-спама. Хакер берет под контроль сайт, а затем создает обратные ссылки или вручную, или с помощью программы, автоматизирующей данный процесс.

Веб-сайт с хорошей репутацией представляет для киберпреступников особую ценность. Однако, каждый случай использования такого сайта злоумышленниками, подрывает его репутацию в поисковой системе.

5. Спам по электронной почте

Спам-рассылки доставляют пользователям неудобства, забивая почтовый ящик. Однако, на спам-рассылках можно заработать. Поэтому злоумышленники часто взламывают сайты, чтобы отправить спам и получить прибыль.

Взломав веб-сайт, киберпреступники будут использовать домен, чтобы избежать попадания в папку со спамом. Кроме того, хакеры смогут отправить большие партии сообщений, не отключаясь от собственного почтового провайдера.

Наихудшим последствием атаки является потеря репутации. Получатели спама, скорее всего, будут считать отправителем владельца взломанного сайта.

6. Вредоносное ПО

В настоящее время получение доступа к вредоносному ПО не является сложной задачей. Многие киберпреступники даже не создают вредоносные программы, а просто покупают их. Самое сложное в заработке на вредоносном ПО - найти способ установить его на чужие компьютеры.

Взломанный веб-сайт идеально подходит для подобной цели. Если Google доверяет вашему сайту, его можно использовать для распространения вредоносных программ без каких-либо предупреждений со стороны поисковика. Доверяя сайту, пользователь, не задумываясь, может разрешить загрузку странного файла.

7. Бесплатная реклама

Сайты с большим трафиком рискуют быть взломанными в рекламных целях. Например, злоумышленник может разместить на сайте рекламу своего продукта.

Другим вариантом является перенаправление трафика. Пользователи, заходящие на взломанный сайт, будут автоматически отправляться на сайт хакеров.

8. Практика

Взлом - навык, требующий практики. Конечно, научиться взламывать можно в безопасной среде, многие онлайн-сервисы были созданы для такой цели. Однако, большинство хакеров начинают свою деятельность с реальных веб-сайтов.

Начинающий киберпреступник, вероятно, выберет для практики небольшой веб-сайт, прежде чем перейти к чему-то более прибыльному.

9. Развлечения

Иногда хакерам просто нравится взламывать. Множество громких кибератак осуществлялось исключительно по одной причине: злоумышленники хотели проверить свои возможности. Другими словами, хакер может выбрать целью ваш веб-сайт, чтобы проверить, сможет ли он его взломать.

Еще одна популярная мотивация - хвастовство. Хакер просто хочет похвастаться перед друзьями, что контролирует ваш сайт.

10. Перевод сайта в автономный режим

Хакеры часто взламывают веб-сайты с целью отключения. Сайты отключают из мести. Возможно, вы сказали или сделали что-то, что не понравилось хакеру. Также отключение сайта производят ради прибыли.

Сайты, приносящие деньги, - лакомая добыча для киберпреступников. Переведя такой сайт в автономный режим, хакер будет требовать у владельцев оплату в обмен на возобновление работоспособности ресурса.

3. Ранжирование угроз

Почти любая методика оценки угроз начинается с составления перечня всех возможных угроз. При этом актуальность обычно определяется экспертным путем. Хорошая методика оценки угроз должна снижать фактор предвзятости эксперта и стараться получать воспроизводимые результаты раз за разом.

Каждая угроза характеризуется набором показателей - наличие доступа для реализации угрозы, масштаб последствий, требуемое время восстановления, легкость обнаружения, необходимые навыки для реализации, требуемые ресурсы и т.п. Пять градаций могут быть заменены на три, а количество показателей может быть как увеличено, так и уменьшено. Например, в данном примере веса факторов, связанных с последствиями нарушения конфиденциальности и доступности выше, чем для нарушения целостности. Чем выше значение фактора (от 1 до 5), тем опаснее угроза

Таблица 1

Сравнение показателей угроз

Показатель угрозы	1	2	3	4	5	Вес показателя
Какой доступ нужен для реализации угрозы?	Не требуется ни сетевой, ни физический доступ	Доступ через разрешенные протоколы на периметре	Учетная запись пользователя на атакуемом активе (не административная)	Права администратора на атакуемом активе	Физический доступ к атакуемому активу	0,1
Насколько локализованы последствия в случае успешной реализации угрозы?	Нет заметного эффекта	Эффект ограничен атакованным активом	Атакованный актив и сегмент, в котором он находится	Подвержены внешние сети и системы	Глобальный эффект	0,1
Как долго потребует восстановление после успешной реализации угрозы?	Восстановление не требуется	< 1 часа	< 24 часов	< 72 часов	>= 72 часов	0,1
Насколько велика стоимость восстановления или замены атакованного актива?	Восстановление не требуется	< 500 тысяч рублей	< 5 миллиона рублей	< 10 миллионов рублей	>= 10 миллионов рублей	0,1
Насколько велики последствия нарушения конфиденциальности в случае успешной реализации угрозы?	Нет последствий	Ограниченные негативные последствия	Серьезные негативные последствия	Тяжелые негативные последствия	Катастрофические негативные последствия	0,2
Насколько велики последствия нарушения целостности в случае успешной реализации угрозы?	Нет последствий	Ограниченные негативные последствия	Серьезные негативные последствия	Тяжелые негативные последствия	Катастрофические негативные последствия	0,1
Насколько велики последствия нарушения доступности в случае успешной реализации угрозы?	Нет последствий	Ограниченные негативные последствия	Серьезные негативные последствия	Тяжелые негативные последствия	Катастрофические негативные последствия	0,2
Обнаруживали ли вы данную угрозу ранее?	Нет, встречаю впервые	Возможно встречались отдельные ТТУ	Есть подтверждение в базе инцидентов (своей или внешней)	Частое подтвержденное повторение угрозы	Широко распространенная угроза	0,1

Таблица 2

Продолжение таблицы 1

Какой уровень навыков или знаний требуется от нарушителя для реализации данной угрозы?	Специальные навыки и знания не требуются	Базовые технические навыки и знания	Необходимы некоторые знания об атакованном активе	Детальные знания об атакованном активе	Детальные знания об атакованном активе, а также о его предназначении	0
Какие ресурсы требуются нарушителю для реализации данной угрозы?	Ресурсы не требуются	Требуются минимальные ресурсы	Требуются среднее количество ресурсы	Требуется большое количество ресурсов	Максимально возможное количество ресурсов	0
Насколько легко обнаружить данную угрозу?	Не детектируется	Обнаружение возможно со специализированным мониторингом	Обнаружение вероятно будет возможно со специализированным мониторингом	Обнаружение возможно с базовым мониторингом	Угроза наблюдается без мониторинга	0
Приведут ли оставленные угрозой следы к атрибуции нарушителя?	Нет оставленных следов	Некоторые следы оставлены; атрибуция маловероятна	Атрибуция возможна, опираясь на характеристики угрозы	Такая же или аналогичная угроза была атрибутирована	Атрибуция осуществляется по сигнатуре	0

После того, как для каждой угрозы/техники указываются их значения, осуществляется подсчет итогового значения рейтинга (сумма по всем показателям, умноженным на весовые коэффициенты), что и позволяет нам получить не просто список всех актуальных угроз, а угроз систематизированных по уровню опасности для нашей компании. В примере выше 4 "фиолетовых" показателя имеют нулевые веса и соответственно в расчете не учитываются. В реальности это происходит очень часто - мы просто не можем оценить отдельные показатели по угрозы - требуемые ресурсы и навыки, легкость атрибуции и т.п. Но тогда надо учесть, что такие показатели с нулевым весом будут приводить к автоматическому снижению рейтинга угроз, хотя и незначительно.

У данного подхода есть, как минимум, три преимущества. Во-первых, он легко автоматизируется - я прикладываю к заметке табличку в Excel, которую вы можете использовать для своих нужд и которая позволит вам ускорить процесс моделирования. Во-вторых, такое матричное представление и ранжирование угроз гораздо более компактное и помещается на половине страницы А4, что позволяет методики на ее основе делать также более компактными.

4. Выбор защитных мер

4.1. Ранжирование защитных мер

Можно оценить любую защитную меру с трех позиций - покрытие угроз (чем больше угроз покрывает защитная мера, тем лучше), стоимость внедрения

и стоимость эксплуатации. При этом второй показатель складывается из стоимости разработки (покупки) защитной меры, стоимости ее тестирования (пилотирования) и стоимости интеграции защитной меры в защищаемую среду. Стоимость эксплуатации в свою очередь также складывается из ряда параметров - стоимость обслуживающего персонала (можно иметь классную систему защиты, но не иметь персонала, умеющего с ней работать), стоимость обучения персонала (попробуйте найти в России или СНГ нормальные курсы по threat hunting или SOCам), стоимость обслуживания, поддержки, утилизации и перехода на новую или обновленную меру.

Таблица 3

Сравнение показателей оценки защитной меры

Показатель оценки защитной меры						Вес показателя	Мера 1	Ме
Показатели внедрения	1	2	3	4	5			
Насколько технически зрела защитная мера?	Доказанная временем технология	Новый для рынка продукт, подход, технология	Работающий прототип	Демонстрационный прототип	Лабораторный или исследовательский прототип	0,2		
Требуются ли для защиты специализированные или труднодоступные аппаратные или программные возможности для разработки и внедрения?	Требуются минимальные возможности	Требуются некоторые возможности	Требуются средние возможности	Требуется широкий спектр специализированных возможности	Требуются дорогостоящиеся и сложнодоступные возможности	0,1		
Снижается ли эффектиность защитной меры со временем?	90% эффективность остается через 5 лет	75% эффективность остается через 3 года	60% эффективность остается через 2 года	40% эффективность остается через 1 год	10% эффективность остается через 6 месяцев	0,1		
Использует ли защитная мера стандартные протоколы и интерфейсы, облегчающие интеграцию с другими технологиями?	Взаимодействует через стандартные и признанные в отрасли интерфейсы	Ограниченное взаимодействие с другими продуктами и технологиями	Проприетарные интерфейсы и нестандартные протоколы	Внешние интерфейсы отсутствуют	Нейтрализация реализована как стандартная возможность	0,1		
Требует ли базовое ПО и железо сереьзных изменений для внедрения защитной меры?	Никаких изменений не требуется	Требуются незначительные изменения в конфигурации	Требуются значительные изменения в конфигурации	Требуются изменения в программном обеспечении	Требуются изменения в аппаратном обеспечении	0,1		

Таблица 4

Сравнение показателей эксплуатации

Показатели эксплуатации	1	2	3	4	5			
Требует ли защитная мера интенсивного и глубокого обучения?	Обучение не требуется	Требуется минимальное обучение	Требуется нерегулярное обучение	Требуется регулярное обучение	Требуется непрерывное обучение	0,1		
Требует ли защитная мера много и квалифицированного персонала для своей эксплуатации?	Дополнительный персонал не требуется	Требуется минимальный персонал	Требуется среднее число новых сотрудников	Требуется много персонала	Требуется интенсивная работа с кадрами	0,1		
Требуются ли для защиты специализированные или труднодоступные аппаратные или программные возможности для эксплуатации?	Не требуется никаких специальных возможностей	Требуются минимальные возможности	Требуются некоторые возможности	Требуется широкий спектр специализированных возможности	Требуются дорогостоящиеся и сложнодоступные возможности	0,1		
Требует ли защитная мера регулярного обновления ПО, железа или алгоритмов для того, чтобы оставаться эффективной?	Нечасто	От случая к случаю	Регулярно	Часто	Постоянно	0,1		

Выбор защитных мер это не только оценка стоимости их внедрения но и эффективность, которая в самом простейшем случае определяется тем, сколько угроз можно нейтрализовать с помощью конкретной защитной технологии, средства или меры.

Таблица 5

Сравнение угроз

Угрозы	Мера 1	Мера 2	Мера 3	Мера 4	Мера 5	Мера 6	Мера 7	Мера …
Фишинг	X				X	X		
Вредоносное ПО	X	X	X			X		
Отказ в обслуживании				X				
Спам	X							
Атаки на Web-приложения							X	
Перехват / утечка информации	X							
Кибершпионаж	X	X	X	X	X	X	X	X
Потеря актива								X
Кража актива								X
…								
Итого	*5*	*2*	*2*	*2*	*2*	*3*	*2*	*3*

По таблице 5 видно, что мера 1 "закрывает" 5 угроз, 6-я и последняя мера - по 3, а остальные по 2 угрозы. Выбор в пользу первой меры не вызывает вопросов - с ее помощью мы сможем нейтрализовать большее число угроз. Но у данного подхода, несмотря на его очевидные преимущества, есть и один недостаток. Он не учитывает эффект, которого достигает защитная мера. Если вспомнить NIST Cybersecurity Framework, то все защитные меры там разделены на 5 блоков - идентификация, предотвращение, обнаружение, реагирование и восстановление. Это и есть эффекты защиты, которые, для упрощения (если функцию восстановления отдать в ИТ, а функцию идентификацию реализовывать по любому), можно свести к трем:

– Предотвращение. Защитные меры этого типа делают атаку невозможной. Например, межсетевой экран или средство установки патчей.

– Обнаружение. Защитные меры этого типа позволяют определить, что атака/угроза произошла, происходит или может произойти. Сюда можно отнести антиспам, обнаружение вторжений и т.п.

– Реагирование. Защитные меры этого типа позволяют снизить негативный эффект в случае реализации угрозы.

– Понятно, что одна и та же защитная мера может иметь разный эффект на разные угрозы, а также несколько разных эффектов на одну и ту же угрозу. Поэтому в матрице выше стоит ставить не просто крестик, а указывать конкретный эффект от защитной меры. Зачем нам защитная мера, которая позволяет только обнаруживать угрозы, но никак на них не реагирует? Ту же самую идею можно применить и к эффекту от защитной меры и выделить для них три уровня:

– Высокий. Эффект защитной меры подтвержден демонстрацией, сертификацией, тестами, пилотом и т.п.

– Средний. Оценка эффекта защитной меры базируется на предположении эксперта.

– Низкий. Эффект имеет правдоподобную картину, но еще никак не подтвержден.

В итоге, если объединить эффект защитной меры с его уровнем и поместить в матрицу, то мы получим следующий вариант (P, D и R означают эффект - prevention, detection и response, а H, M и L - уровень - High, Medium и Low):

Таблица 6

Объединенная таблица эфеекта защитной меры с его уровнем

Угрозы	Мера 1	Мера 2	Мера 3	Мера 4	Мера 5	Мера 6	Мера 7	Мера …
Фишинг	**DH**				**RH**	**DM**		
Вредоносное ПО	**DM**	**DH, RH**	**PH**			**DM**		
Отказ в обслуживании				**PM**				
Спам	**DH**							
Атаки на Web-приложения							**DH**	
Перехват / утечка информации	**DM**							
Кибершпионаж	**DL**	**RL**	**PL**	**PL**	**RL**	**DL**	**DL**	**PL**
Потеря актива								**PM**
Кража актива								**PM**
…								
Итого для предотвращения	***0***	***0***	***2***	***2***	***0***	***0***	***0***	***3***
Итого для реагирования	***0***	***2***	***0***	***0***	***2***	***0***	***0***	***0***
Итого	***0***	***2***	***2***	***2***	***2***	***0***	***0***	***3***

Обратите внимание - результат поменялся, так как первая мера защиты много обнаруживает, но ничего не предотвращает и не снижает негативный эффект от обнаруженных угроз. В итоге рейтинг защитных мер у нас поменялся, но стал выглядеть более адекватным. К нему можно также добавить еще и веса, но это уже опционально.

Если сложить А и Б, вчерашний рейтинг защитный меры и сегодняшний, то поделив сегодняшний рейтинг на вчерашний и умножив результат на 100, получим итоговый рейтинг защитной меры, проранжировав которые получим список того, с чего стоит начинать построение системы защиты.

4.2. Способы защиты от мошенников

Чтобы не стать жертвой мошенников, рекомендуется ознакомиться с простыми правилами:

1. Надежные пароли. Не нужно задавать слишком простые пароли вроде 12345 или qwerty. Сейчас разработано множество программ, которые умеют вычислять пароли подбором. Если мошенник знает человека, то подобрать данные для входа не так сложно. Для безопасности своего ПК рекомендуется придумывать пароли с использованием больших и маленьких букв, цифр и символов.

2. Шифрование данных. В этом случае доступ предоставляется только с использованием ключа. Подходит также для безопасности отдельных файлов и папок. Для этого они переносятся в запароленный архив zip или rar.

3. Антивирус. Чтобы получить доступ к чужому компьютеру, злоумышленники используют вирусы. Во избежание взлома рекомендуется устанавливать антивирусные программы и регулярно обновлять их.

4. Протокол HTTPS. Не допускает перехвата данных. Но нужно, чтобы сервер поддерживал эту технологию. Использование в одностороннем порядке невозможно.

5. Защита беспроводной сети. Если к wi-fi не ограничен доступ, это привлечет мошенников. Во избежание кражи данных рекомендуется выбрать метод шифрования данных WPA/WPA2 и придумать сложный пароль.

6. Родительский контроль. Удобен, если интернетом пользуются дети. Для ребенка можно создать отдельную учетную запись с ограниченным доступом к сайтам.

К сожалению, несмотря на большое количество способов, они по-своему уязвимы. Поэтому рекомендуется использовать сразу несколько вариантов в комплексе.

Для безопасности личных данных при использовании сети интернет рекомендуется не впадать в крайности, а следовать простым советам:

1. Антивирус. По стандарту это самая распространенная мера безопасности. Программа обнаруживает вредоносное ПО, шпионские ссылки, фишинговые сайты и подозрительный трафик. Антивирус спасает от угроз, которые атакуют компьютер, но не защищает от действий клиента на сервисах.

2. VPN — сеть, скрывающая ip. Для обхождения блокировки сайта или обеспечения анонимности рекомендуется использовать данную программу. VPN оберегает от кражи информации, шифрует ее, скрывает личные данные.

3. Двухфакторная аутентификация. Для авторизации на сайте придется ввести два доказательства того, что аккаунт принадлежит пользователю. Обычно это пароль и смс-код на телефон. Если мошенник получил доступ к паролю, взломать аккаунт у него не получится.

4. Внимательность и осторожность с почтой. Не рекомендуется открывать письма от неизвестных источников и переходить по сомнительным ссылкам.

5. Регулярное обновление программного обеспечения. Разработчики ПО постоянно мониторят методы взлома сайтов мошенниками. На основе полученных данных создается программное обеспечение, которое снижает риски хищения личных сведений. Поэтому рекомендуется регулярно обновлять ПО.

Заключение

По словам экспертов в последующие годы кибермошенники будут активно продвигать «преступление как услугу». Следует признать, что развитие искусственного интеллекта в глобальном информационном пространстве открывает новые возможности не только для ведущих корпораций мира, но и для

преступников, поэтому к новым средствам киберзащиты в ближайшие годы будут предъявлены повышенные требования.

Несмотря на всю масштабность киберугроз, при согласованности действий, возможно им успешно противодействовать. Если государство осуществляет борьбу с киберпреступниками законодательными и организационными мерами, то в силах каждого пользователя внести свой неоценимый вклад в общее дело -знать и соблюдать элементарные правила кибербезопасности, своевременно и грамотно реагируя на неполадки в работе компьютерной системы.

Таким образом, можно считать, что поставленные цели достигнуты. Мы узнали много нового, интересного и полезного. Полученные знания пригодятся в жизни всем нам. Чем сильнее становится зависимость жизни общества от компьютерных систем, тем опаснее уязвимость России и других стран от всевозможных мастей киберпреступников. О безопасности надо думать сегодня, завтра уже может быть поздно.

СПИСОК ЛИТЕРАТУРЫ

1. Алексей Лукацкий: Бизнес без опасности: портал [Электронный ресурс]. – Режим доступа: https://lukatsky.blogspot.com/.
2. 10 причин, по которым киберпреступники взламывают сайты [Электронный ресурс]. – Режим доступа: https://www.securitylab.ru/analytics/524702.php
3. Здоровье и безопасность в мире компьютерных технологий и Интернет. Учебно-методический комплект. - М.: СОЛОН-ПРЕСС, 2010
4. Защита от вредной информации в сети интернет: портал [Электронный ресурс]. - Режим доступа: http://www.intemet-kontrol.ru/.
5. Азбука безопасности: портал [Электронный ресурс]. - Режим доступа: http://azbez.com/safety/intemet.
6. Безопасный Интернет в России: портал [Электронный ресурс]. – Режим доступа: http://www.saferinternet.ru/.
7. http://cdb96.ru/p0207.htm - Как сделать Интернет более безопасным?
8. Защита информации: ключевые тенденции: портал [Электронный ресурс]. – Режим доступа: https://www.anti-malware.ru/analytics/Threats_Analysis/Data-protection-trends-in-2020

УДК 004.056.57

М. Р. СИБАГАТОВ, В. А. АНИКИН, АХМЕД-НУР ХУССЭИН
manajatwa21@gmail.com, anvi21@mail.ru, dhicis68@gmail.com
Науч. руководв. – канд. техн. наук, ст. преп. К. В. МИРОНОВ

Уфимский государственный авиационный технический университет

МЕТОДЫ ОБНАРУЖЕНИЯ СОВРЕМЕННОГО ВРЕДОНОСНОГО ПО НА ПРИМЕРЕ БУТКИТОВ

***Аннотация*.** В данной статье рассмотрены методы обнаружения современного вредоносного ПО, история компьютерных вирусов, методы обнаружения и способы внедрения вредоносного ПО в информационные системы, буткиты и современные методы его обнаружения.
***Ключевые слова*:** буткит; вредоносное ПО; ELAM.

С каждым годом появляется все больше разнообразного вредоносного ПО. Зародившись как весьма необычное явление, примитивные вирусы, начиная с 1980-х годов, постепенно превращались в сложные технологические разработки, осваивали новые ниши, проникали в компьютерные сети.

Самые первые вредоносные программы, такие как Cookie Monster, Animal и Creeper [1], появились в 1970-е годы, но они несли для пользователей скорее раздражающий характер, чем вредоносный и разрушительный. Позднее, появились вирусы Elk Cloner (1981 г.), Brain (1986 г.), червь Морриса (1988 г.) – их уже можно назвать полноценными вредоносными программами, так как последствия от выполняемых этими программами действий были куда более серьезными, чем от вирусов 70-х годов.

Постоянно совершенствуясь, вредоносное ПО создается и в настоящее время. Так, 5 октября 2020 «Лаборатория Касперского» обнаружила целевую кампанию кибершпионажа с использованием сложной модульной структуры MosaicRegressor, куда в том числе входит буткит для встроенной в материнскую плату микропрограммы UEFI. Атаки были обнаружены с помощью технологии Firmware Scanner. Она входит в состав продуктов «Лаборатории Касперского» с начала 2019 года и разработана специально для детектирования

угроз, скрывающихся в микросхемах ROM BIOS, включая образы прошивок UEFI [2].

В данной научно-исследовательской работе описываются принципы работы вредоносного ПО, методы их обнаружения, и как они внедряются в систему.

В 1969 году Крис Таварес написал на языке PL/1 программу Cookie Monster. Он вручную отправлял сообщения, которые блокировали процессы и выводили на терминал просьбу «дай мне печенья». Программа блокировала терминал до тех пор, пока оператор не вводил слово «печенье». Данное вредоносное ПО ошибочно называют вирусом из-за особенности его реализации, но оно не самовоспроизводится и не распространяется, и поэтому считается противирусом. Операционная система Multics позволяет установить таймер и завершить программу, а когда таймер срабатывает, программа запускается вновь, как будто бы вызов произошел с терминала. Таким образом, можно было подумать, что программа, исполнение которой было прервано, «заражена».

Историю компьютерных вирусов условно можно разделить на несколько этапов: доисторический, «до-интернетовский», интернет-этап, и современный (криминальный) этап [3].

Один из первых вирусов доисторического этапа Creeper был обнаружен в военной компьютерной сети ARPANET – прототипе современного интернета. Программа была написана для подсистемы RSEXEC операционной системы Tenex, отвечающей за удаленное исполнение программ в компьютерной сети. Он перемещался по серверам и мог самостоятельно войти в сеть через модем и передать свою копию удаленной системе. На зараженных системах вирус обнаруживал себя сообщением: «I’M THE CREEPER: CATCH ME IF YOU CAN», которое выводилось на дисплей или на принтер. Для удаления вируса была написана первая антивирусная программа Reeper, которая аналогичным образом распространялась по сети, удаляла обнаруженные копии Creeper и затем

(предположительно — через определенный промежуток времени) самоликвидировалась.

Во времена «до-интернетовского» этапа Компьютеры становятся все более и более популярными. Появляется все больше и больше программ, авторами которых являются не фирмы-производители программного обеспечения, а частные лица. Развитие телекоммуникационных технологий дает возможность относительно быстро и удобно распространять эти программы через серверы общего доступа — BBS (Bulletin Board System). Позднее, полулюбительские, университетские BBS перерастают в глобальные банки данных, охватывающие практически все развитые страны. Они обеспечивают быстрый обмен информацией между самыми удаленными точками планеты. «Глобальная сеть» серверов BBS становится популярной и в результате привлекает внимание программистов-хулиганов. Появляется большое количество разнообразных «троянских коней» — программ, не имеющих способности к размножению, но при запуске наносящих системе какой-либо вред.

Apple II, разработанный в 1977, стал одним из наиболее успешных персональных компьютеров того времени — было произведено около двух миллионов компьютеров этой марки. Он предназначался не только для профессионалов, но и для массового пользователя — это был компьютер для дома, он использовался в школах и университетах. В результате своей массовости он стал жертвой первого документально зафиксированного компьютерного вируса — некто Ричард Скрента (Richard Skrenta), один из миллионов пользователей Apple II, догадался разработать для этого компьютера саморазмножающуюся программу-вирус.

Вирус, получивший название Elk Cloner, записывался в загрузочные секторы дискет, к которым обращалась ОС компьютера. Проявлял себя вирус весьма многосторонне: переворачивал изображение на экране, заставлял мигать текст. [4]

Интернет-этап. В январе 1999 года разразилась глобальная эпидемия почтового интернет-червя Happy99 (также известного как Ska). По сути, это был первый современный червь, открывший новый этап в развитии вредоносных программ. Он использовал для своего распространения программу MS Outlook, являющуюся корпоративным стандартом в США и во многих странах Европы.

К современному вредоносному ПО можно отнести загрузчик Mlw #41 (2019) APT-группировки TA505. Данный образец закрепляется в системе, собирает сведения и пересылает их на управляющий сервер.

Вирусные атаки являются одной из первостепенных угроз информационной безопасности. Такие действия наносят финансовый ущерб, а также позволяют реализовать многие другие опасные угрозы. Выделяется три основных класса методов: сигнатурный, статистический и эвристический.

Сигнатурный метод анализа обнаружения вредоносного ПО заключается в проверке наличия в принимаемых файлах сигнатур вирусов. Сигнатурой вируса можно считать совокупность черт, позволяющих идентифицировать наличие вируса в файле. Такая сигнатура должна содержать только уникальные строки из этого файла, настолько характерные для вируса, чтобы гарантировать минимальную возможность ложного срабатывания. Таким образом, процесс проектирования защищенных автоматизированных информационных систем должен основываться на знаниях и строгом соблюдении требований действующих нормативных документов, как со стороны его создателей, так и пользователей» Гафнер В.В. [6]

Данный метод реализуется следующим образом: поддерживается база данных сигнатур для известных атак с возможностью пополнения без потерь в производительности. В результате анализа происходит сопоставление регистрируемой последовательности событий известным сигнатурам атак. В случае соответствия выдается сигнал о попытке вторжения. Дальнейшие действия определяются алгоритмами модуля реакции: удаление вируса или оповещение.

Пошаговый процесс обнаружения на основе сигнатур выглядит так:

1. Обнаруживается новый тип вредоносного ПО.

2. Заносится в базу данных след вредоносного ПО.

3. Обновляется антивирусное ПО и база данных.

4. Антивирус способен найти данное вредоносное ПО во время сканирования, при использовании поиска по следу. [7]

Синтаксический метод анализа предназначен для выявления безопасности поведения программ и систем обнаружения нарушителя. Данный метод делится на 2 типа методов анализа: статический анализ последовательности системных вызовов и метод конечных автоматов.

Статистический анализ последовательности системных вызовов основывается на том, что каждое новое наблюдение переменной должно укладываться в некоторых границах. Если этого не происходит, то имеет место отклонение. Ресурсоемкость метода высокая, время выявления вирусного ПО высокая, эффективность выявления на ранней стадии высокая, эффективность выявления на поздней стадии низкая, ложные срабатывания минимальны.

Метод конечных автоматов состоит в разработке конечного автомата для распознавания «языка» трассы программы. Для этого существует много методик, основанных на использовании как детерминированных, так и вероятностных автоматов. Ресурсоемкость метода низкая, время выявления вирусного ПО низкая, эффективность выявления на ранней стадии высокая, эффективность выявления на поздней стадии низкая, ложные срабатывания максимальны. [8]

Эвристический метод анализа - это метод обнаружения вирусов путем изучения кода на предмет подозрительных свойств. [9]

Выделяют два основных типа эвристического анализа: динамический и статический.

В ходе динамического эвристического анализа сканируемый файл запускается в безопасном виртуальном пространстве - «песочнице», после чего антивирус анализирует его действия, производимые в операционной системе. Ос-

новной недостаток динамического анализа – его требовательность к вычислительным ресурсам для эмуляции операционной системы.

Статистический эвристический анализ, напротив, не обладает данным недостатком. В ходе анализа рассматривается структура и содержимое файла и выявляются признаки, характерные для других, ранее изученных вирусов. В основе статического эвристического анализа лежит задача бинарной классификации, состоящая из двух основных этапов: обучения классификатора и распознавания (определения является ли неизвестный файл вредоносным или легитимным). Этап обучения – первоочередной и во многом предопределяет верность классификации. [10]

Классификация методов по критичным к обнаружению атак параметрам

Класс	Метод	Ресурсоемкость	Время выявления	Эффективность на ранней стадии	Эффективность на поздней стадии	Ложные срабатывания	Универсальность	Наличие обновляемых баз	Простота критериев оценки	Самостоятельность метода	Необходимость обучения системы
Сигнатурный метод анализа	Продукционные / экспертные системы обнаружении вторжения	+/–	+	–	+	+	–	–	–	+	+
	Обнаружение вторжений, основанное на модели	+/–	+	–	+	+	–	–	–	–	+
	Анализ перехода системы из состояния в состояние	+	+	–	+	+	–	–	–	+	+
	Изменение состояний и сети Петри	–	–	–	+	+	–	–	+	+	+
Статистический метод анализа	Статистический анализ последовательности системных вызовов	+	+	+	–	–	+	+	–	+	–
	Машина конечных состояний	–	–	+	–	–	+	+	–	+	–
Эвристический метод	Анализ поведения системы	+	+	+/–	+	+/–	–	+	–	+	+

Рис. 1. Классификация методов по критичным к обнаружению атак параметрам

Теперь перейдем к известным на сегодняшний день способам внедрения вредоносного ПО в информационные системы.

На данный момент существует два актуальных способа внедрения компьютерных вирусов, о которых пользователи не догадываются, а антивирусы не имеют достаточного опыта для своевременного их отслеживания:

– Использование джойнера (joiner) файлов с последующим распространением под видом рядовой программы.

– Использование символов юникода в названии файлов вирусов. [11]

Джойнер (joiner) — программа, которая позволяет “склеивать” вредоносную программу с любым файлом в конечный формат “.exe”. Таким образом, взяв, к примеру, дистрибутив программы 2ГИС, становится возможным связать его с вирусом и отправить как обычный инсталлятор обычному пользователю.

Самым простым джойнером является любой архиватор (например, WinRAR). Архиваторы имеют функцию создания самораспаковывающихся архивов SFX, у которых на выходе расширение “.exe”.

Таким образом, в архив добавляются два исполняемых файла и запаковываются. Далее, остается методом простого обмана заставить пользователя компьютера открыть данный архив и с этого момента процесс не обратим. К слову, антивирусы никак не реагируют на данный метод склейки файлов, так как он считается легальным. SFX-архивы используются в повсеместном использовании, хоть и не так часто, как это было задумано. Разработчики антивирусов не берут во внимание тот факт, что данным способом также пользуются в корыстных целях.

Юникод — стандарт кодирования символов, позволяющий представить знаки почти всех письменных языков. Стандарт предложен в 1991 году некоммерческой организацией «Консорциум Юникода». Применение этого стандарта позволяет закодировать очень большое число символов из разных письменностей: в документах Unicode могут соседствовать китайские иероглифы, математические символы, буквы греческого алфавита, латиницы и кириллицы, при этом становится ненужным переключение кодовых страниц. [12]

Юникод в название файла добавить очень просто, достаточно вызвать контекстное меню и выбрать нужный символ. В нашем случае, это код RLO. Суть данного кода — зеркалирование символов после вставленного кода. Например, файл имеет название “TESTgpj.exe”, вставив RLO после “TEST”, то получим: “TESTexe.jpg”. Смысл перестановки расширений файлов в том, что обычный пользователь в первую очередь посмотрит на расширение файла, чтобы не заразить свой компьютер. Жертва, руководствуясь своими базовыми зна-

ниями, поймет, что это изображение (формат “.jpg”) и отбросит всякие подозрения.

Антивирусные программы также бессильны в данном случае, так как просто-напросто не проверяют названия файлов на символы юникода в нем. Данная функция в операционной системе Windows является стандартной.

В настоящее время буткиты представляют из себя самую передовую технологию, доступную киберпреступникам. Технология позволяет вредоносному коду запускаться до загрузки операционной системы, она реализована во многих вредоносных программах. Буткиты существуют; они востребованы на черном рынке и широко используются киберпреступниками для разных целей, в том числе для проведения целевых атак. [13]

Далее будет рассмотрен внедренный в Windows 8, и, в последствии, Windows 10 модуль раннего запуска противодействия вредоносному ПО.

Windows 8/10 включает в себя новую функцию безопасности, называемую Безопасная загрузка, которая защищает конфигурацию и компоненты загрузки Windows и загружает драйвер Раннего запуска для защиты от вредоносного ПО.

Этот драйвер запускается раньше других драйверов при запуске и позволяет оценить эти драйверы и помогает ядру Windows решить, следует ли их инициализировать. ELAM запускается сначала ядром, поэтому он запускается раньше, чем любое другое стороннее программное обеспечение. Следовательно, он способен обнаруживать вредоносное ПО в самом процессе загрузки и предотвращать его загрузку или инициализацию. [14]

Драйвер ELAM регистрирует подпрограммы обратного вызова, которые имеющееся ядро применяет для оценки данных в своем узле реестра и драйверах старта запуска. Эти обратные вызовы выявляют вредоносные данные и модули и предотвращают их загрузку и инициализацию со стороны Windows.

Имеющееся ядро Windows вносит в реестр и исключает из него такие обратные вызовы реализуя такие подпрограммы API:

CmRegisterCallbackEx и CmUnRegisterCallback

Заносят в реестр и исключают из него обратные вызовы для отслеживания данных реестра.

- IoRegisterBootDriverCallback

- IoUnRegisterBootDriverCallback

Заносят в реестр и исключают из него драйверы старта запуска.

Эти подпрограммы обратного вызова применяют установленный прототип EX_CALLBACK_FUNCTION.

```
NTSTATUS EX_CALLBACK_FUNCTION(
1 IN PVOID CallbackContext,
2 IN PVOID Argument1,          // callback type
3 IN PVOID Argument2           // system-provided context structure
);
```

Рис. 2. Прототип обратного вызова ELAM

Параметр (1) CallbackContext получает некий контекст из своего драйвера ELAM после того, как этот драйвер исполнил один из упомянутых выше обратных вызовов подпрограмм для регистрации обратного вызова. Значение контекста - это указатель на некий буфер в памяти, удерживающий относящиеся к драйверу ELAM параметры, доступ к которым может выполняться одной из таких подпрограмм обратного вызова. Такой контекст является неким указателем, который также применяется для хранения значения текущего состояния самого драйвера ELAM.

Значение аргумента (2) предоставляет тот тип обратного вызова, который может быть одним из перечисленных ниже для своих драйверов старта запуска:

- BdCbStatusUpdate (Предоставляет состояние обновлений для какого-то драйвера ELAM в зависимости от зависимостей самого загружаемого драйвера или драйверов старта запуска.)

- BdCbInitializeImage (Применяется этим драйвером ELAM для классификации драйверов старта запуска и их зависимостей.)

Значение аргумента (3) предоставляет сведения, которые сама операционная система использует для классификации такого драйвера старта запуска как заведомого хорошего (known good, драйвера, о котором известно, что он легитимен и чист), неизвестного (unknown good, драйвера, который ELAM не способен классифицировать) и заведомо плохого (known bad, драйвера, о котором известно, что он вредоносен). [15]

ELAM предоставляет программному обеспечению безопасности некое преимущество перед угрозами руткитов, но не против буткитов. ELAM способен отслеживать лишь законно загружаемые драйверы, однако большинство буткитов загружает драйверы режима ядра, которые пользуются недокументированными функциональными возможностями операционной системы.

Это означает, что некий буткит способен обходить принуждения безопасности и внедрять свой код в адресное пространство ядра несмотря на ELAM.

Код вредоносного буткита запускается до инициализации ядра своей операционной системы и до загрузки каких бы то ни было драйверов режима ядра, включая ELAM. Это означает, что некий буткит способен уклоняться от защиты ELAM.

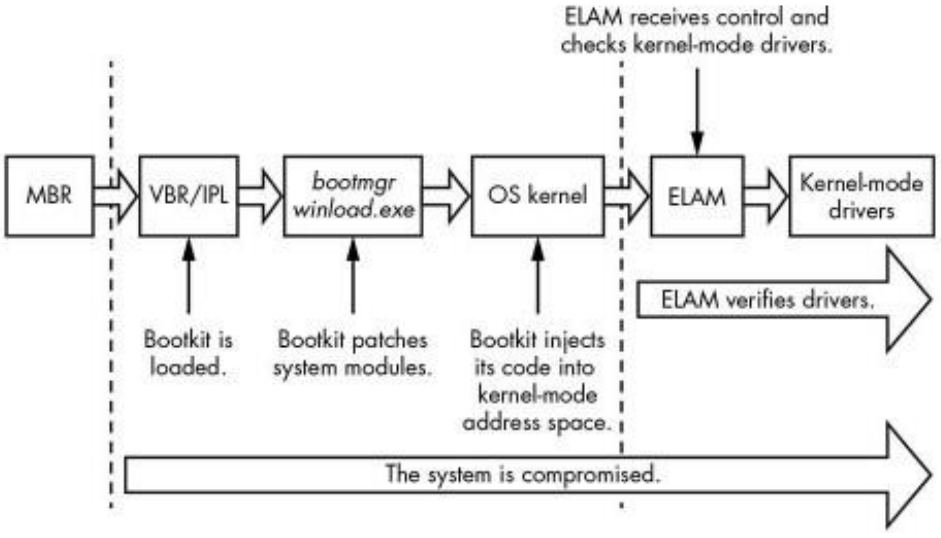


Рис. 3. Поток процесса запуска с ELAM

Большинство буткитов загружает свой код режима ядра в середине инициализации ядра, когда все подсистемы ОС (подсистема ввода/ вывода, диспет-

чер объектов, диспетчер подключаемых модулей и тому подобное) уже проинициализировано, но до выполнения ELAM. ELAM, естественно, не способен препятствовать исполнению того вредоносного кода, который загружается до него, а потому он не обладает никакой защитой против технологий буткитов. [16].

Семейство буткитов ведет себя достаточно скрытно, на зараженной системе его нельзя обнаружить штатными средствами, так как при обращении к зараженным объектам он «подставляет» оригинальные копии. Кроме того, основное тело вредоносной программы (драйвер уровня ядра) не присутствует на файловой системе, а расположено в неиспользованной части диска за границей последнего раздела.

Вредоносная программа загружает драйвер самостоятельно, без помощи операционной системы. Сама же операционная система не подозревает о наличии драйвера. Обнаружение и лечение данного буткита является наиболее сложной задачей из всех, с которыми приходилось сталкиваться специалистам антивирусной индустрии на протяжении нескольких лет. Способом борьбы с буткитами является загрузка системы с любого съемного неинфицированного носителя, чтобы избежать основной загрузки вируса после включения компьютера, и последующая перезапись загрузочного сектора его резервной копией BOOTSECT.BAK, которая всегда находится в корневом каталоге системного тома.

В данной статье была рассмотрена история компьютерных вирусов от доисторического до современного этапов. Подробно рассмотрены такие методы анализа как сигнатурный, эвристический и статистический и способы внедрения вредоносного по в информационные системы, а также, современные методы обнаружения буткитов.

СПИСОК ЛИТЕРАТУРЫ

1. Национальный открытый Университет НОУ «ИНТУИТ». [Электронный ресурс] / - Режим доступа: https://encyclopedia.kaspersky.ru/knowledge/history-of-malicious-programs/

2. Мозаика регресса: обнаружено новое вредоносное ПО для заражения компьютера на низком уровне [Электронный ресурс] / - Режим доступа: https://www.kaspersky.ru/about/press-releases/2020_mozaika-regressa-obnaruzheno-novoe-vredonosnoe-po-dlya-zarazheniya-kompyutera-na-nizkom-urovne
3. История вирусологии [Электронный ресурс] / - Режим доступа: https://www.sites.google.com/site/komputernyevirusy25/istoria-virusologii
4. 1980-е [Электронный ресурс] / - Режим доступа: https://encyclopedia.kaspersky.ru/knowledge/years-1980s/ (дата обращения 13.05.2020)
5. Н. Г. Булахов, В. Т. Калайда - «Методы обнаружения и обезвреживания саморазмножающихся вирусов». 2008 г.
6. А. Н. Горбунов, Т. Г. Емельяненко – «Принципы использования сигнатурного анализа для обнаружения вредоносных программ». 2013 г.
7. What is Signature-Based Malware Detection? [Электронный ресурс] / - Режим доступа: https://www.logixconsulting.com/2020/12/15/what-is-signature-based-malware-detection/
8. А. В. Корнейченко – «Аналитический обзор методов обнаружения вредоносных программ в распределенных вычислительных системах» 2019 г.
9. Эвристический анализ – Heuristic analysis [Электронный ресурс] / - Режим доступа: https://ru.qaz.wiki/wiki/Heuristic_analysis
10. Р. Ю. Демина, И. М. Ажмухамедов – «Повышение эффективности эвристического анализа в антивирусном пакете Stronghold Antimalware» 2018 г.
11. А. К. Рудниченко, М. В. Шаханова – «Актуальные способы внедрения компьютерных вирусов в информационные системы» 2016 г.
12. Unicode (Национальная библиотека им. Н. Э. Баумана Bauman National Library [Электронный ресурс] / - Режим доступа: https://ru.bmstu.wiki/Unicode
13. Sajedul Talukder – «Tools and Techniques for Malware Detection and Analysis» 2020 г.
14. Понимание технологии защиты от вредоносных программ раннего запуска (ELAM) в Windows [Электронный ресурс] / - Режим доступа: https://techarks.ru/general/osobennosti/ponimanie-tehnologii-zashhity-ot-vredonosnyh-programm-rannego-zapuska-elam-v-windows/ (дата обращения 13.05.2020)
15. A. Matrosov, E Rodionov, S. Bratus - «Rootkits and Bootkits Reversing Modern Malware and Next Generation Threats» 2019 г.
16. Безопасность процесса запуска [Электронный ресурс] / - Режим доступа: http://onreader.mdl.ru/RootkitsAndBootkits/content/Ch06.html

УДК 004.056

А. С. СПИРИН, Е. А. БОГДАНОВ, А. И. САФАРОВ, К. В. МИХАЙЛОВ
evgeny.bogdanov.al@gmail.com
Науч. руководв. – канд. техн. наук А. М. ВУЛЬФИН

Уфимский государственный авиационный технический университет

ТЕХНИЧЕСКАЯ РЕАЛИЗАЦИЯ SOC

Аннотация. SOC (Security Operations Center, или Центр обеспечения безопасности) – то, что объединяет людей, процессы и технологии в достижении глобальной цели: снижение рисков через повышение киберзащиты в организации. В данной статье рассмотрен пример реализации SOC с помощью ПО с открытым исходным кодом.
Ключевые слова: SOC; SIEM; реагирование на инциденты; мониторинг; анализ логов.

Введение

SOC — это структурное подразделение организации, которое оказывает услуги мониторинга состояния информационной безопасности. Под мониторингом информационной безопасности понимается централизованный сбор и анализ событий, идентификация инцидентов ИБ, их расследование и последующее реагирование.

Центр мониторинга позволяет решать следующие задачи:

− мониторинг ИБ, выявление инцидентов — утечек информации, нарушений политик, ошибок конфигурации, вторжений в корпоративную сеть и сбоев в работе средств защиты информации;

− технические расследования инцидентов информационной безопасности;

− разработка аналитических записей для устранения причин и драйверов инцидентов;

− управление уязвимостями;

− поддержка средств защиты информации;

− внутренние технические аудиты и простые комплаенс-проверки, тесты на проникновение, процессы выявления индустриального мошенничества;

Если изучить историю развития SOC, то можно узнать, что в период зарождения интернета первые поколения SOC использовались в основном для нужд оборонных предприятий и государственных учреждений. Основной задачей центров тогда была защита организаций от вредоносных программ невысокого уровня сложности. В тот период средства обнаружения и реагирования на инциденты были слабо развиты. Но, по мере развития интернета и технологий, SOC обрастал новыми технологиями: средства обнаружения вторжений, SIEM, средства обнаружения целевых атак, средства эвристического анализа, и т.д. В результате к 2016 году, начинают появляться SOC нового поколения (Next Generation, NG), в которых начали применяться проактивные методы обнаружения угроз.

В данной статье рассмотрена техническая реализация SOC на базе программного обеспечения с открытым исходным кодом.

Архитектура SOC

Архитектуру SOC можно рассматривать в виде отдельных блоков. Основными блоками SOC являются: блок сбора и архивирования, блок анализа событий, блок базы знаний, блок реагирования на инциденты и консоль управления.

Блок сбора и архивирования принимает, классифицирует, нормализует и определяет приоритеты событий. Эти события хранятся в архиве. В блоке анализа происходит корреляция событий на основе правил и паттернов. Правила атак, сигнатуры вирусов и червей хранятся в базе знаний. В блоке реагирования развернуты процедуры сортировки, обработки инцидентов и реагирования, а также процедуры после атаки.

Исходя из этой концепции, возможно построить SOC на базе следующих программных продуктов с открытым кодом. Блок сбора и архивирования: ELK stack, Wazuh, Beats, Suricata, Nessus Essentials. Блок анализа событий: Cortex, The Hive, ELK stack. Блок реагирования на инциденты: The Hive, ElastAlert.

Стек ELK

ELK stack – сокращение от трех проектов с открытым исходным кодом: Elasticsearch, Logstash и Kibana. Elasticsearch — является ядром всей системы, которое сочетает в себе функции базы данных, поисковой и аналитической системы. Logstash — конвейер обработки данных на стороне сервера, который получает данные из нескольких источников одновременно, выполняет парсинг логов, а затем отправляет их в базу данных Elasticsearch. Kibana визуализирует данные из Elasticsearch при помощи диаграмм и графиков. ELK stack дает возможность агрегировать журналы из всех ваших систем и приложений, анализировать эти журналы и создавать визуализации для мониторинга приложений и инфраструктуры, быстрого устранения неполадок, аналитики безопасности и многого другого.

Beats

Beats – набор программ-коллекторов данных с низкими требованиями к ресурсам, которые устанавливаются на клиентские устройства для сбора системных журналов и файлов. Beats подразделяется на модули, которые можно интегрировать по отдельности в стек ELK:

− Filebeat предназначен для сбора данных из системных журналов и файлов, основанных на ОС Linux;

− Packetbeat сетевой анализатор пакетов, который отправляет информацию о сетевой активности;

− Metricbeat предназначен для сбора метрик ОС, характеризующие, состояние системы и сервисов, запущенных на сервере;

− Auditbeat собирает данные инфраструктуры аудита Linux и проверяет целостность файлов;

− Winlogbeat предназначен для сбора данных из журналов событий в Windows-системах.

Wazuh

Wazuh – это бесплатная платформа с открытым исходным кодом для обнаружения угроз, мониторинга безопасности, реагирования на инциденты и соблюдения нормативных требований. Данную платформу можно использовать для мониторинга конечных точек, облачных сервисов и контейнеров, а также для агрегирования и анализа данных из внешних источников. Wazuh предоставляет следующие возможности:

- аналитика безопасности;
- обнаружения вторжений;
- анализ данных журнала;
- мониторинг целостности файлов;
- обнаружение уязвимости;
- реагирование на инцидент.

Wazuh состоит из двух компонентов:

- агент Wazuh позволяет, на отслеживаемом хосте, собирать системные журналы, обнаруживать вторжения, управлять его конфигурацией;
- сервер Wazuh собирает и анализирует данные от агентов.

TheHive

TheHive – это масштабируемая бесплатная SOAR платформа с открытым исходным кодом, разработанная, чтобы облегчить жизнь SOC, CSIRT, CERT и любому специалисту по информационной безопасности, имеющему дело с инцидентами безопасности, которые необходимо расследовать и быстро принимать меры. TheHive поддерживает различные методы хранения данных, файлов и индексов в соответствии с потребностями.

Nessus Essentials

Nessus Essentials является сканером уязвимостей. Он позволяет оценивать системы, сети и приложения на наличие уязвимостей, производить аудит конфигурации и проверку соответствия сетевых активов политикам и отраслевым стандартам.

Cortex

Cortex – программный продукт от той же команды, что и TheHive, и дополняет этот продукт обогащением данных. Cortex позволяет использовать "анализаторы" для получения дополнительной информации о показателях, уже имеющихся в ваших журналах. Он позволяет запрашивать сторонние сервисы по таким индикаторам, как IP, URL и хэш файла, и помечает оповещение этой дополнительной информацией.

Suricata

Suricata – это механизм обнаружения угроз с открытым исходным кодом, разработанный Фондом открытой информационной безопасности (OISF). Suricata может выступать в качестве системы обнаружения вторжений (IDS) и системы предотвращения вторжений (IPS), а также использоваться для мониторинга сетевой безопасности.

Принцип работы SOC, построенного на базе вышеперечисленных программных продуктов, следующий. С хостов на базе ОС Windows собираются журналы ОС при помощи WinlogBeat и Wazuh Agent. С хостов на базе ОС Linux журналы ОС собираются, с помощью Filebeat и Wazuh Agent, метрики ОС, данные о состояния систем и сервисов с помощью Metricbeat. Также Filebeat, при включении модуля Suricata, позволяет получать логи и оповещения от Suricata IDS. Wazuh Agent в свою очередь, помимо сбора журналов, может применяться для автоматического ответа на подозрительные действия в системе. Например, в случае перебора паролей по протоколу SSH, можно заблокировать блокировать IP-адрес злоумышленника, через межсетевой экран (iptables, ipfilter и т.д). Собранные WinLogBeat, Filebeat и Metricbeat журналы поступают в Logstash для их обработки. Wazuh Agent отправляет собранные данные на сервер Wazuh. После агрегации и обработки данные с Logstash и сервера Wazuh поступают в Elasticsearch. Который проводит индексацию данных для оптимизации процесса поиска и хранения. Обработанные и проиндексированные в Elasticsearch данные, можно визиализировать при

помощи Kibana. Также данные могут быть отправлены в ElastAlert для отслеживания событий и генерации оповещений. Оповещения затем передают в The Hive, который используется в качестве платформы управления оповещениями об инцидентах от его создания до закрытия. Инциденты в The Hive могут быть дополнены данными из Cortex.

Заключение

Предложенное решение на базе бесплатного ПО позволяет осуществлять мониторинг, анализ и хранение журналов, генерацию предупреждений и отчетов, управление реагированием на инциденты в составе центра обеспечения безопасности.

СПИСОК ЛИТЕРАТУРЫ

1. Ibrahim Ayadhi «Deploying of infrastructure and technologies for a SOC as a Service» [Электронный ресурс] URL: https://medium.com/@ibrahim.ayadhi/deploying-of-infrastructure-and-technologies-for-a-soc-as-a-service-socass-8e1bbb885149, 2020;
2. Manfred Vielberth, Fabian Böhm, Ines Fichtinger,Günther Pernul «Security Operations Center: A Systematic Study and Open Challenges» [Электронный ресурс] URL: https://www.researchgate.net/publication/347520429_Security_Operations_Center_A_Systematic_Study_and_Open_Challenges, 2020;
3. Tala Tafazzoli, Hossein Gharaee Garakani « Security operation center implementation on OpenStack» [Электронный ресурс] URL: https://www.researchgate.net/publication/315471789_Security_operation_center_implementation_on_OpenStack , 2016;
4. Данил Светлов «Строим SIEM на основе open souce компонентов для анализа логов» [Электронный ресурс] URL: https://xakep.ru/2017/05/04/lightsiem/ 2017.

УДК 004.056

В. Э. ТИМЕРГАЗИН, Р. И. ИЛЬЯСОВА, А. Ю. СЕНЦОВА
regiliasova@mail.ru
Науч. руководитель – канд. техн. наук, доц. А. Ю. СЕНЦОВА

Уфимский государственный авиационный технический университет

ПРОТИВОДЕЙСТВИЕ СХЕМАМ МОШЕННИЧЕСКИХ ДЕЙСТВИЙ С ПОМОЩЬЮ АНТИФРОД-СИСТЕМ

Аннотация. В статье рассматривается необходимость применения в банковских организациях антифрод-систем. В частности, приводится статистика Банка России по мошенническим действиям за период 2019-2020 годов, рассматривается единый концепт работы антифрод-систем. Также разбираются схемы совершения мошеннических действий и предлагаются индикаторы, по которым можно их выявить. Актуальность темы не вызывает сомнений в силу того, что для противодействия мошенничеству и краже конфиденциальной информации почти все банки РФ используют антифрод-системы. Данная сфера сейчас активно развивается, поскольку появляются новые схемы мошеннических действий и объем операций без согласия клиентов постоянно растет. Постоянное совершенствование антифрод-систем является обязательным условием для повышения уровня защищенности банковских систем.
Ключевые слова: антифрод-система; банки, банковские системы; дистанционное банковское обслуживание; мошенничество; транзакция; фрод-мониторинг.

Введение

Проблемы безопасности информации в автоматизированных банковских системах и в системах дистанционного банковского обслуживания особо актуальны на сегодняшний день. Это связано с увеличивающейся популярностью новых платежных технологий и развития платежных инструментов, которые приводят к мошеннической активности в банковской сфере.

Наиболее подвержены мошенничеству операции с банковскими картами, так как они непосредственно взаимодействует с системами дистанционного банковского обслуживания [1]. По данным Банка России в 2020 году, по сравнению с 2019 годом, объем операций осуществленных без согласия клиентов посредством мошенничества через банкоматы, терминалы и импринтеры в России составил около 239 млн рублей, против 268 млн рублей, через оплату товаров и услуг в интернете составил 2048 млн рублей против 1272 млн, через системы дистанционного банковского обслуживания (ДБО) физических лиц и юридических лиц составил 1711 млн рублей против 1156 млн рублей. Суммар-

ный объем мошеннических операций в 2020 году составил около 4 млрд рублей против 2,7 млрд рублей в 2019 [2], что говорит об увеличении объема операций без согласия клиентов. Возникает необходимость проводить дополнительные проверки для подтверждения данного платежа [3].

В целях предотвращения мошеннических действий, а также противодействия хищений конфиденциальной информации клиентов в финансовой сфере, в частности онлайн-банкинге, прибегают к антифрод-системам. Эти системы занимаются оценкой вероятности того, что совершенная транзакция была осуществлена мошенниками, а не держателем карты.

Алгоритм работы антифрод-систем

Большинство антифрод-систем работают по единому концепту, состоящему из 5 основных модулей [4]:

– отслеживание действий клиента;

– автоматизированная проверка транзакций (при помощи любых методов: от эвристических до машинного обучения);

– оценка мошеннического риска;

– управление пользователями при помощи специально-разработанных интерфейсов;

– хранение базы данных о действиях клиента.

Если система обнаруживает подозрительные действия пользователя, то она принимает одно из следующих решений:

– отправить транзакцию на дополнительную проверку специалисту антифрод мониторинга;

– прекратить транзакцию без формирования инцидента;

– прекратить транзакцию, заблокировать операции по счету клиента и сформировать инцидент.

Выделяют транзакционный, сессионный и комбинированные антифрод-системы.

Транзакционный антифрод занимается обработкой данных внутрибанковских систем. Основной задачей данного типа антифрод-систем является выявление тех транзакции, которые не соответствуют обычным операциям клиентов (выявление отклонений от типичного поведения пользователей) на основе анализа платежных операций и неплатежных активностей клиента (неуспешные попытки входа в ДБО, фиксация перемещений пользователя по страницам личного кабинета, изменение информации о себе в кабинете, дата, время и геолокация проведения платежных операций.), а также анализ платежей по «черным спискам».

Еще одной задачей транзакционного антифрода является корреляция событий, которые показались незаконными аналитикам через систему сбора и обработки информации, а также анализ существующих мошеннических систем и работа с подозрительными операции и/или информирование о них клиентов.

Сессионный антифрод, на основе собранных обезличенных данных о пользователе, устройстве, о его окружении помогает фиксировать данные во время пользовательских сессиях и выявлять создание мошеннических сессий. Информация о денежных транзакциях, такие как сумма операций, реквизиты - не собираются.

Совместную работу транзакционного и сессионного антифрода называют комбинированной. Эта связка помогает комплексно подходить к защите средств клиентов и оптимизировать работу с любыми мошенническими действиями, в том числе, с использованием социальной инженерии [5].

Индикаторы мошеннических операций

Антифрод-системы постоянно совершенствуются, расширение функционала и увеличение количества методик, применяемых в таких системах, приводит и к усовершенствованию мошеннических схем, используемых злоумышленниками.

Распознавание пользователя по различным параметрам производится посредством машинного обучения. Одним из примеров использования средства

машинного обучения является составление шаблонов поведения пользователя на основе алгоритмов кластеризации, с помощью фиксации суммы операций и покупок. Аномалиями будут считаться операции с одной суммой в разных местах, переводы маленьких сумм на разные счета.

Для создания и использования системы фрод-мониторинга на основе машинного обучения необходимо определить специальные индикаторы для того, чтобы система могла определять является ли данная операция мошеннической или является легитимной [1].

При выборе критериев для построения модели предотвращения мошеннических действий предлагается рассмотреть схемы мошеннических действий и ответные реакции:

1. Нарушители для преодоления лимита платежа выводят денежные средства большим количеством мелких операций. Для предотвращения данного типа мошенничества возможно использование счетчика количества транзакций за фиксированное время (15 минут - краткосрочный промежуток времени и 1 час – долгосрочный промежуток);

2. Нарушители выполняют транзакции из стран черного списка (с высоким уровнем мошеннических действий), выводят денежные средства в другую страну, инициализируют транзакции из разных стран за короткий промежуток времени. Для противодействия данной схеме мошенничества возможно сравнение геолокации устройства пользователя и шаблона пользователя, если данный тип операций нормальный для клиента, при инициализации транзакции.

3. Нарушители с использованием методов социальной инженерии выведывают данные карт клиентов, а после для обхода систем фрод-мониторинга крадут денежные средства путем «маскировки» источника и суммы платежа под обыденные для пользователя транзакции (например, платные подписки на музыку, продовольственные магазины, кафе). С помощью обучения антифрод-системы стандартным суммам платежа для соответствующих категорий покупок можно уменьшить влияние такого сценария атаки на платежную систему

банка. Также можно установить определенное количество транзакций из одной категории в определенный период времени.

4. Злоумышленники при помощи мошеннических программ списывают денежные средства по имеющейся базе данных платежных карт. В данном случае можно использовать индикатор проверки одинаковых и математически отличающихся транзакций на один счет с разных карт за определенный период времени.

Мошеннические операции могут возникать и со стороны работников банковской сферы. Для определения вышеупомянутых действий, со стороны сотрудников возможно использование следующих индикаторов [1]:

– мониторинг досрочного закрытия депозитных счетов и вкладов клиентов;

– отмена ошибочных операций по приходу и расходу в течение одного операционного дня;

– совершение операций по счетам клиентов, длительное время не использующих денежные средства;

– совершение операций по счетам клиентов, попадающих в зону повышенного риска: несовершеннолетние лица, пенсионеры, лица, получающие социальные пособия и пр.;

– массовая выдача кредитных карт, оформление вкладов за короткий промежуток времени на большие суммы.

Выводы

Благодаря антифрод-системам оперативно выявляются подозрительные транзакции и предотвращается потеря денежных средств клиентов.

Банковское мошенничество останется довольно актуальной проблемой еще очень долго, но внедрение банками антифрод-систем может колоссально снизить количество мошеннических действий. Сегодня существует большое разнообразие антифрод-систем от различных производителей: Featurespace, FICO Application Fraud Manager, FraudWall (компания Фродекс) и другие.

СПИСОК ЛИТЕРАТУРЫ

1. Разина, О.М., Костерина Т.М. Инновационные инструменты фрод-мониторинга в практике внутреннего аудита банка, 2015.
2. Банк России // Обзор отчетности об инцидентах информационной безопасности при переводе денежных средств, 2020 [Электронный ресурс]. – Режим доступа: https://cbr.ru/analytics/ib/review_1q_2q_2020/
3. Левашов М.В., Овчинников П.В. Эффективность классификаторов для выявления фрода в финансовых транзакциях, 2019.
4. Кудряшова О.А., Ильина А.В. Аналитическая система антифрод как комплекс мер для оценки риска финансовых транзакций // Актуальные вопросы экономической теории: развитие и применение в практике российских преобразований: материалы VII междунар. науч.-практ. конф. Уфа: УГАТУ, 2018. С. 193-196.
5. Itweek, 2020 [Электронный ресурс]. – Режим доступа: https://www.itweek.ru/security/news-company/detail.ph..

УДК 004.056

В. В. УРАЗАЕВ
v.urazaev@yandex.ru
Науч. руководов. – канд. техн. наук, проф. Т. А. ИВАНОВА

Уфимский государственный авиационный технический университет

ПОПУЛЯРНЫЕ ТЕХНИКИ АТАК ПРОГРАММ-ВЫМОГАТЕЛЕЙ ПО КЛАССИФИКАЦИИ MITRE ATT&CK

Аннотация. В статье рассматривается использование матрицы MITRE ATT&CK для описания популярных техник атак программ-вымогателей в 2020 году.
Ключевые слова: программа-вымогатель; уязвимость; техника атаки; MITRE ATT&CK; ransomware.

MITRE — это некоммерческая организация, которая работает в США и управляет центрами исследований и разработок на уровне федерального правительства и местного самоуправления. В зону интересов MITRE входят: искусственный интеллект, квантовая информатика, информатика в области здравоохранения, космическая безопасность, обмен данными о киберугрозах и средствах защиты.

Одним из наиболее популярных проектов компании является MITRE ATT&CK (Adversarial Tactics, Techniques and Common Knowledge). Проект представляет собой структурированный список известных техник, приемов и тактик злоумышленников, представленный в виде таблиц.

MITRE представил матрицу ATT&CK в 2013 году как способ описания и категоризации поведения злоумышленников (составления паттернов поведения) на основе реальных наблюдений. Она описывает 3 ключевых понятия:

– Тактика – действия злоумышленника на разных этапах своей операции, определяет цель или задачу злоумышленника на определенным шаге (например, TA0002 Execution – исполнение вредоносного код на атакуемой машине);

– Техника – каким образом злоумышленник достигает цели или поставленной задачи и какие, при этом, использует инструменты, технологии,

эксплоиты (например, субтехника T1059.001 PowerShell – злоупотребление командами и сценариями PowerShell);

– Процедура — как выбранная техника выполняется и для чего (например, вредоносная программа, используя PowerShell, скачивает полезную нагрузку, которая, в свою очередь, подгружает Cobalt Strike для попытки запуска на удаленных хостах).

Описанные в матрице MITRE ATT&CK техники позволяют построить модели возможных атак на информационную систему и разработать решения, направленные на анализ и защиту системы от атак.

Компания Group-IB – один из ведущих разработчиков в сфере кибербезопасности – в марте этого года выпустила отчет, в котором анализирует растущую активность программ-вымогателей (ransomware). В отчете описываются совершенные в 2020 году атаки на информационные системы с целью получения прибыли, а также вероятные перспективы развития программ-вымогателей. В этом же отчете приводится топ 10 популярных техник, используемых для атак вымогателей.

1. External Remote Services (Внешние удаленные службы) - T1133.

Общедоступные серверы RDP по-прежнему являются наиболее частой целью для многих авторов программ-вымогателей, от Dharma до REvil. В связи с пандемией COVID-19, которая перевела многих людей на работу из дома, количество таких серверов начало расти в геометрической прогрессии. Многие успешные вторжения начинались с подбора пароля или заполнения учетных данных – субтехник Brute Force (T1110).

Во большинстве случаев программа-вымогатель была развернута после установления RDP-подключения к скомпрометированному серверу с последующим распространением на один из контроллеров домена.

Серверы RDP - не единственные внешние удаленные сервисы, на которые злоумышленники нападают с брутфорс атак. Такие атаки были также инициированы против устройств VPN, не имеющих многофакторной аутентификации.

Как обезопасить систему?

– Отключить ненужные внешние удаленные сервисы;

– Установить политики блокировки учетной записи для предотвращения подбора пароля;

– Использовать двух- или многофакторную аутентификацию для таких услуг;

– Организовать сбор и мониторинг журналов внешних удаленных служб на предмет несанкционированного доступа.

2. Command and Scripting Interpreter (Интерпретатор команд и сценариев) - T1059.

Поскольку многие злоумышленники на начальном этапе доступа часто использовали вредоносные вложения электронной почты, также широко использовалось множество различных интерпретаторов, включая PowerShell (T1059.001), Windows Command Shell (T1059.003), Visual Basic (T1059.005) и JavaScript/Jscript (T1059.007).

Поскольку многие злоумышленники использовали постэксплуатационные или C2-фреймворки (включая Cobalt Strike и PowerShell Empire), интерпретатор PowerShell также использовался для сетевой разведки, бокового перемещения и даже кражи данных на контролируемые злоумышленником серверы.

Windows Command Shell также была чрезвычайно популярна, особенно на начальном этапе доступа. Например, в недавних кампаниях операторы Emotet выполняли сценарий много раз, чтобы избежать обнаружения.

Visual Basic использовался для вооружения тысяч документов с помощью вредоносных макросов, но некоторые злоумышленники также использовали сценарии VB, обычно в заархивированной форме, в качестве вложения электронной почты, чтобы побудить жертву загрузить исходную полезную нагрузку.

Использование же JavaScript/Jscript было направлено, например, на поддельное обновление от SocGholish, которое распространялось в виде заархивированного файла Jscript.

Как обезопасить систему?

– Настроить разрешение выполнения только подписанных сценариев PowerShell;

– Удалить PowerShell с конечных ПК, на которых он не используется;

– Создать список разрешений для известных скриптов и блокировки выполнение неизвестных;

– Отслеживать сетевую инфраструктуру на предмет подозрительного и вредоносного выполнения powershell.exe, cscript.exe или wscript.exe и изменений в политике выполнения PowerShell.

3. Scheduled Task/Job (Запланированные задачи) - T1053.

Запланированные задачи широко использовались для обеспечения постоянства на хостах, которые уже были скомпрометированы, но это был не единственный вариант использования этого метода. Филиалы Maze создали запланированные задачи, замаскированные под обновления безопасности, для запуска программы-вымогателя в определенное время.

Как обезопасить систему?

– Ограничить права учетной записи пользователя, чтобы только авторизованные администраторы могли создавать запланированные задачи;

– Следить за созданием новых запланированных задач и уметь определять подозрительные и вредоносные задачи.

4. Valid Accounts (Действительные учетные записи) - T1078.

Поскольку многие вторжения начинались с несанкционированного доступа по протоколу RDP или использования общедоступного приложения, злоумышленники получали учетные данные с различными уровнями привилегий во время первоначального доступа. Злоумышленники использовали эти учетные данные (или те, которые были собраны на этапе доступа к учетным данным) для получения избыточного доступа к скомпрометированной инфраструктуре.

Как обезопасить систему?

– Убедиться, что не используются учетные данные по умолчанию или ненадежные учетные данные, особенно для общедоступных приложений;

– Отслеживать учетные записи на предмет аномальной активности, например, внешних подключений RDP с необычных IP-адресов.

5. Process Injection (Внедрение кода в процессы) - T1055.

Частое использование массовых вредоносных программ, а также фреймворков для постэксплуатационных работ сделало внедрение кода в процессы одним из наиболее распространенных методов, используемых в 2020 году.

Первой популярной подтехникой было внедрение динамически подключаемых библиотек (T1055.001). Например, SDBbot часто вставлял свою DLL во вновь созданный процесс rundll32.exe. То же самое можно сказать и о многих образцах программ-вымогателей. Например, Netwalker внедрял свою DLL в процесс explorer.exe.

Другой популярной подтехникой было выдалбливание процесса (Process Hollowing, T1055.012). Trickbot использовал эту подтехнику для внедрения полезной нагрузки в svchost.exe. Bazar Loader сделал то же самое, но с помощью другой подтехники – двойника процесса (Process Doppelganging, T1055.013).

Также наблюдались менее распространенные подтехники, в том числе использование асинхронного вызова процедур (Asynchronous Procedure Call, T1055.004) для внедрения кода. Dridex использовал глобальные атомные таблицы Windows и асинхронные вызовы процедур для внедрения кода в удаленный процесс.

Как обезопасить систему?

– Необходимо убедиться, что используемые решения по обеспечению безопасности конечных ПК способны обнаруживать и блокировать хотя бы распространенные методы внедрения вредоносного кода в процессы.

6. Brute Force (Метод грубой силы / перебора) - T1110.

Как упоминалось ранее, многие операторы программ-вымогателей получили свои первые позиции через RDP. Чтобы получить действительные учет-

ные данные, злоумышленники использовали угадывание пароля (Password Guessing, T1110.001), распыление пароля (Password Spraying, T1110.003) и заполнение учетных данных (Credential Stuffing, T1110.004).

Наиболее популярными инструментами для атак методом перебора были NLBrute и Hydra. В некоторых случаях NLBrute также использовался, чтобы проверить, действительны ли полученные учетные записи для всего предприятия.

Взлом паролей (Password Cracking, T1110.002) также был популярен. Во время постэксплуатации злоумышленники могут извлекать хэши паролей из ntds.dit для дальнейшего взлома в автономном режиме. Trickbot даже получил модуль для сброса базы данных Active Directory через ntdsutil, а также различные файлы реестра, необходимые для взлома.

Как обезопасить систему?

– Установить политики блокировки учетной записи для предотвращения подбора пароля;

– Использовать двух- или многофакторную аутентификацию для таких услуг;

– Смотреть рекомендации NIST при создании политик паролей;

– Делать упреждающий сброс скомпрометированных учетных записей после обнаружения попыток перебора.

7. OS Credential Dumping (Выгрузка учетных данных ОС) – T1003.

Выгрузка учетных данных оставалась наиболее распространенным методом, используемым операторами программ-вымогателей для получения действительных привилегированных учетных данных и горизонтального перемещения. Основываясь на наблюдениях Group-IB, тремя наиболее распространенными инструментами были ProcDump, Mimikatz и LaZagne.

Злоумышленники обычно использовали ProcDump для дампа памяти процесса службы Local Security Authority Subsystem Service (LSASS Memory, T1003.001). Mimikatz позволял злоумышленникам использовать различные

вспомогательные методы выгрузки учетных данных, включая LSASS Memory, менеджер учетных записей безопасности (Security Account Manager, T1003.002), секреты Local Security Authority (LSA Secrets, T1003.004) и кэшированные учетные данные домена (Cached Domain Credentials, T1003.005).

Благодаря расширенным возможностям, LaZagne использовался не только для выгрузки учетных данных, но и для извлечения учетных данных из различных систем хранения (например, веб-браузеров).

Некоторые злоумышленники, такие как операторы программ-вымогателей Ryuk, раскрыли файл NTDS с помощью ntdsutil (NTDS T1003.003). Другой пример - операторы программы-вымогателя Pysa, которые обращались к файлам NTDS с помощью теневого копирования тома.

Как обезопасить систему?

– Включить Credential Guard для защиты секретов LSA (применимо для Windows 10);

– Отключить хранение паролей WDigest в памяти;

– Убедиться, что учетные записи локального администратора имеют уникальные пароли на разных хостах;

– Включить Protected Process Light для LSA (применимо для Windows 8.1 и Windows Server 2012 R2);

– Отключить или ограничить NTLM;

– Обеспечить защиту резервных копий контроллера домена, если таковые имеются;

– Добавить пользователей в группу безопасности «Защищенные пользователи», чтобы ограничить доступ к учетным данным.

8. Remote System Discovery (Удаленное обнаружение системы) – T1018.

Поскольку операторы программ-вымогателей сосредоточились на атаках корпоративных сетей, злоумышленники обычно собирали информацию об Active Directory, в том числе о пользователях, группах и доверительных отношениях доменов.

Одним из наиболее распространенных инструментов для сбора вышеупомянутой информации был AdFind. Другим распространенным инструментом разведки Active Directory был BloodHound (SharpHound), который также позволял злоумышленникам собирать и анализировать информацию о пользователях, группах и доверии доменов.

Прежде чем начать боковое движение, злоумышленники иногда выполняли сканирование портов (Network Service Scanning, T1046). Наиболее распространенными инструментами были Advanced Port Scanner и SoftPerfect Network Scanner. В некоторых случаях злоумышленники использовали возможности сканирования портов постэксплуатационных фреймворков, таких как Cobalt Strike или Metasploit.

Операторы программ-вымогателей использовали обнаружение общего доступа к сети (Network Share Discovery, T1135) как для сбора информации для дальнейшего использования, так и для определения потенциальных целей для бокового движения.

Как обезопасить систему?

– Использовать распространенные инструменты разведки Active Directory;

– Знать, как обнаружить использование распространенных постэксплуатационных фреймворков;

– Проверить, правильно ли защищены конечные ПК от массового вредоносного ПО.

9. Remote Services (Удаленные службы) – T1021.

RDP (Remote Desktop Protocol, T1021.001) был не только наиболее распространенным вектором начального доступа, но и распространенным способом горизонтального перемещения по сети. В своих арсеналах некоторые операторы программ-вымогателей даже имели сценарии для включения RDP на удаленных хостах. Обычно они выполнялись через PsExec.

Субтехника блока сообщений сервера (SMB/Windows Admin Shares, T1021.002) также использовалась из-за популярности PsExec и постэксплуатационных фреймворков, таких как Cobalt Strike, который включает аналогичные возможности для горизонтального перемещения с полезной нагрузкой Beacon.

Ряд фреймворков постэксплуатации также позволил злоумышленникам использовать как распределенную компонентную объектную модель (Distributed Component Object Model, T1021.003), так и удаленное управление Windows (Windows Remote Management, T1021.006) для горизонтального перемещения. Во время одной из встреч Group-IB с операторами Maze по реагированию на инциденты, компания стала свидетелем того, как группа злоупотребляла удаленным управлением Windows (WinRM) с помощью Cobalt Strike.

Операторы RansomEXX также атаковали инфраструктуру Linux, поскольку у них были соответствующие версии программ-вымогателей. Злоумышленники обычно использовали Secure Shell (SSH, T1021.004) для доступа и горизонтального перемещения через такие инфраструктуры.

Как обезопасить систему?

– Ограничить членство в группе пользователей удаленного рабочего стола;

– Отслеживать массовые события включения RDP;

– Отключить RDP на рабочих станциях и серверах там, где это не нужно;

– Следить за инфраструктурой на предмет подозрительных событий выполнения PsExec и аналогичных инструментов;

– Убедиться, что пароли локального администратора не используются повторно в масштабах всего предприятия;

– Использовать многофакторную аутентификацию для SSH-соединений.

10. Data Encrypted for Impact (Шифрование данных для воздействия) – T1486.

Основной целью операторов программ-вымогателей было зашифровать данные. Многие семейства программ-вымогателей распространялись через программы RaaS, и, поскольку каждая программа имеет несколько филиалов, могут быть изменения в TTP, используемых злоумышленниками. Некоторые программы (например, REvil, Netwalker и DarkSide) были общедоступными, в то время как другие (например, Ryuk, DoppelPaymer и Egregor) не были.

Перед фактическим развертыванием программы-вымогателя операторы старались найти и удалить все доступные резервные копии, чтобы жертва не могла восстановить зашифрованные данные (Inhibit System Recovery, T1490). В то же время в большинстве образцов программ-вымогателей были встроенные команды для отключения или удаления функций восстановления системы. Например, Netwalker использовал WMI для удаления теневых копий тома.

Как правило, два фактора заставляли жертв платить операторам программ-вымогателей. Во-первых, у компаний не было резервных копий для восстановления зашифрованных критически важных данных. Во-вторых, конфиденциальные данные были украдены и могут быть опубликованы в Интернете. Некоторые злоумышленники использовали другие методы вымогательства. Например, филиалы Suncrypt проводили DDoS-атаки (Service Stop, T1498) против своих жертв, чтобы заставить их быстрее принять «правильное решение».

Матрица MITRE ATT&CK является обширным описанием техник и субтехник, которые были применены для организации атак на информационные системы. Знание наиболее популярных техник и понимание их принципов позволяет повысить уровень безопасности обслуживаемой инфраструктуры без необходимости глубокого изучения всех 400 представленных техник и субтехник. Однако следует не забывать, что MITRE ATT&CK лишь предоставляет информацию об уже проведенных атаках, а значит необходимо обдуманно планировать и организовывать защиту информационной системы.

СПИСОК ЛИТЕРАТУРЫ

1. ATT&CK Matrix for Enterprise: [Электронный ресурс] // URL: https://attack.mitre.org. (Дата обращения 23.09.2021).
2. Матрица ATT&CK. Как устроен язык описания угроз и как его используют: [Электронный ресурс] // «Хакер» - Безопасность, разработка, DevOps. URL: https://xakep.ru/2021/03/17/mitre-att-ck. (Дата обращения 23.09.2021).
3. Что такое MITRE ATT&CK: [Электронный ресурс] // Энциклопедия «Касперского». URL: https://encyclopedia.kaspersky.ru (Дата обращения 24.09.2021).
4. Annual Ransomware Report: [Электронный ресурс] // Ransomware Uncovered 2020/2021. URL: https://explore.group-ib.com/ransomware-reports/ ransomware_uncovered_2020. (Дата обращения 24.09.2021).

УДК 004.056

Р. Р. ФАХРЕТДИНОВ, В. А. КУЛАГИН
rusel1362@gmail.com
Науч. руководв. – канд. техн. наук, проф. К. В. МИРОНОВ

Уфимский государственный авиационный технический университет

ОБЗОР СИСТЕМ ПРОТИВОДЕЙСТВИЯ БАНКОВСКОМУ МОШЕННИЧЕСТВУ (АНТИФРОД)

***Аннотация*.** В данной статье рассмотрены существующие на мировом рынке системы противодействия банковскому мошеничеству, а также их функции и способы обнаружения.
***Ключевые слова*:** антифрод; ДБО; мошенничетсво; кибератаки; компоненты.

С тех пор как многие банковские и платежные операции перешли в область информатизации, мошенничество в этой сфере активно развивается. Наиболее известные атаки на банковские системы за последние несколько лет были выполнены преступными группировками Cobalt, Carbanak, Lazarus и Lurk. По оценкам Сбербанка, убытки России от кибератак составляют порядка 650 млрд рублей в год. При этом только в первые две недели 2019 года Сбербанк подвергся 18 кибератакам. Злоумышленники производят атаки на системы межбанковских переводов, карточный процессинг, управление банкоматами, интернет-банкинг и платежные шлюзы.

По данным отчета Positive Technologies, злоумышленники используют простой сценарий для совершения атаки, который состоит из 5 последовательных этапов:

- Предварительная разведка и подготовительные работы.
- Проникновение во внутреннюю сеть.
- Закрепление во внутренней сети и развитие атаки.
- Компрометация банковских систем и хищение средств.
- Сокрытие следов.

Эти этапы актуальны при фишинге, заражении компьютера или смартфона жертвы известным ранее вредоносом, проведении атак типа man-in-the-middle, использовании кейлогеров и даже уязвимостей нулевого дня.

Специалисты Group-IB выделили 7 распространенных схем хищения денежных средств при атаках на системы дистанционного банковского обслуживания (ДБО):

- Социальная инженерия.
- Переводы с карты на карту.
- Переводы через онлайн-банкинг.
- Перехват доступа к мобильному банкингу.
- Поддельный мобильный банкинг.
- Покупки с помощью Apple Pay и Google Pay.

Мировой рынок систем противодействия банковскому мошенничеству

В 2018 году мировой рынок систем противодействия мошенничеству был оценен в 13,59 млрд долларов США. По прогнозам на 2024 год, масштаб должен достигнуть 31,15 млрд долларов США (CAGR = 16,42 %). Это связано с повышением возможностей мошенничества из-за увеличения количества транзакций (как денежных, так и ориентированных на информацию), технологических достижений, а также общей цифровизации финансового сектора.

По отчетам Markets and Markets, основными поставщиками систем противодействия банковскому мошенничеству по всему миру являются следующие компании:

- IBM (США);
- FICO (США);
- SAS Institute (США);
- BAE Systems (Великобритания);
- NICE Systems (Израиль);
- LexisNexis Risk solutions (США)

Рынок систем противодействия банковскому мошенничеству в России

Рынок антифрод-систем в России прошел несколько характерных ступеней развития. Эволюционными прорывами были такие важные вехи, как появление Chip Liability Shift в 2007 — 2008 гг., а до этого появление стандарта

мониторинга операций по банковским картам от Visa в 2003 г., которые дали толчок компонентам антифрод-систем в процессинге.

В 2011-2012 гг. произошла массовая серия атак на ДБО, поначалу затронувших преимущественно юридических лиц и впоследствии распространившихся на граждан.

В 2014-2015 гг. банковский троян Lurk и другие вредоносные программы дали толчок к появлению российских решений от компаний Group-IB и «Лаборатории Касперского».

В 2018 г. принятый Федеральный закон от 27.06.2018 № 167-ФЗ «О внесении изменений в отдельные законодательные акты РФ в части противодействия хищению денежных средств» [1] вновь накалил вопрос об антифрод-системах, особенно для тех представителей кредитно-финансового сектора, для которых акты реализации транзакционного мошенничества были невелики и по факту измерялись ниже стоимости самих антифрод-решений.

По данным Сбербанка, за 2018 год с помощью внедренной антифрод-системы удалось сохранить более 32 млрд рублей, принадлежащих вкладчикам.

Функции систем противодействия банковскому мошенничеству

Процесс обнаружения и предотвращения мошенничества не имеет начальной или конечной стадии, он должен выполняться непрерывно и включать в себя следующие подпроцессы:

- Мониторинг;
- Обнаружение;
- Принятие решений;
- Обучение.

Системы противодействия мошенничеству могут иметь в своем арсенале следующие технологии и возможности: Текстовая аналитика, которая выполняется с помощью технологий поиска, категоризации контента и извлечения сущностей. Расчет статистических параметров, который используется для выявления отклонений, которые могли бы указать на мошенничество. Сетевая анали-

тика, которая используется для идентификации соединений, выявления закономерностей. Gap-тестирование подразумевает обнаружение любых недостающих элементов в последовательных данных там, где их не должно быть. Подтверждение даты входа используется для оценки неподходящего или подозрительного времени для размещения или ввода информации. Контролируемое машинное обучение, которое производится на основе исторических данных, что позволяет выявлять определенные шаблоны. Обучение без учителя, что подразумевает анализ и оценку данных, которые не содержат сведений о выявленном мошенничестве. Используется для выявления новых аномалий.

Функция у всех антифрод-систем едина — выявлять и предотвращать мошенничество. Однако они могут по-разному решать данную задачу и сравнивать антифрод-системы без проведения дополнительной классификации является неверным решением. Так, например, есть так называемые core-системы — мощные аналитические платформы, позволяющие реализовывать логику в отдельных сегментах (ДБО или процессинг банковских карт), также существуют специализированные системы, контролирующие параметры устройств и риски на их стороне. И в то же время разрабатываются отдельные системы, заточенные под распознавание фото, видео, речи. Многие из систем не конкурируют, а, наоборот, дополняют функции друг друга. Например, конкретное узкоспециализированное решение не может само по себе закрывать требования Федерального закона от 27.06.2018 № 167-ФЗ «О внесении изменений в отдельные законодательные акты РФ в части противодействия хищению денежных средств» [1] и существовать как независимая платформа.

Исходя из этого мы разделили существующие системы противодействия банковскому мошенничеству на 3 класса:

1 класс. Решения данного класса направлены на выявление и идентификацию следов мошенничества и выявление аномалий.

2 класс. Решения данного классы направлены на идентификацию инструментов мошенничества, причины или риска (например, наличие вредоносных программ, компонентов удаленного управления, компонентов фишинга).

3 класс. Решения данного класса решают узкоспециализированные задачи. В частности, они могут быть предназначены для распознавания изображений для выявления мошенничества, могут быть оснащены системой распознавания речи.

Краткий обзор систем противодействия банковскому мошенничеству

Далее будет рассмотрено 4 вида систем противодействия банковскому мошенничеству:

1). Комплексные системы обнаружения банковского мошенничества и выявления аномалий;

2). Системы идентификации инструментов банковского мошенничества;

3). Узкоспециализированные системы обнаружения признаков банковского мошенничества;

4). Смешанные системы противодействия банковскому мошенничеству.

К комплексным системам обнаружения банковского мошенничества и выявления аномалий можно отнести следующие:

FraudWall. Систему FraudWall от компании «Фродекс» можно отнести к классу общеаналитических платформ. Она предназначена для предотвращения кражи средств клиента в системах дистанционного банковского обслуживания (ДБО), борьбы с внутренним мошенничеством (например, несанкционированные платежи в АБС), предотвращения кражи средств банка через АРМ КБР. Когда система выявила подозрительный платеж, она совершает звонок клиенту и ведет с ним живое общение, распознавая ответы клиента. По завершению звонка FraudWall принимает решение об исполнении платежа или остановке операции.

IBM Safer Payments [11]. Решение IBM Safer Payments от компании IBM относится к общеаналитическим платформам. Оно разработано на основе платформы IRIS после приобретения компанией IBM компании IRIS Analytics. Си-

стема предназначена для обнаружения попыток мошенничества в реальном времени. При этом обеспечивается безопасность как при проведении безналичных платежей во многих системах (автоматизированные расчетные палаты, банки-эквайеры, Единая зона платежей в евро, Chip & Pin и других), так и через торговые терминалы, банкоматы, онлайн- и мобильные банки.

К системам идентификации инструментов банковского мошенничества можно отнести следующие:

Kaspersky Fraud Prevention [20]. Решение Kaspersky Fraud Prevention от «Лаборатории Касперского» предназначено для решения проблемы цифрового мошенничества в онлайн-банкинге, ритейле, государственных сервисах, онлайн-играх и других отраслях, использующих веб-сайты и мобильные приложения для предоставления своих услуг.

WEB ANTIFRAUD [23]. Система направлена на предотвращение кражи пользовательских аккаунтов в онлайн-сервисах. Для этого используется формирование отпечатка и анализ устройства пользователя, анализ поведения на сайте, поиск присутствия троянов в браузерах (в том числе автоматический перевод средств и MITB атаки), поиск принадлежащих одному владельцу аккаунтов (в целях реализации мер по предотвращению отмывания денег, AML), а также другие технические инструменты, препятствующие деятельности мошенников на сайте онлайн-сервиса. Антифрод решение WEB ANTIFRAUD работает автоматически без участия человека, но при необходимости предоставляет подробную аналитику по произошедшим инцидентам. WEB ANTIFRAUD помогает принять решение о необходимости двухфакторной аутентификации в каждом конкретном случае, а также сообщает об инцидентах безопасности и признаках кражи аккаунтов.

К узкоспециализированным системам обнаружения признаков банковского мошенничества можно отнести следующие:

FPS.Bio. Система противодействия банковскому мошенничеству FPS.Bio от компании «ВижнЛабс» относится к классу узкоспециализированных плат-

форм. Система разработана на базе решения по биометрической верификации и идентификации физических лиц. Ядром FPS.Bio является нейронная сеть, которая, по словам разработчиков, использует уникальные алгоритмы. К функциям системы относится формирование биометрического портрета клиента, сравнение его с миллионами аналогичных портретов и предоставление результатов для принятия решений.

SmartTracker.FRAUD. Программно-аппаратный комплекс фотобиометрический идентификации SmartTracker.FRAUD позволяет заменить проверку подлинности документов и предоставленной клиентами банка информации на совершено другой метод, основанный на контроле идентификации внешности (той информации, которую человек не может подделать).

К смешанным системам противодействия банковскому мошенничеству можно отнести следующие:

RSA Adaptive Authentication and Transaction Monitoring. Данная система от компании RSA относится к классу общеаналитических платформ 1 класса, но включает в себя возможности и 2 класса. Система позволяет выявлять попытки мошенничества в режиме реального времени и производит мониторинг транзакций после входа пользователя в систему, что позволяет защититься от атак типа MITM и MITB. При этом RSA Transaction Monitoring and Adaptive Authentication может быть внедрена как на серверах организации, так и использоваться в качестве облачного сервиса.

Заключение

Мошенничество в банковской сфере продолжает прогрессировать с каждым годом. А потому растет рынок систем противодействия банковскому мошенничеству. Лидерами в данной сфере являются США. Однако обеспечение безопасности от фрода актуально и для российских финансовых организаций. При выборе системы противодействия мошенничеству необходимо в первую очередь определиться с тем, какие задачи ей следует выполнять. В большинстве

случаев для того чтобы защитить банк от мошенничества, потребуется использование антифрод-систем нескольких классов.

СПИСОК ЛИТЕРАТУРЫ

1. ФЗ Российской Федерации №167-ФЗ О внесении изменений в отдельные законодательные акты РФ в части противодействия хищению денежных средств [Текст] : Федеральный закон от 27 июня 2018 г.
2. Отчет “Атаки на банки” от компании Positive Technologies [Электронный ресурс] / – Режим доступа: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Banks-attacks-2018-rus.pdf
3. Международная компания Group-IB [Электронный ресурс] / – Режим доступа: https://www.group-ib.ru/
4. Отчет Markets and Markets [Электронный ресурс] / – Режим доступа: https://www.marketsandmarkets.com/PressReleases/fraud-detection-prevention.asp
5. Газета Коммерсантъ, статья от 28.11.2017, “Сбербанк оценил ежегодные убытки российской экономики от кибератак в 650 млрд рублей” [Электронный ресурс] / – Режим доступа: https://www.kommersant.ru/doc/3481202
6. Отчет Сбербанка “Банковские тренды - 2018” [Текст]
7. ARIC White Label [Электронный ресурс] / – Режим доступа: https://www.featurespace.com/
8. FICO Application Fraud Manager [Электронный ресурс] / – Режим доступа: https://www.fico.com/
9. FraudWall [Электронный ресурс] / – Режим доступа: http://www.fraudwall.ru/
10. FRAUD-Анализ [Электронный ресурс] / – Режим доступа: http://www.bssys.com/
11. IBM Safer Payments [Электронный ресурс] / – Режим доступа: https://www.ibm.com/ru-ru
12. Intellinx [Электронный ресурс] / – Режим доступа: https://www.iitdgroup.ru/
13. Jet Detective [Электронный ресурс] / – Режим доступа: https://jet.su/services/software-development/products/jetdetective/
14. Nice Actimize [Электронный ресурс] / – Режим доступа: https://www.niceactimize.com/
15. SAS Fraud Management [Электронный ресурс] / – Режим доступа: https://www.sas.com/ru_ru/home.html/
16. БИФИТ [Электронный ресурс] / – Режим доступа: https://bifit.com/ru/
17. Digital Banking Fraud Detection [Электронный ресурс] / – Режим доступа: https://guardianananalytics.com/
18. F5 WebSafe [Электронный ресурс] / – Режим доступа: https://www.f5.com/
19. IBM Trusteer Rapport [Электронный ресурс] / – Режим доступа: https://www.ibm.com/ru-ru
20. Kaspersky Fraud Prevention [Электронный ресурс] / – Режим доступа: https://kfp.kaspersky.com/ru/
21. ThreatMetrix [Электронный ресурс] / – Режим доступа: https://www.threatmetrix.com/
22. Group-IB Secure Bank [Электронный ресурс] / – Режим доступа: https://www.group-ib.ru/fraud-hunting-platform.html
23. WEB ANTIFRAUD [Электронный ресурс] / – Режим доступа: https://www.antifraud2.ru/antifraud
24. FPS.Bio [Электронный ресурс] / – Режим доступа: https://visionlabs.ai/ru/index.html
25. SmartTracker.FRAUD [Электронный ресурс] / – Режим доступа: https://www.speechpro.ru/
26. RSA Transaction Monitoring and Adaptive Authentication [Электронный ресурс] / – Режим доступа: https://www.rsa.com/
27. BI.ZONE Cloud Fraud Prevention [Электронный ресурс] / – Режим доступа: https://bi.zone/products/bcfp/

УДК 004.056

Э. Р. ХАЙРУЛЛИН
bdevelop@ya.ru
Науч. руководитель – канд. техн. наук, доц. А. М. ВУЛЬФИН

Уфимский государственный авиационный технический университет

ТЕНДЕНЦИИ РАЗВИТИЯ МЕТОДОВ ЗАЩИТЫ В ПРОТОКОЛАХ ПРОМЫШЛЕННОМ ИНТЕРНЕТЕ ВЕЩЕЙ

***Аннотация*.** Рассмотрены основные современные протоколы в промышленном интернете вещей, а также используемые в них методы защиты от сетевых атак.
***Ключевые слова*:** кибербезопасность; промышленный интернет вещей; промышленные сети

Как и любая другая сеть, промышленная имеет ряд сходств и отличий в структуре, методах, принципах и средствах защиты с сетями общего назначения.

К сходствам промышленной сети с обычными компьютерными сетями можно отнести топологию, например, в промышленной сети имеется аналог построения сети вида «звезда», с одним централь-ным и многими дочерними устройствами – головное устройство с PLC/SCADA-системой и подключенные напрямую к нему датчики и исполни-тельные механизмы, управляемые PLC/SCADA-системой, установленной на центральном устройстве.

Кроме того к сходствам можно отнести и используемые среды передачи данных: медные и оптоволоконные кабели, беспроводную связь, – а также классификацию таких сетей по масштабу: LAN, WAN, в соответствии с классификацией сетей общего назначения.

Основные же отличия промышленных сетей от корпоративных заключается в том, что промышленные сети обладают [7]:

– специальным конструктивным исполнением кабельной инфраструктуры, коммутационного и оконечного оборудования, обеспечивающим дополнительную защиту от пыли, влаги, вибрации, ударов, ПЭМИ(н) и перепадов температуры;

– дополнительным резервированием для повышения надежности пе-

редачи данных;

– возможностью работы с малой или незначительной задержкой;

– возможностью самовосстановления после сбоев и др.

Промышленные сети могут взаимодействовать с компьютерными сетям общего назначение, в частности использовать информационно-телекоммуникационную сеть Интернет.

Существуют реализации промышленных протоколов, работающие на базе Ethernet. Данные протоколы позволяют обеспечить ряд специфических функций: дополнительные методы автоматической корректировки, диагностические функции и функции синхронизации, а также новые алгоритмы сетевого взаимодействия.

Для подключения устройств с помощью таких протоколов может быть использовано уже имеющиеся оборудование корпоративной сети, что намного упрощает внедрение и обслуживание системы промышленной автоматизации.

Соединение в промышленной сети между ее узлами выполняется с помощью физических интерфейсов. Промышленные интерфейсы обычно обеспечивают гальваническую развязку между соединяемыми узлами [18]. Наиболее распространенными в промышленной автоматизации интерфейсы RS-485, RS-232, RS-422, Ethernet и протоколы на его основе (POWERLINK, EtherCAT), PROFIBUS, Modbus, CAN, HART и AS-интерфейс.

Основные компоненты промышленных сетей:

- датчики, получающие информацию с места;
- исполнительные механизмы: электромагнитные, гидравлические…;
- программируемые логические контроллеры;
- человеко-машинные интерфейсы;
- головные устройства: ПК операторов и другие ЭВМ.

Современные промышленные сети, как и промышленность в целом, также претерпели множество изменений. Одним из таких изменения стало внедрение технологий «интернета вещей» для отраслевого применения.

В рамках технологии промышленного интернета вещей происходят следующие действия: в самом начале на ключевые части оборудования в промышленной сети устанавливаются датчики, исполнительные механизмы, котроллеры и человеко-машинные интерфейса, после чего осуществляется сбор информации, которая в последствии позволяет проанализировать состояние предприятия.

Обмен данными между компонентами сети промышленного интернета вещей обеспечивается в пределах построенной промышленной сети, ее нового сегмента или вновь созданной сети.

Информация с IIoT-датчиков накапливается и передается на вышележащие уровни управления, что помогает наладить взаимодействие между сотрудниками разных подразделений и принимать своевременные решения – предотвращения внеплановых простоев оборудования, сокращения времени технического обслуживания и числа сбоев. Таким образом, промышленный интернет вещей позволяет организациям работать эффективнее за счет оперативного сбора и обработки накапливаемых данных нижнего уровня.

Как информация от самих полевых датчиков, так и данные от IIoT-датчиков требуют защиты в соответствии с действующими нормативными актами.

Информационная безопасность, в общем случае, направлена на достижение трех свойств – конфиденциальности, целостности и доступности. План информационно-технической безопасности для информационных систем общего назначения может ставить приоритетнее задачи обеспечения конфиденциальности и мер по управлению доступом, необходимых для ее достижения. Затем может быть целостность и последней – доступность [5], как это показа-но на рисунке 2.

В рамках сетей и систем промышленной автоматики и контроля приоритет между фундаментальными свойствами зачастую отличается. Безопасность в таких системах затрагивает в основном поддержание работоспособности всех

компонентов системы, которое в том числе предполагает непрерывность некоторого процесса. Таким образом, приоритеты меняются, и конфиденциальность становится менее важной.

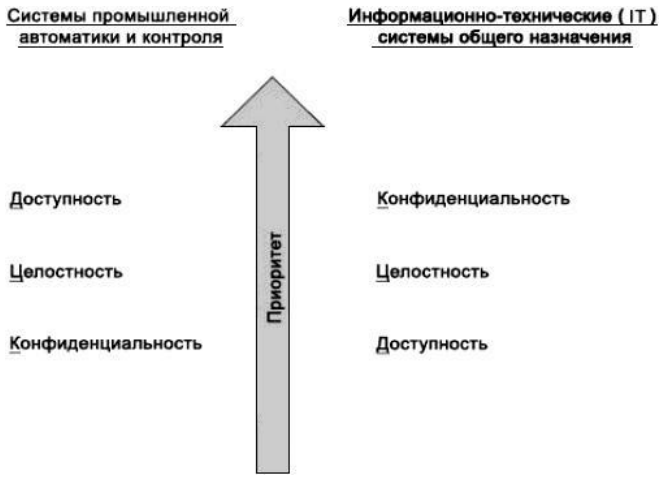


Рис. 1. Сравнение приоритетов целей промышленных систем и ИС общего назначения

В соответствии с федеральным законом от 26 июля 2017 года №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» были определены категории и критерии, по которым необходимо провести категорирование объектов критической информационной инфраструктуры организации, к которым можно отнести промышленную сеть.

Для таких организаций в соответствии с требованиями, установленными приказом ФСТЭК №239 от 25 декабря 2017 года, определено, что любая информация, передаваемая по информационно-телекоммуникационной сети, подлежит защите от угроз безопасности информации.

К мерам по обеспечению безопасности, которые необходимо обеспечить при реализации промышленной сети по выше упомянутому приказу, можно отнести ряд мер из групп:

- Идентификация и аутентификация;
- Аудит безопасности;
- Защита технических средств и систем;

– Защита информационной (автоматизированной) системы и ее компонентов;

– Управление конфигурацией и др.

В случае если промышленная сеть не соответствует ни одному критерию значимости как объекту КИИ, то ей не присваивается ни одна из таких категорий и организация вправе категорировать информацию, передаваемую в промышленной сети, как коммерческую тайну.

В настоящий момент для начала работы с технологиями промышленного интернета вещей организациям и их разработчикам приходится сталкиваться со следующими проблемами:

– выбор протокола или стека протоколов, с помощью которых будет происходить обмен между устройствами в сети;

– соответствие законодательству Российской Федерации в случае, если промышленная сеть определена как значимый объект КИИ;

Как отмечалось ранее, промышленный интернет вещей можно построить как отдельную сеть от промышленной, так и как новую независимую сеть со своим стеком протоколов, поэтому обозревая протоколы, следует выделить также две группы: протоколы, используемые в IoT, и протоколы межмашинного взаимодействия, используемые в промышленных сетях. Рассмотрим каждую группу по отдельности.

СПИСОК ЛИТЕРАТУРЫ

1. А. Е. Жуков, “Легковесная криптография. Часть 1,” – Вопросы кибербезопаснить, №1, 2015, pp. 26–43.
2. В. И. Васильев, А. М. Вульфин, В. В. Берхольц, А. Д. Кириллова и С. М. Бельский, “Анализ рисков для обеспечения целостности телеметрической информации с использованием технологии когнитивного моделирования,” – Вестник УГАТУ, том 23, № 4(86), 2019, С. 122–131.
3. А. С. Галеев, Р. И. Арсланов, П. П. Ермилов и И. А.Кузьмин, «Контроль технического состояния ШСНУ в условиях периодической эксплуатации» – Сетевое издание «Нефтегазовое дело», №. 1, 2012, С. 24–29.
4. Г. В. Миловзоров, М. И. Хакимьянов, Т. А. Редькина, А. Г. Миловзоров, «Системы управления для интеллектуальных скважин, эксплуатируемых глубиннонасосным способом» – Интеллектуальные системы в производстве, № 1, 2015, С. 55–58.

5. Некоторые подходы к криптографической защите IoT и M2M коммуникаций [Электронные ресурс] Режим доступа: https://www.ruscrypto.ru/accociation/archive/rc2018.html
6. В. И. Васильев, А. М. Вульфин, М. Б. Гузаиров и А. Д. Кириллова, «Интервальная оценка информационных рисков с использованием нечетких серых когнитивных карт» / Информационные технологии, №10, том. 24, 2018, С. 657–664.
7. В. И. Васильев, А. М. Вульфин, И. Б. Герасимова and В. М. Картак «Анализ риска кибербезопасности с использованием нечетких когнитивных карт» / Вопросы кибербезопасности № 2(36), 2020, С.11–21.
8. Д. В. Чернов, А. А. Сычугов, «Формализация модели нарушителя информационной безопасности автоматизированной системы управления технологическими процессами» / Известия ТулГУ. Технические науки, № 10, 2018, С. 22–27.
9. Я. А. Сухин, Д. И. Правиков, А. А. Кузичкин «Разработка безопасных архитектур для систем управления технологическими процессами» – Безопасность ИТ, том 27, № 2, 2020, С. 97–117.
10. Промышленные компании: векторы атак [Электронный ресурс] Режим доступа: https://www.ptsecurity.com/ru-ru/research/analytics/ics-attacks-2018/
11. Актуальные угрозы кибербезопасности: результаты за 2019 [Электронный ресурс]Режим доступа: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape- 2019/
12. A. Goel, «Cybersecurity in O&G Industry» – Proceedings of the Offshore Technology Conference, Houston, TX, USA, 2017, С. 6–9.
13. E. Nugent and M. R. August, «SCADA cybersecurity in the age of the Internet of Things: supervisory control and data acquisition (SCADA) systems' traditional role is changing as the Industrial Internet of Things (IIoT) continues to take a larger role. SCADA systems need to adjust» in Control Engineering, том 63, №9, 2017, С. 36.
14. N. M. Lakhoua, "Review on scada cybersecurity for critical infrastructures" – Journal of Computer Science and Control Systems, том 10, №1, 2017, С. 15.
15. A. Lamba "Protecting 'Cybersecurity & Resiliency'of Nation's Critical Infrastructure– Energy, Oil & Gas," in International Journal of Current Research, том 10, 2018, С. 76865–76876.
16. I. A. Grachkov, "Information security of industrial control systems: possible attack vectors and protection methods," in IT Security, том 25, № 1, 2018, С. 90–98..
17. D. K. Shadkova, A. N. Korkishko, "Cost engineering as the project management framework of arrangement of the field on the example of the public joint-stock company "Gazprom Neft," in Fundamental Research, том 4, №12, 2016, С. 930–934.
18. C. W. Ten, C. C. Liu, G. Manimaran, "Vulnerability assessment of cybersecurity for SCADA systems" – IEEE Transactions on Power Systems, том. 4, С. 4, 2008, С. 1836–1846.
19. A. Creery and E. J. Byres, "Industrial cybersecurity for power system and SCADA networks" – Record of Conference Papers Industry Applications Society 52nd annual petroleumand chemical industry conference. IEEE, 2005, С. 303–309.

УДК 004.056

Р. Р. ХАКИМОВ
s.flek.xcmo.rwae@mail.ru
Науч. руководов. – доц. Т. А. ИВАНОВА

Уфимский государственный авиационный технический университет

ЭФФЕКТИВНОСТЬ АВТОМАТИЗИРОВАННОГО ПУБЛИЧНОГО ТЕСТА ТЬЮРИНГА В ВИДЕ РЕЧЕВОГО СИГНАЛА, ИСПОЛЬЗУЮЩЕГОСЯ В ВЕБ-СЕРВИСАХ

Аннотация. В данной статье анализируются уязвимости автоматизированного публичного теста Тьюринга, представленного в виде речевого сигнала, и оценивается его эффективность.
Ключевые слова: информационная безопасность; распознавание речи; CAPTCHA; эффективность аудио-капчи; защита данных.

Введение

Ка́пча (от CAPTCHA — англ. Completely Automated Public Turing test to tell Computers and Humans Apart — полностью автоматизированный публичный тест Тьюринга для различения компьютеров и людей) — компьютерный тест, используемый для того, чтобы определить, кем является пользователь системы: человеком или компьютером.Данный тест используется для предотвращения автоматического заполнения веб-форм авторизации пользователя, от таких программ как брутфорс[1]. Современная капча в большинстве своем представлена в виде изображений, среди которых необходимо выбрать правильную картинку. По общепринятым нормам доступности интернета для людей с ограниченными возможностями такая капча должна дополняться вариантом, основанным на распознавании речи (аудио-капча). Типичные звуковые капчи состоят из разных произносящихся слов или цифр через случайно расположенные интервалы с переменной частотой или скоростью, часто с акцентом и искажением / шумом. Чтобы решить капчу, пользователь должен правильно определить цифры или слова, произнесенные в аудиофайле. Наиболее крупными кампаниями, использующие и предоставляющие аудио-капчу являются Google и Yandex.

Анализ эффективности аудио-капчи

Для демонстрации уязвимостей аудио-капчи рассмотрим алгоритм ее распознавания, который может быть применен в программах автоматического

заполнения веб-форм, на примере сервиса Яндекс.Почта. Данный сервис для "защиты от робота" предлагает прослушать звуковой файл, имеющий искажения, предназначенные для защиты от автоматического распознавания речи, и распознать четыре цифры. Анализируя полученные и отправленные запросы, возможно получить доступ к звуковому файлу для дальнейшей обработки.

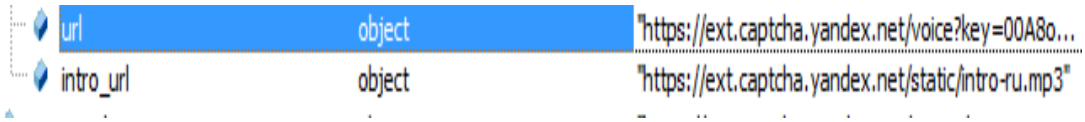


Рис. 1. Вид адреса, содержащей в себе звуковой речевой файл

На рис.2 представлен амплитудно-частотный график полученного звукового файла, содержащий в себе речевые сигналы с закодированными цифрами 6, 8, 4,3.

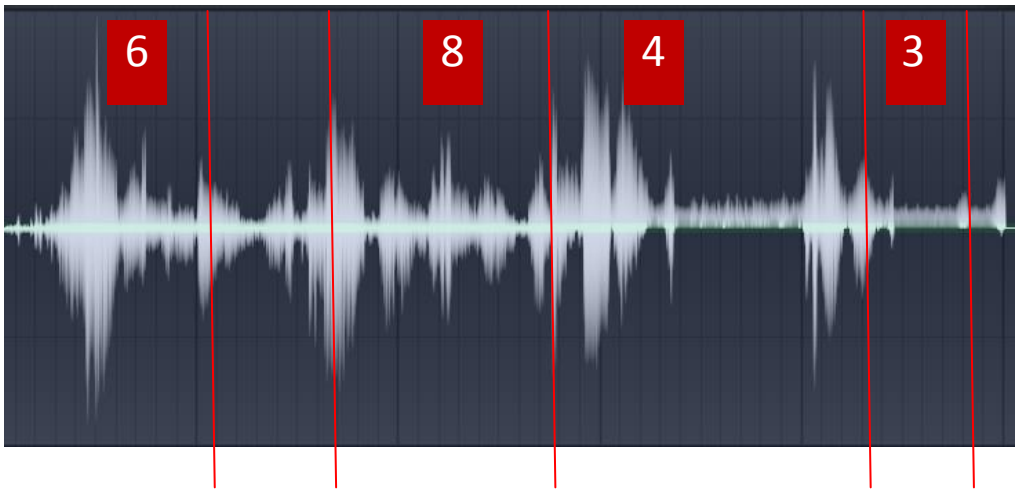


Рис. 2. Амлитудно-частотный график аудио-капчи

Формат аудиокоманды, представленный в виде графика на рис.2. представляет из себя серию чисел различной длины, произнесенных на разных скоростях, акцентах и через фоновый шум. Чтобы распознать эту капчу, звуки идентифицируются и автоматически разбиваются по частям. При этом в каждой аудио-капче звуковые искажения располагаются на одних и тех же частотах. С помощью быстрого преобразования Фурье[2] возможно определить амплитудные и частотные спектры звуковых искажений. Определив эти параметры, звуковые искажения можно подавить. После их подавления и нормализации ам-

плитуды речевого сигнала, амплитудно-частотный график аудио-капчи принимает вид, представленный на рис.3.

Рис. 3. Амлитудно-частотный график аудио-капчи после обработки

В таком виде содержимое речевого сигнала может быть распознан автоматизированными системами по распознаванию речи. Для оценки эффективности капчи в виде звукого речевого сигнала было исследовано 15 аудио-капчи на возможность их распознавания. Распознавание речи происходило с помощью различных систем, находящейся в свободном доступе. Результаты представлены в таблице 1.

Таблица 1

Эффективность аудио-капчи

№ звуковой капчи	Зашифрованная речь	Распознанная речь, %
1	Шесть восемь четыре три	100
2	Шесть четыре один два	75
3	Один один один один	100
4	Пять девять один восемь	100
5	Два четыре три восемь	75
6	Семь три семь четыре	50
7	Пять шесть два два	75
8	Пять семь один семь	75
9	Пять девять один семь	75
11	Три девять два девять	50
12	Пять шесть один два	60
13	Семь семь три шесть	100
14	Четыре девять один шесть	75
15	Пять два шесть шесть	100

По результатам, представленным в таблице 1, можно сделать следующий вывод: после предобработки аудио-капчи возможно полностью распознать речь, содержащейся в ней, что говорит о малой эффективности данного метода защиты.

В пользу данного утверждения говорит наличие автоматизированной системы " UnCaptcha ", которая может решить звуковую reCaptcha от кампании Google с 85,15% точностью. Поскольку аудио-капча достаточно для прохождения всей системы reCaptcha, эта работа представляет собой почти полное поражение системы reCaptcha, делая сотни тысяч сайтов, которые полагаются на нее, уязвимыми для злоупотреблений или автоматических атак[3].

Алгоритм работы автоматизированной системы по распознаванию аудио-капчи можно представить в виде схемы, изображенной на рис.4.

Рис. 4. Алгоритм работы автоматизированной системы распознаванию аудио-капчи

Вывод

В ходе анализа автоматизированного публичного теста тьюринга в виде речевого сигнала, использующегося в веб-сервисах были найдены следующие уязвимости:

1. Возможность доступа к звуковому файлу, представляющей из себя аудио-капчу, с помощью отслеживания поступающих, отправленных запросов при авторизации пользователя.

2. Возможность распознавания аудио-капчи с помощью обработки речевого сигнала и автоматизированных систем по распознаванию речи.

Ранее предполагалось, что добавление семантического шума позволит решить проблему распознавания звуковой капчи, но по мере развития автоматизированных систем для распознавания речи данная проблема не потеряла свою актуальность.

Таким образом, аудио-капча как вид защиты от автоматического заполнения веб-форм на данный момент времени показывает малую эффективность от автоматизированных систем по заполнению веб-форм.

СПИСОК ЛИТЕРАТУРЫ

1. М.И.Николаевич АВТОМАТИЧЕСКИЙ ТЕСТ ТЬЮРИНГА «CAPTCHA« // Наука, техника и образование — 2019.—№11. — С.64.
2. М.А. Кройц, О.А. Морозов МЕТОДЫ ФИЛЬТРАЦИИ И ЛИНЕЙНОГО ПРЕДСКАЗАНИЯ В ЦИФРОВОЙ ОБРАБОТКЕ СИГНАЛОВ – Нижний Новгород: Нижегородский госуниверситет, 2020. – 26 с.
3. Е.М. Сергеевич НЕДОСТАТКИ И УЯЗВИМОСТИ RECAPTCHAV2 // Наука и иновации в XXI веке — 2020—С.54

УДК 004.056

В. Э. ХАЛИУЛИН
vadimh96@mail.ru
Науч. руководов. – канд. техн. наук, доцент Т. А. ИВАНОВА

Уфимский государственный авиационный технический университет

ПРОБЛЕМЫ ЗАЩИЩЕННОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Аннотация. В данной работе рассматриваются проблемы защиты персональных данных субъектов Российской Федерации у операторов. Проведен анализ предложения и спроса определенных услуг, связанных с персональными данными на теневых информационных ресурсах. Рассматриваются возможные пути ее уменьшения.
***Ключевые слова*:** персональные данные; теневые информационные ресурсы.

Персональные данные - это любая информация о человеке, которая связана с ним, дает возможность идентифицировать его, получить какие-либо сведения о нем, совершать какие-либо посягательства на тайну его личной жизни и на имущество. В группе риска утраты важной информации при проведении обработки персональных данных оказываются многие люди, среди них:

- граждане, пользующиеся банковскими картами;
- граждане, получающие медицинские услуги;
- владельцы пенсионных накоплений;
- вкладчики банков;
- владельцы недвижимости.

Чем больше цифровизация общества – тем больше подвергаются риску персональные данные. Так же увеличивается количество тех, кто ими оперирует. Финансы, медицина, государственные услуги все больше становятся цифровыми и пропорционально этому росту, увеличиваются инциденты связанные с утечкой персональных данных.

В России за последние 5 лет динамика таких происшествий выше, чем была раньше. Думаю, это связано с повышенным вниманием СМИ и общества к этой теме. Важность защиты информации становится все более очевидной для различного рода организаций, а не только для банков и спецслужб.

Последствия утечек могут оказаться серьезными и для владельцев данных, и для операторов. Для первой группы существуют многочисленные риски стать жертвой злоумышленников. Они могут пострадать:

- от разглашения любой информации, имеющей отношение к личности;
- от шантажа;
- от неправомерного списания средств с банковской карты;
- от вмешательства в личную жизнь;
- от угроз детям, например, в случае публикации в СМИ данных о школах, где они учатся.

Минимальным риском станет неправомерная передача сведений, например, адреса электронной почты, каким-либо компаниям, которые начнут преследовать их обладателя рекламными объявлениями. Но даже это дает возможность возбудить дело и о неправомерной рекламе, и об утечке данных и приведет к штрафам, налагаемым на операторов, если источник утечки или спама удастся достоверно установить.

Операторы, в свою очередь, допустившие утечку персональных данных, понесут ответственность:

- гражданскую, в виде взыскания в судебном порядке понесенных гражданами убытков и морального вреда;
- административную, в виде наложения штрафа, приостановления или запрета деятельности, связанной с обработкой персональных данных;
- уголовную, в случае неправомерного распространения ПДн, причинившего существенный ущерб и передаче информации в правоохранительные органы.

Пока серьезность исков о возмещении морального вреда, связанного с утечкой конфиденциальной информации, компаниями серьезно не рассматривается. Даже если судом установлен такой факт, размер присужденных сумм редко превышает несколько десятков тысяч рублей даже в столице. В регионе

суд скорее откажет в удовлетворении требований, предъявляемых как к банкам, так и к интернет-магазинам. Более серьезными становятся ситуации, когда в спор вмешиваются регуляторы и доводят ситуацию до возбуждения уголовного дела.

Зачастую бизнес-компании пренебрегают защитой персональных данных и вовсе не уведомляют Роскомнадзор об оперировании персональными данными. Причиной тому может служить не осведомленность, динамическое изменение законодательства, требования, которые ведут к дополнительным вложениям, проверки и как итог, компаниям проще заплатить относительно маленький штраф, чем организовывать защиту.

Львиная доля случаев утечек в России приходится из-за внутренних нарушений, так называемый инсайдерский тип, около 80% случаев, по зарегистрированным данным. Это означает, что большая часть таких происшествий в нашей стране идет через внутренних сотрудников. Чаще всего, злоумышленник вступает в сговор с внутренним сотрудником, который и передает ему данные.

На теневых интернет-ресурсах можно найти кучу предложений получения полного досье о почти любом интересующем субъекте, вплоть до текущего местоположения. И стоимость этих услуг доступна почти любому действительно интересующемуся лицу. Так, к примеру, стоимость данных из паспорта в среднем по форумам (фото, родственные связи, прописка, браки) – 1200 рулей; железнодорожные, авиа-передвижения – от 1500 (в зависимости от срока); Система "Поток" ГИБДД(адреса передвижения по камерам) – от 5000; местонахождение абонента (операторы связи) – от 3000; по номеру сотового телефона(Данные при регистрации – ФИО, дата рождения, прописка) – 800 рублей. Вся информация предоставляется в короткие сроки. Продавцы такой информации имеют репутацию, отзывы и многие сделки проводятся через «гаранты», поэтому усомниться в реальности их «продукта» затруднительно. Так же множество «вакансий» на подобного рода сайтах, где постоянно требуются новые лица, имеющие отношения и доступ к базам всех государственных органов,

банков, сотовых операторов и попробовать себя в этом деле может каждый желающий.

По сути, информация о продаже в открытом доступе и продается комплексно по многим службам, банкам и организациям, и вероятнее всего, преступники действуют группой. И, на мой взгляд, занимаются поиском таких преступников не охотно, так как преступление не является тяжким, тратить ресурсы на поиск и распутывание цепочки не эффективно. А преступникам достаточно простых схем, знаний и доступного программного обеспечения для анонимности, чтобы обезопасить в свою очередь от «пробива» себя соответствующими службами.

Каким образом можно защититься?

От непреднамеренных утечек организации хорошо защищают DLP-системы (Data Leakage Prevention — с англ. "предотвращение утечки данных"). Например, от действий человека, который, не задумываясь, отправляет куда-то конфиденциальные документы или печатает их на общем принтере. Система перехватывает такие документы и просто не дает их отправить или напечатать. Злоумышленник, прежде чем совершить кражу данных, внимательно изучает систему защиты. И в итоге хорошо понимает не только то, как она работает, но и как ее обойти. Например, использует канал, который многим даже в голову бы не пришел, — копирует чувствительную информацию и оставляет ее в буфере обмена на рабочем ноутбуке, а дома вытаскивает. Борьба с преднамеренными утечками так сложна еще и потому, что конфиденциальную информацию в основном воруют люди, легально имеющие к ней доступ. Те, кто может на законных основаниях посмотреть, как устроена система, взять информацию и унести ее домой. Поэтому "безопасникам", планирующим в очередной раз улучшать свои DLP-решения, нужно обратить особое внимание именно на эту категорию сотрудников. Говоря о том, как нужно бороться с утечками, нужно, во-первых, сказать, что современным организациям все же не нужно пренебрегать традиционными инструментами, обеспечивающими безопасность. Без ан-

тивируса можно точно подвергнуться заражению. А без системы защиты от утечек — гарантированно потерять конфиденциальную информацию, причем не раз. Поэтому несмотря на то, что ни антивирус, ни DLP не дают 100-процентной гарантии, совсем без них обойтись нельзя.

Операторы могут столкнуться с проблемами при внедрении DLP, так как они должны четко рассчитать оценку рисков, масштаб планируемого внедрения; нормативные требования, которые могут повлиять на них; подготовить планы, политики, руководства к DLP; организовать управление программой DLP;

Во-вторых, организациям нужно обучать сотрудников элементарной цифровой гигиене.

В-третьих, важно правильно проводить организационные мероприятия по недопущению утечек. В число этих мероприятий входит: ограничение доступа посторонних лиц в помещение, подписание сотрудниками соответствующих письменных обязательств, разграничение доступа к информации и так далее. Это целый комплекс действий, без которого никакая автоматическая система не будет эффективной.

Если еще как-то возможно контролировать наиболее популярные каналы утечки информации как сеть, съемные носители, принтеры. Но от внутренних сотрудников сделать это затруднительно – можно просто сделать фото экрана. На такой случай необходимо внедрять (совершенствовать) системы контроля и управления доступом, системы видеонаблюдения, ограничить количество лиц, имеющим доступ к таким данным; назначать ответственных лиц, мониторящих их деятельность и внедрить все это на законодательном уровне.

На мой взгляд, ужесточение наказания за нарушения законов в этой области оказали бы положительный эффект. Рост утечек и растущие угрозы, которую они таят в эпоху цифровизации, недооценены нашими законодательными органами, по моему субъективному мнению.

В наших реалиях абсолютно универсального подхода быть не может, в каждой организации должен быть свой оптимальный набор средств защиты, созданный на основе ее специфики.

СПИСОК ЛИТЕРАТУРЫ

1.А.И. Савельев, Научно-практический постатейный комментарий к Федеральному закону «О персональных данных», 2017 г. - 470 стр. Книга для изучения вопроса с юридической стороны.
2. Михаил Брауде-Золотарев, Виталий Негородов, Евгения Сербина, Иван Волошкин, Персональные данные в государственных информационных ресурсах, 2016 г. - 60 стр
3. Федеральный закон "О персональных данных": научно-практический комментарий. Под редакцией А.А. Приезжевой, 2015 г. – 177 стр. От коллектива Роскомнадзора.

УДК 004.85

Е. В. ХОМУТОВ
KapitanMGN@yandex.ru
Науч. руководитель – канд. техн. наук, доц. Т. А. ИВАНОВА

Уфимский государственный авиационный технический университет

СИСТЕМА ОБНАРУЖЕНИЯ СЕТЕВЫХ АТАК В ПРОМЫШЛЕННЫХ СЕТЯХ

Аннотация. В данной статье рассматривается возможность обеспечение безопасности промышленных сетей различных АСУ ТП с помощью методов машинного обучения, проводится анализ «типичных» сетевых атак и способов их обнаружения, а также описываются основные методы обнаружения сетевых атак. Помимо этого, приводится функциональная схема мониторинга промышленной сети АСУ ТП, а также один из возможных вариантов реализации сетевой защиты с помощью вышеописанных алгоритмов.
Ключевые слова: программное обеспечение; машинное обучение; кибербезопасность SCADA систем; сетевой трафик; промышленные сети.

Указом президента Российской Федерации от 7 мая 2018 года № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года» цифровая трансформация энергетической инфраструктуры является приоритетным направлением развития российской экономики [1]. Это возможно благодаря развитию области промышленного интернета вещей (Industrial Internet of Things – IIoT). Основная концепция промышленного Интернета вещей (IIoT) заключается в использовании преимуществ технологии Интернета вещей (IoT) в системе управления производством (ICS), она же АСУ ТП. АСУ ТП являются неотъемлемой частью критических инфраструктур и долгое время использовались для контроля промышленных машин и процессов. Они выполняют мониторинг и взаимодействие с устройствами в реальном времени, сбор и анализ данных в реальном времени, а также регистрацию всех событий, происходящих в промышленных системах. Использование технологии IoT в этих системах улучшает сетевой интеллект и безопасность при оптимизации и автоматизации производственных процессов.

Система диспетчерского управления и сбора данных (SCADA) является самым большим подмножеством ICS. Она предоставляет графический интер-

фейс пользователя (GUI) через человеко-машинный интерфейс (HMI). HMI упрощает операторам наблюдение за состоянием системы, взаимодействие с устройствами IIoT и получение сигналов тревоги, указывающих на ненормальное поведение. Развитие индустрии 4.0 ускорило процесс интеграции исполнительных устройств и систем управления. IIoT становится неотъемлемой частью цикла производства в промышленности.

АСУ ТП – это в основном критически важные системы с высокими требованиями к доступности. Их непрерывная работа приводит к созданию огромного количества данных. В прошлом эти системы были автономными и изолированными от мира, что делало их невосприимчивыми к внешним злонамеренным атакам. В последнее время возросшее количество соединений АСУ ТП с корпоративными сетями и использование Интернет-коммуникаций для более удобной передачи информации сделало эти системы уязвимыми для злонамеренных атак.

Из-за чувствительности многих промышленных приложений безопасность стала главной задачей в системах SCADA. В частности, отсутствие соображений безопасности в их протоколах связи напрямую ставит под угрозу доступность, безопасность и надежность этих систем. Одним из ключевых направлений обеспечений энергетической безопасности является повышение состояния защищенности таких объектов как: критические информационные инфраструктуры (КИИ), топливно-энергетические комплексы (ТЭК) и др. Эти объекты являются наиболее вероятными целями для проведения спланированных компьютерных атак, так как энергетика обеспечивает функционирование социально значимых объектов. При осуществлении кибератак на ТЭК могут возникнуть риски нарушения нормальной работы других отраслей экономики.

Целями злоумышленников могут быть как промышленный шпионаж и финансовая выгода, так и попытки саботировать производственный и другие процессы. Системы являются достаточно уязвимыми перед атаками из-за использующихся в них протоколов передачи данных. Такие протоколы как Mod-

bus, Building Automation and Control Network (BACnet), Distributed Network Protocol версии 3 (DNP3) и Message Queuing Telemetry Transport (MQTT) разрабатывались без учета киберрисков или механизмов безопасности для противодействия им.

Рост количества уязвимостей, найденных в оборудовании автоматизированных систем управления технологическими процессами (АСУ ТП) способствует этому. По данным отчета Claroty в 2020 году их число выросло почти на 25% по сравнению с 2019 годом. Обнаруженные уязвимости, в основном, затрагивают сектора промышленного производства, энергетики и водоснабжения. В первом полугодии 2020 года, по сравнению с 2019 годом, число уязвимостей в сфере промышленности выросло на 87,3%, в секторе водоснабжения – на 122%, в энергетическом секторе – на 58,9%.

С начала 2020 года количество атак на промышленные и энергетические предприятия в России держится на высоком уровне. По данным аналитических отчетов Positive Technologies промышленность уже на протяжении двух лет входит в тройку наиболее часто атакуемых отраслей. Количество атак на промышленность увеличилось почти в 2 раза по сравнению с 2019 годом: прирост составил 91%.

В IV квартале 2020 года треть всех инцидентов в промышленной отрасти были совершены с помощью хакинга, в 84% атак применялось вредоносное ПО

Таким образом, охрана периметра и точек входа в промышленные системы становится критически важной задачей. Для промышленного оборудования и пограничных систем, точек входа в промышленную сеть необходимо обеспечить глубокий анализ трафика на наличие попыток сетевых атак и аномалий с поддержкой анализа промышленных протоколов. Совершенствование средств защиты сетевой инфраструктуры направлено на развитие инструментов интеллектуального мониторинга сетевого трафика и состояния объектов и узлов промышленной сети.

Учитывая вышесказанное, можно сделать вывод об актуальности темы и необходимости совершенствования систем обнаружения сетевых атак на основе применения методов искусственного интеллекта, как ключевого элемента обеспечения кибербезопасности SCADA систем в концепции развития цифровой экономики.

В [2] описана общепринятая классификация обнаружения атак по способам выявления атак, а именно системы обнаружения аномалий и системы обнаружений злоупотреблений. Все существующие на данный момент методы обнаружения сетевых атак используются либо в системах обнаружения аномалий, либо в системах обнаружения злоупотреблений.

Поведенческие методы обнаружения атак основываются на использовании информации о нормальном поведении системы и ее сравнении с параметрами текущего, наблюдаемого поведения [3]. По мере функционирования данные методы сравнивают текущую активность в системе с заранее установленным шаблоном «нормального» поведения и обнаружив множественные отклонения от шаблона можно охарактеризовать как атаку. Эти методы склонны к наличию ложноположительных срабатываний, в зависимости от того, насколько полно и корректно составлен шаблон нормального поведения системы. От ложноположительных срабатываний избавиться полностью практически невозможно, особенно если система обширна и многофункциональна, так как полностью и с достаточной точностью описать все действия пользователей системы практически невозможно. Кроме того, период получения такого шаблона может занимать большие промежутки времени. Из-за недостатков данных методов многие отказываются от построения систем, основанных на поведенческих методах в пользу других, которые могут предоставить более точные и надежные представления о злонамеренных атаках.

К поведенческим методам можно отнести:

- Вейвлет-анализ
- Статический анализ

- Анализ энтропии
- Спектральный анализ
- Фрактальный анализ
- Кластерный анализ

Методы на основе знаний используют правила и факты, отражающие признаки заданных атак и производят обнаружение атак по заложенным механизмам поиска [3]. Для поиска могут использоваться такие алгоритмы как сопоставление по образцу, анализ перехода состояний, аппарат регулярных выражений и т.д. Методы на основе знаний работают с некоторой базой данных или базой «знаний», которая имеет в себе описание различных, и что немаловажно, известных атак. Такой аппарат при правильном подходе к составлению базы «знаний» может эффективно справляться с большинством типов стандартных кибератак при этом не используя минимальное количество ресурсов системы, но против хорошо спланированных, последовательных или стратегически продуманных, то есть не стандартизированных попытках взлома системы безопасности методы на основе знаний показывают себя не с лучшей стороны. Такая система попросту не распознает продуманную попытку проникновения.

К методам на основе знаний можно отнести:

- Сигнатурные методы
- Языки описания сценариев
- Метод на основе конечных автоматов
- Экспертные системы
- Метод проверки моделей

Методы машинного обучения используются и в системах обнаружения аномалий, и в системах обнаружений злоупотреблений. Это объясняется тем, что для обучений данных методов пользуются шаблоны нормального и аномального поведения в сети. Один из самых распространенных подходов для обнаружения вторжений это Байесовская сеть – модель, кодирующая вероят-

ностные отношения между события и предоставляющая механизм для вычисления условных вероятностей их наступления [4]

Также имеются методы на основе MAP-сплайнов, которые позволяют построить весьма точную аппроксимацию поведения как злоумышленника, так и обычного пользователя системы.

Кластерный анализ или алгоритмы кластеризации, выполняющие сбор данных об объектах, после чего упорядочивая эти объекты в сравнительно однородные группы [5]. Он используется не только в разработках систем безопасности, но и в других научных сферах, таких как химия, биология, медицины, маркетинг и т.д. Метод случайного леса (Random forest) использует ансамбль деревьев решений, применяющийся для классификации, регрессии и кластеризации. Он заключается с использованием огромного объема ансамбля деревьев решений, в котором каждое из таких деревьев дает очень малую точность, но за счет количества выходных данных результирующие показатели получают высокую степень точности.

Методы вычислительного интеллекта представляют собой различные искусственные нейронные сети – набор нейронов, связанных между собой синапсами и посредством данных связей преобразующие наборы входных значений в обработанные выходные данные. Нейронные сети нашли себя не только в поприще алгоритмов по обнаружению аномалий или злоупотреблений, они также широко применяются в криптографии, распознавании образов, в алгоритмах сжатия данных и т.д. Искусственные нейронные сети способны обучаться по образцам, которые включают в себя различные шумы и неполноценность данных, подстраиваясь и адаптируясь в процессе обучения.

К методам вычислительного интеллекта можно отнести [6]:

- Радиально-базисные нейронные сети
- Рекуррентные нейронные сети
- Самоорганизующиеся карты или карты Кохонена
- Генетические алгоритмы

- Вычислительные иммунные системы
- Отрицательный отбор
- Клональная селекция

Атаки делятся на пять классов, в зависимости от того, какие аспекты безопасности (целостность, доступность, конфиденциальность, аутентификация и авторизация) скомпрометированы. Однако практически невозможно определить отдельную классификацию, потому что классы, в которые попадают эти атаки, не исключают друг друга. Часто компрометация одного аспекта приводит к компрометации и других.

Атаки нацеленные на целостность системы.

- Переполнение буфера
- Внедрение кода
- Неправильная проверка ввода

При атаках переполнения буфера злоумышленник пытается записать в буфер большие данные (превышающие размер буфера), в результате чего дополнительные биты переполняются и перезаписывают другие буферы и изменяют их значения. Эта атака обычно вызвана плохими механизмами проверки типа или размера ввода и делает систему ненадежной или даже аварийной. Атаки переполнения буфера широко распространены в системах SCADA по двум основным причинам. Во-первых, большинство операционных систем в АСУ ТП написано на таких языках программирования, как C, в котором отсутствуют механизмы безопасности типов. Кроме того, устройства SCADA работают непрерывно. Операционные системы, которые не перезагружались годами, более уязвимы из-за накопившейся фрагментации памяти. Проблема переполнения буфера в системах SCADA может повлиять как на систему диспетчерского управления, так и на полевые устройства, такие как датчики. Инструкции ПЛК для выходных элементов (например, включение или выключение водяных насосов) и считываемые данные (например, уровень воды) могут управляться посредством этой атаки [21].

При атаке путем внедрения кода злоумышленник пытается выполнить вредоносные команды или ввести вредоносные данные в систему. Например, при атаке с использованием SQL-инъекции запросы SQL отправляются для управления или взлома сервера базы данных. Эта атака использует уязвимость системы из-за отсутствия пользовательских методов проверки входных данных. Эта атака позволяет злоумышленнику получить доступ к конфиденциальной информации, такой как имена пользователей и пароли, а также изменить данные (например, разрешить доступ неавторизованному пользователю, удалить данные и т. Д.). Атака с введением команд может манипулировать командами управления в системе и нарушить нормальную работу. Поскольку основная функция систем SCADA - сбор и хранение информации, эта атака может иметь серьезные последствия для системы. В частности, если система управляется удаленно через веб-интерфейс, эта атака может скомпрометировать данные и процедуры аутентификации.

Эта уязвимость связана с отсутствием надлежащих механизмов для проверки ввода пользователя. Это более общий тип уязвимости, который может привести к другим типам рисков. Злоумышленник может ввести неправильные значения, которые могут сделать систему нестабильной. Более того, поскольку эти системы не проверяются регулярно из-за их детерминированного характера, эта атака может оставаться незамеченной в течение длительного времени [7].

Основная атак, которая затрагивает доступность системы является DoS-атака (Отказ в обслуживании). Злоумышленник выполняет DoS-атаку, чтобы затопить целевой компьютер (например, ПЛК и HMI). Эта атака нарушает доступность системы SCADA, отправляя большое количество случайных пакетов на целевой узел с высокой скоростью, чтобы цель не отвечала на запросы и даже могла привести к сбою всей системы. SYN-атаки – это постоянные поддельные запросы на синхронизацию, а HTTP-атаки – это либо GET, либо POST запросы, чтобы веб-сервер цели был занят и не мог отвечать на обычный трафик. Если каналы в сети перегружены, мониторинг и управление ICS будет очень

трудным, если не невозможным. Таким образом, основная цель DoS-атаки – нанести ущерб доступности системы, чтобы пользователи не могли получить доступ к ресурсам.

Основной атакой при попытке нарушить конфиденциальность системы является разведывательная атака. При разведывательной атаке злоумышленник взаимодействует с сетью SCADA для сбора информации о системе, такой как подключенные устройства, политики безопасности, IP-адреса, информация о хостах и т. Д. После идентификации элементов сети злоумышленник отображает архитектуру сети для выявления уязвимостей в системе. В конце концов, злоумышленник может использовать эту информацию для запуска эксплойтов на уязвимых устройствах чтобы нарушить работу системы. Злоумышленники могут начать эту атаку с помощью снифферов. Они подслушивают и проверяют текущий сетевой трафик, чтобы получить информацию об элементах сети и их статусе. Скрытое сканирование в сети SCADA может происходить на канале связи между любым из двух узлов сети; например, связь между сетью ввода-вывода и ПЛК или связь между компьютером HMI и ПЛК. Эта атака считается пассивной, поскольку злоумышленники молчат и не вводят трафик, который мог бы их раскрыть. Хотя эту атаку нельзя считать серьезной, сетевая информация раскрывается неуполномоченным лицам, и ее очень сложно обнаружить.

Можно выделить 2 типовые атаки, нацеленные на нарушение аутентификации: Доступ без аутентификации и человек посередине. Уязвимость доступа без аутентификации связана с плохими механизмами аутентификации в системах SCADA. Поскольку эти системы работают непрерывно и автономно, персонал не может регулярно менять свои имена пользователей и пароли. Они могут даже использовать имена пользователей и пароли по умолчанию для облегчения запоминания [8]. Для получения этой информации можно использовать методы грубой силы или регистрацию нажатий клавиш пользователем. Кроме того, широко применялись фишинговые атаки для сбора учетных данных операторов АСУ ТП [7]. Если злоумышленник каким-то образом узнает эти учет-

ные данные, он может злоупотребить своим доступом и провести другие типы атак. Поскольку под этой категорией мы рассматриваем исключительно «доступ» к данным, для которых обычно root-доступ не предоставляется. Мы классифицировали эту атаку как слабую. В противном случае они будут отнесены к более серьезным типам атак, таким как обход каталога.

При атаке «человек посередине» злоумышленник перехватывает каналы связи и пытается скомпрометировать сообщения между двумя узлами, в то время как узлы думают, что они все еще общаются друг с другом напрямую. Например, злоумышленник может посылать злонамеренные команды исполнительным механизмам, выдавая себя за ПЛК, или отправлять ложные ответы от датчиков на ПЛК. Кроме того, злоумышленник может отбрасывать сообщения или манипулировать ими. Этот тип атаки будет иметь допустимый синтаксический код; следовательно, IDS на основе правил не сможет идентифицировать его по формату сообщения [9]. Этот тип атак в основном можно предотвратить с помощью методов шифрования.

Так же имеется 2 основных типа атак, нацеленных на авторизацию в системе: Обход каталогов и черный ход. В атаке «Обход каталогов» злоумышленник пытается получить доступ к ограниченным каталогам или файлам, которые должны иметь только root-доступ. Эта уязвимость связана с плохими механизмами фильтрации или проверки вводимых пользователем данных. Еще одна причина этих атак - плохой контроль над списком каталогов. В этом типе атаки злоумышленник сможет загрузить из системы конфиденциальные файлы и информацию. Эта атака часто также приводит к компрометации других уязвимостей в системах SCADA, таких как конфиденциальность, поскольку злоумышленник может получить доступ к частным файлам в системе. Правильные методы проверки ввода могут предотвратить этот тип атаки

При атаке через бэкдор злоумышленник пытается обойти процесс аутентификации, чтобы войти в систему. Через бэкдор злоумышленник может войти в систему, получить доступ ко всем данным и файлам в системе и выполнять

команды. Установка бэкдора на систему-жертву может быть произведена инсайдером. После установки очень сложно обнаружить этот тип атаки, и он считается очень опасным, поскольку предоставляет злоумышленнику полный доступ к системе. В случае с АСУ ТП некоторые поставщики и производители имеют бэкдор-аккаунты в своих продуктах для удаленной поддержки и обновлений [10]. Эта уязвимость подвергает систему опасности, и в случае успешной атаки все данные SCADA будут доступны злоумышленнику.

IDS широко используется как эффективный механизм защиты от вторжений. IDS, основанные на неправильном использовании, такие как методы на основе правил, сигнатур, потоков и трафика, - это лишь некоторые примеры обычных IDS. Поскольку традиционно большая часть соединений и трафика в сетях SCADA была предопределена; эти типы IDS успешно выявляли аномальные действия. Например, когда злоумышленник устанавливает новые соединения с жертвой или отправляет другой тип трафика, в сети будут возникать необычные потоки данных. Однако, учитывая частые обновления в сетях, приводящие к регулярным изменениям топологии, устаревшие IDS не работают должным образом. Кроме того, для противодействия новым типам атак, которые появляются каждый день, или в сценариях, когда атака планируется грамотно (например, атака «человек посередине»), требуются интеллектуальные IDS. IDS, как правило, полезны всякий раз, когда злоумышленник влияет на сетевой поток данных. Это верно даже для IDS на основе машинного обучения. Если злоумышленник не взаимодействует ни с одним из сетевых элементов, очень сложно даже узнать о вторжении. Однако, чтобы начать атаку или нарушить работу сети, злоумышленник должен каким-то образом нарушить работу сети. Способность алгоритмов машинного обучения обнаруживать небольшие аномалии отличает их от любых других типов IDS. Алгоритмы машинного обучения могут обнаруживать паттерны аномалий, которые трудно обнаружить людям. Чтобы обеспечить безопасность сети, IDS на основе ML может быть спроектирована с движущейся целью. Эта способность моделей машинного

обучения учиться и развиваться ценна, потому что атаки постоянно развиваются, а новые уязвимости обнаруживаются каждый день. Это еще одна причина, по которой IDS на основе сигнатур становятся устаревшими, а IDS на основе аномалий с использованием машинного обучения становятся новой тенденцией. Теперь мы обсудим пригодность IDS на основе машинного обучения для каждого из элементов безопасности.

Машинное обучение может быть очень полезным в качестве средства обнаружения угроз целостности данных. Обучая IDS на основе машинного обучения с использованием допустимых данных о трафике, IDS будет изучать обычные данные, которые передаются в системе. Например, в случае внедрения команды ML обнаружит необычные вредоносные запросы в системе. Эта специализированная IDS способна распознать источник, нарушающий целостность данных, чтобы заблокировать его доступ в систему для поддержания надежности данных. Следовательно, изучая общее поведение системы, IDS на основе ML может быть очень полезной против атак, нацеленных на этот элемент безопасности.

ML может быть очень полезным при обнаружении DoS-атак. Правильный алгоритм машинного обучения может обнаруживать конкретные характеристики атак, нацеленных на доступность, например, обнаружение источников с незнакомыми или широковещательными адресами, тех, которые демонстрируют ненормальное поведение, узлов, которые отправляют необоснованный объем трафика или, когда нормальный рабочий трафик останавливается, потому что HMI или ПЛК переполнены и недоступны. Несмотря на то, что простой сетевой анализатор может обнаруживать DoS-атаки, для анализа сетевых журналов попрежнему требуется оператор-человек. С другой стороны, IDS на основе машинного обучения не только обеспечивает надлежащую автоматизацию, но также не подвержена человеческим ошибкам. Более того, было показано, что он эффективен в обнаружении такого необычного поведения.

В этом типе атаки, если злоумышленник просто перехватывает сетевой трафик (т. е. Не отправляет трафик и не устанавливает соединение с устройствами в сети), его очень сложно обнаружить с помощью ML. Как упоминалось ранее, когда поведение злоумышленника не меняет сетевой поток, очень сложно обнаружить атаку с помощью любого метода, включая ML. Однако, как только злоумышленник входит в сеть, IDS на основе аномалий, основанная на машинном обучении, сможет распознать ненормальное поведение злоумышленника, пытающегося отслеживать или запрашивать необычную информацию у других узлов в сети. Однако после взаимодействия с сетью вредоносные действия выходят за рамки простой атаки с перехватом и классифицируются по другим категориям атак.

Как упоминалось ранее, аутентификация — это метод контроля безопасности. Атаки, нацеленные на этот элемент безопасности, должны найти способ обойти этот шаг. Для противодействия этим угрозам будет эффективнее использовать методы предотвращения, а не методы обнаружения. Например, для предотвращения доступа без аутентификации можно использовать шифрование, надежные пароли или методы управления ключами. Несмотря на то, что у этих методов есть свои недостатки, они повышают устойчивость системы к несанкционированному доступу.

Действия, которые не соответствуют нормальному шаблону трафика даже от проверенных пользователей, могут быть идентифицированы с помощью методов машинного обучения. Некоторые примеры включают выполнение аномальных команд, манипулирование датчиками и исполнительными механизмами или отправку случайного трафика в сети. Если злоумышленник запускает атаки нулевого дня или время от времени обращается к системе, он может какое-то время оставаться незамеченным, но в конечном итоге будет обнаружен IDS на основе ML. Однако чувствительность методики обучения должна быть высокой. IDS изучает нормальные условия системы и выявляет оскорбительные команды, неавторизованных пользователей или злоумышленников. IDS будет

подавать сигнал тревоги каждый раз, когда обнаруживает ненормальное поведение пользователя в сети, которое должно быть проверено оператором. Повышение чувствительности используемого машинного обучения для обнаружения этих злоумышленников увеличит количество ложных срабатываний (нормальный трафик, классифицируемый как трафик атаки). Тем не менее, в вопросах безопасности лучше соблюдать осторожность, обеспечивая безопасность сети IIoT. Ложноотрицательный результат (необнаруженная атака) может привести к более высоким затратам, чем ложный положительный результат в критических инфраструктурах.

Предлагаемая схема системы мониторинга сетевого трафика промышленной сети АСУ ТП на основе алгоритмов машинного обучения представлена на рисунке 1.

Рассмотрим основные элементы предлагаемой системы. Сервер логов (1) сетевых сессий и МСЭ (2) являются источником данных для последующего дообучения ML-ядра СОВ при реализации новых сценариев атак.

Модуль предобработки и генерации признаков позволяет выделять существенные параметры сетевой сессии для последующего построения обучающей выборки модели. Для обогащения данных о сетевых сессиях и связанных с ними событиях информационной безопасности используется двухстороннее взаимодействие с SIEM / SOC. Процессом разметки (обогащения) записей сетевых сессий управляет специалист (3) по сетевой безопасности текущего сегмента. Размеченные данные позволяют создать базу примеров для обучения ML-моделей. Банк ML-моделей (5) пополняется протестированными моделями. Процесс подбора гиперпараметров моделей координируется инженером по знаниям (4). Подготовленные модели готовы к встраиванию в виде программных модулей в соответствующее сетевое оборудование (маршрутизаторы, управляемые коммутаторы и МСЭ) или к использованию в составе сетевой СОВ.

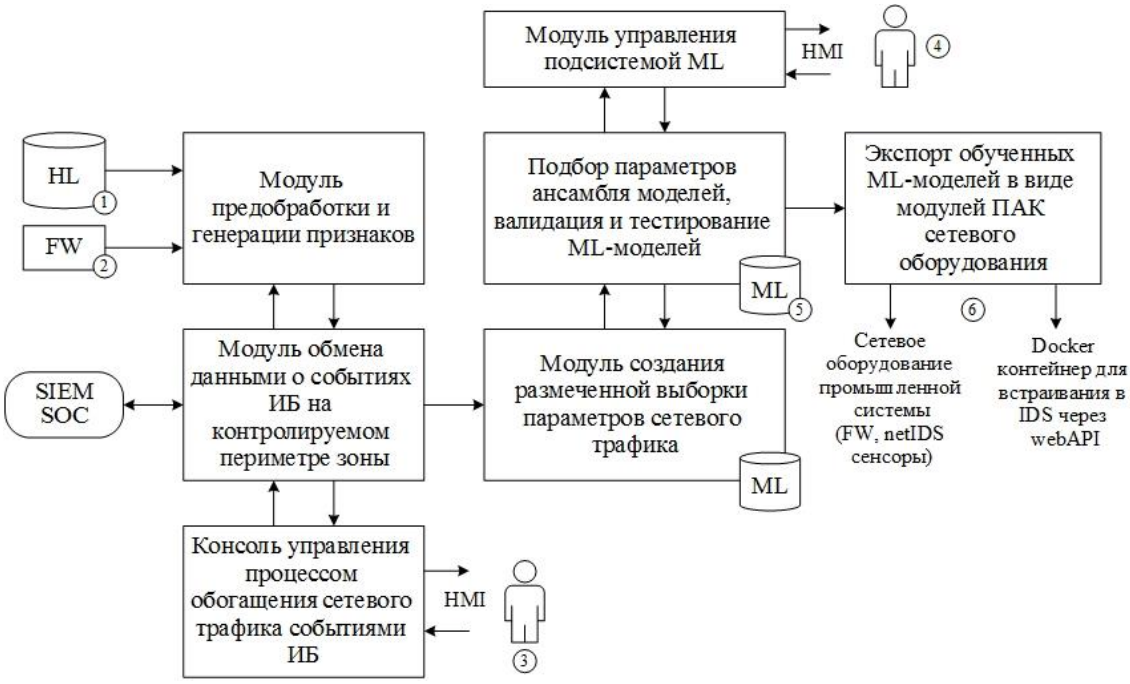


Рис. 1. Схема системы мониторинга сетевого трафика промышленной сети АСУ ТП

В заключении можно отметить, что проблема сетевых атак в АСУ ТП на сегодняшний день является крайне острой, так как нестабильное функционирование АСУ ТП может вызывать серьезные последствия как в экономике, так и в экологии Российской Федерации. В связи с этим необходимость анализа существующих решений по безопасности промышленных сетей и кибератак крайне приоритетная задача, которая в дальнейшем позволит разрабатывать и создавать устойчивые к воздействиям злоумышленников системы.

СПИСОК ЛИТЕРАТУРЫ

1. Указ президента № 204: [Электронный ресурс] // Министерство энергетики РФ. URL: https://minenergo.gov.ru/view-pdf/11246/84473. (Дата обращения 16.09.2021)
2. Лукацкий А. В. Обнаружение атак //СПб.: БХВ-Петербург. – 2001. – Т. 624.
3. Debar H., Dacier M., Wespi A. Towards a taxonomy of intrusion-detection systems //Computer networks. – 1999. – Т. 31. – №. 8. – С. 805-822.
4. Heckerman D. A tutorial on learning with Bayesian networks //Innovations in Bayesian networks. – 2008. – С. 33-82.
5. Райзин Дж. Вэн. Классификация и кластер. – М.: Мир, 1980. – 390 с.
6. Браницкий А. А., Котенко И. В. Анализ и классификация методов обнаружения сетевых атак //Информатика и автоматизация. – 2016. – Т. 2. – №. 45. – С. 207-244.
7. Falco G., Caldera C., Shrobe H. IIoT cybersecurity risk modeling for SCADA systems //IEEE Internet of Things Journal. – 2018. – Т. 5. – №. 6. – С. 4486-4495.

8. Samtani S. et al. Identifying SCADA vulnerabilities using passive and active vulnerability assessment techniques //2016 IEEE Conference on Intelligence and Security Informatics (ISI). – IEEE, 2016. – С. 25-30.
9. Verba J., Milvich M. Idaho national laboratory supervisory control and data acquisition intrusion detection system (SCADA IDS) //2008 IEEE Conference on Technologies for Homeland Security. – IEEE, 2008. – С. 469-473.
10. T. Bartman and K. Carson, "Securing Communications for SCADA and Critical Industrial Systems," 2016 69th Annual Conference for Protective Relay Engineers (CPRE), no. College Station, TX, pp. 1-10, 2016.

УДК 004.056

A. N. HUSSEIN
ahmeddhicis11@gmail.com
Науч. руководд. – д-р физ.-мат. наук, проф. В. М. КАРТАК

Уфимский государственный авиационный технический университет

METHODS FOR DETECTING MODERN MALWARE USING BOOTKITS AS AN EXAMPLE

Abstract. This article discusses methods for detecting modern malware, the history of computer viruses, methods for detecting and introducing malware into information systems, a bootkit and modern methods for its detection.
Keywords: bootkit; malware; analysis method; program

Introduction

More and more different types of malwares appear every year. Originating as a very unusual phenomenon, primitive viruses, starting in the 1980s, gradually turned into complex technological developments, mastered new niches, and penetrated computer networks.

The earliest malware such as Cookie Monster, Animal and Creeper [6] appeared in the 1970s, but they were more annoying to users than malicious and destructive. Later, the viruses Elk Cloner (1981), Brain (1986), the Morris worm (1988) appeared

- they can, already be called full-fledged malicious programs, since the consequences of the actions performed by these programs were much more serious than from virusesof the 70s.

Constantly improving, malware is created and at the moment. For example, on October 5, 2020, Kaspersky Lab discovered a targeted cyber espionage campaign using the complex modular structure of Mosaic Regressor, which, among other things, includes a boot kit for the UEFI firmware embedded in the motherboard. The attacks were detected using Firmware Scanner technology. It has been a part of Kaspersky Lab products since the beginning of 2019 and its specially designed to detect threats hidden in ROM BIOS chips, including UEFI firmware images [8].

This article describes how malware works, how it can be detected, and how it is introduced into the system.

History

In 1969, Chris Tavares wrote the Cookie Monster program in PL / 1. [12] He manually sent messages that would block processes and send a "give me a cookie" request to the terminal. The program blocked the terminal until the operator entered the word "cookie". This malware is mistakenly, called a virus due to the peculiarity of its implementation, but it does not replicate itself and does not spread, and therefore is considered a protovirus.

The Multics operating system allows you to set the timer and end the program, and when the timer expires, the program starts again as if the call came from a terminal. Thus, one might think that the program whose execution was interrupted was "infected".

The history of computer viruses can be conditionally divided into several stages: the pre historic, "pre-Internet", Internet stage, and the modern (criminal) stage [5].

One of the first viruses of the pre historic stage, Creeper, was discovered on the military computer network ARPANET, the prototype of the modern Internet. The program was written for the RSEXEC subsystem of the Tenex operating system, which is responsible for the remote execution of programs on a computer network. He roamed the servers and could independently enter the network via a modem and transmit his copy to a remote system. On infected systems, the virus detected itself with the message “I’M THE CREEPER: CATCH ME IF YOU CAN”, which was displayed on the display or on the printer. To remove the virus, the first anti-virus program Reaper was written, which similarly spread over the network, deleted the detected copies of Creeper and then (presumably - after a certain period of time) self-destructed.

During the pre-Internet era, computers are becoming more and more popular. More and more programs appear, the authors of which are not software companies, but individuals. The development of telecommunication technologies makes it possible to

relatively quickly and conveniently distribute these programs through public access servers - BBS (Bulletin Board System). Later, semi-amateur, university BBSs evolve into global databanks covering virtually all developed countries. They provide a quick exchange of information between the most distant parts of the planet. The "global network" of BBS servers is gaining popularity and, as a result, is attracting the attentionof hooligan programmers. A large number of various "Trojan horses" appear - programs that do not have the ability to replicate, but when launched, causing any harmto the system.

The Apple II, developed in 1977, became one of the most successful personal computers of its time, with nearly two million produced. It was intended not only for professionals, but also for the general user - it was a computer for the home, it was used in schools and universities. As a result of its massiveness, it became a victim of the first documented computer virus - a certain Richard Skrenta, one of the millions of Apple II users, guessed to develop a self-replicating virus program for this computer.

The virus, called Elk Cloner, recorded itself in the boot sectors of floppy disks accessed by the computer's operating system. The virus manifested itself in many ways: it flipped the image on the screen, made the text blink. [17]

Internet stage. In January 1999, the global outbreak of the Happy99 (also known as Ska) Internet mail worm broke out. In fact, it was the first modern worm to open a new stage in the development of malware. He used MS Outlook for his distribution, which is the corporate standard in the United States and in many European countries.

The downloader Mlw # 41 (2019) of the APT group TA505 can be classified as modern malware. This sample is fixed in the system, collects information and sends it to the management server.

Detection methods and methods of implementing malware into information systems

Virus attacks are one of the primary threats to information security. Such actions cause financial damage, and also allow many other dangerous threats to be realized. Three main classes of methods are distinguished: signature, statistical and heuristic. [1]

Signature analysis method.

This method of detecting malware consists of checking the received files for virus signatures. The signature of a virus can be considered a set of features that identify the presence of a virus in a file. Such a signature should contain only unique lines from this file, so characteristic of a virus to guarantee the minimum possibility of false positives.

This method is implemented as follows: a signature database for known attacks is maintained with augmentation without performance loss. As a result of the analysis, the recorded sequence of events is compared with known attack signatures. If it matches, an intrusion attempt signal is issued. Further actions are determined by the algorithms of the reaction module: virus removal or notification. [3]

The step-by-step signature-based detection process looks like this:

1. A new type of malware is being detected.
2. A trace of malware is entered into the database.
3. Antivirus software and database are updated.
4. Antivirus is able to find this malware during scanning, when using the searchon the trail. [16]

Statistical analysis method.

This method is designed to detect the safety behavior of programs and intruder detection systems. This method is divided into 2 types of analysis methods: static analysis of the sequence of system calls and the state machine method.

Statistical analysis of the sequence of system calls is based on the fact that each new observation of a variable must fit within certain boundaries. If this does not happen, then there is a deviation. The resource intensity of the method is high, the virus software detection time is high, the detection efficiency at an early stage is high, the detection efficiency at the late stage is low, and false positives are minimal.

The finite state machine method consists in developing a state machine for recognizing the "language" of the program trace. For this, there are many techniques based on the use of both deterministic and probabilistic automata. The resource

intensity of the method is low, the detection time for virus software is low, the detection efficiency at an early stage is high, the detection efficiency at the late stage is low, and false positives are maximum. [7]

Heuristic analysis method.

Heuristic analysis is a method of detecting viruses by examining the code for suspicious properties. [11]

There are two main types of heuristic analysis: dynamic and static.

During the dynamic heuristic analysis, the scanned file is launched in a safe virtual space - "sandbox", after which the antivirus analyzes its actions in the operating system. The main drawback of dynamic analysis is its demanding computational resources to emulate the operating system.

In contrast, statistical heuristic analysis does not have this drawback. The analysis examines the structure and contents of the file and identifies signs that are characteristic of other previously studied viruses. Static heuristic analysis is based on the binary classification problem, which consists of two main stages: training the classifier and recognition (determining whether an unknown file is malicious or legitimate). The stage of training is a priority and largely determines the accuracy of the classification. [4]

Now let's move on to the currently known methods of introducing malware intoinformation systems.

At the moment, there are two relevant ways to introduce computer viruses that users do not know about, and antiviruses do not have sufficient experience to track them in a timely manner:

– Using a joiner of files and then distributing them under the guise of an ordinary program.

– Using unicode characters in virus file names. [12]

Joiner — program that allows malware to be “glued” with any file into the final “.exe” format. Thus, taking, for example, the distribution kit of the 2GIS program, it

becomes possible to associate it with a virus and send it as a regular installer to an ordinary user.

The simplest joyer is any archiver (for example, WinRAR). Archivers have the function of creating self-extracting SFX archives, with the output extension ".exe".

Thus, two executable files are added to the archive and packed. Further, it remains a method of simple deception to force the computer user to open this archive, and from that moment the process is not reversible. By the way, antiviruses do not react in any way to this method of splicing files, since it is considered legal. SFX archives are used in ubiquitous use, although not as often as intended. Antivirus developers do not take into account the fact that this method is also used for personal gain. [10]

Unicode is a character encoding standard that allows characters to be represented in almost all written languages. The standard was proposed in 1991 by the non-profit organization "Unicode Consortium". The use of this standard allows you to encode a very large number of characters from different scripts: in Unicode documents, Chinese characters, mathematical characters, letters of the Greek alphabet, Latin and Cyrillic alphabet can coexist, thus it becomes unnecessary to switch code pages. [15]

It is very easy to add Unicode to the file name, just open the context menu and select the desired character. In our case, this is the RLO code. The essence of this code is to mirror characters after the inserted code. For example, the file has the name "TESTgpj.exe", inserting RLO after "TEST", we get: "TESTexe.jpg". The point of rearranging file extensions is that an ordinary user will first look at the file extension so as not to infect his computer. The victim, guided by his basic knowledge, will understand that this is an image (".jpg" format) and discard any suspicions.

Antivirus programs are also powerless in this case, because they simply do not check file names for Unicode characters in it. This function is standard in Windows operating system. [10]

Bootkit and modern methods of its detection

Bootkits are currently the most advanced technology available to cybercriminals. The technology allows malicious code to run before the operating system is loaded; it

is implemented in many malicious programs. Bootkits exist; they are in demand on the black market and are widely used by cybercriminals for various purposes, including targeted attacks. [14]

Next, we will consider the early launch module for countering malware, implemented in Windows 8, and subsequently in Windows 10.

Windows 8/10 includes a new security feature called Safe Boot that protects Windows boot configuration and components and loads the Anti-Malware Early

Startup (ELAM) driver. This driver starts before other drivers at startup and allows youto evaluate these drivers, and helps the Windows kernel decide whether to initialize them. ELAM is started first by the kernel, so it starts earlier than any other third partysoftware. Hence, it is able to detect malware in the boot process itself and prevent it from being downloaded or initialized. [9]

The ELAM driver registers callback routines that the existing kernel uses to evaluate data in its registry hive and startup drivers. These callbacks detect malicious data and modules and prevent Windows from loading and initializing them.

The existing Windows kernel enters and excludes such callbacks from the registry by implementing such API routines:

Cm Register Callback Ex и CmUn Register Callback Register and exclude callbacks to track registry data.

- IoRegister Boot Driver Callback
- IoUnRegisterBootDriverCallback

Startup drivers are entered into the registry and excluded from it.

These callback routines use the established prototype EX_CALLBACK_FUNCTION.

ELAM Callback Prototype

```
NTSTATUS EX_CALLBACK_FUNCTION(
1 IN PVOID CallbackContext,
2 IN PVOID Argument1,          // callback type
3 IN PVOID Argument2           // system-provided context structure
);
```

Fig. 1.

Parameter (1) CallbackContext gets some context from its ELAM driver after that driver has executed one of the above callbacks to register some callbacks. The context value is a pointer to a buffer in memory that holds ELAM driver-specific parameters that can be accessed by one of these callback routines. Such a context is a kind of pointer, which is also used to store the value of the current state of the ELAM driver itself.

The argument value (2) provides a callback type, which can be one of the following for their startup start drivers:

- BdCb Status Update (Provides the status of updates for some ELAM driver, depending on the dependencies of the loaded driver itself or the startup start drivers.)
- BdCbInitializeImage (Used by this ELAM driver to classify startup drivers andtheir dependencies.)

The value of argument (3) provides information that the operating system itself uses to classify such a startup driver as known good (driver known to be legitimate and clean), unknown (unknown good, driver that ELAM is not able to classify) and known bad (known bad, drivers known to be malicious). [13]

ELAM gives security software an edge over rootkit threats, but not against bootkits. ELAM is only capable of keeping track of legally loaded drivers, however most bootkits load kernel-mode drivers that take advantage of undocumented functionality of the operating system.

This means that a certain bootkit is able to bypass security compulsions and inject its code into the kernel address space despite ELAM.

The malicious bootkit code runs before the kernel of its operating system is initialized and before any kernel-mode drivers are loaded, including ELAM. This means that some bootkit is able to evade ELAM protection.

The thread of the startup process with ELAM

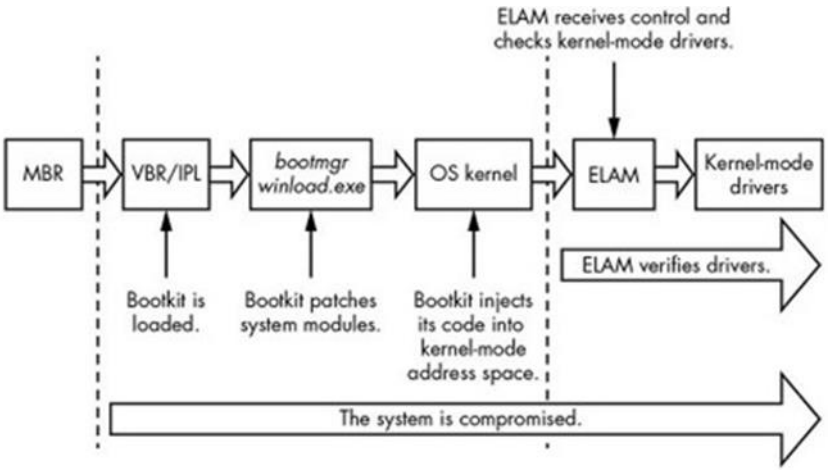


Fig. 2.

The malicious bootkit code runs before the kernel of its operating system is initialized and before any kernel-mode drivers are loaded, including ELAM. This means that some bootkit is able to evade ELAM protection.

Most bootkits load their kernel mode code in the middle of kernel initialization, when all OS subsystems (Input / Output subsystem, object manager, plug-in manager, etc.) have already been initialized, but before ELAM is executed. ELAM, of course, is not able to prevent the execution of the malicious code that is loaded before it, and therefore it does not have any protection against bootkit technologies. [2].

The family of bootkits behaves quite stealthily; it cannot be detected by standard means on an infected system, since when accessing infected objects it "substitutes" the original copies. In addition, the main body of the malware (kernel-level driver) is not present on the file system, but is located in an unused part of the disk outside the last partition.

The malicious program loads the driver on its own, without the help of the operating system. The operating system itself is unaware of the presence of a driver. Detecting and treating this bootkit is the most challenging task the antivirus industry has faced over the years. The way to deal with bootkits is to boot the system from any removable uninfected media in order to avoid the main boot of the virus after turning on the computer, and then overwrite the boot sector with its BOOTSECT.BAK backup, which is always in the root directory of the system volume.

Conclusion

This article reviewed the history of computer viruses from prehistoric to modern times. Methods for detecting and introducing malware into information systems, modern methods for detecting bootkits are considered in detail.

REFENCES

1. Bulakhov N.G., Kalayda V.T. "Methods for the detection and neutralization of self-replicating viruses." 2008 r.
2. Security of the launch process [Electronic resource] Access mode: http://onreader.mdl.ru/RootkitsAndBootkits/content/Ch06.html.
3. Gorbunov A.N., Emelianenko T.G. "Principles of using signature analysis to detect malware." 2013 g.
4. Demina R.Yu., Azhmukhamedov I.M. "Improving the efficiency of heuristic analysis in the antivirus package Stronghold Antimalware" 2018
5. History of Virology [Electronic resource] Access mode: https://www.sites.google.com/site/komputernyevirusy25/istoria-virusologii.
6. History of computer viruses and malware [Electronic resource] Access mode: https://encyclopedia.kaspersky.ru/knowledge/history-of-malicious-programs.
7. Korneychenko A.V. Analytical review of methods for detecting malware in distributedcomputing systems 2019
8. Mosaic of regression: new malware detected to infect a computer at a low level [Electronic resource] Access mode: https://www.kaspersky.ru/about/press- releases/2020_mozaika-regressa-obnaruzheno-novoe-vredonosnoe-po- dlya-zarazheniya-kompyutera-na-nizkom-urovne.
9. Understanding the technology of protection against early launch malware (ELAM) in Windows [Electronic resource] Access mode: https://techarks.ru/general/osobennosti/ponimanie-tehnologii-zashhity-ot-vredonosnyh-programm-rannego-zapuska- elam-v-windows.
10. Rudnichenko A.K., Shakhanova M.V. "Actual ways of introducing computer viruses into information systems."
11. Heuristic analysis [Electronic resource] Access mode: https://ru.qaz.wiki/wiki/Heuristic_analysis.
12. Cookie Monster [Electronic resource] Access mode: https://ru.wikipedia.org/wiki/Cookie_Monster.
13. Matrosov A., Rodionov E., Bratus S. - "Rootkits and Bootkits Reversing Modern Malware and Next Generation Threats" 2019
14. Sajedul Talukder - "Tools and Techniques for Malware Detection and Analysis" 2020
15. Unicode (Bauman National Library [Electronic resource] Access mode: https://ru.bmstu.wiki/Unicode.
16. What Is Signature-Based Malware Detection? [Electronic resource] Access mode: https://www.logixconsulting.com/2020/12/15/what-is-signature-based-malware-detection.
17. 1980s [Electronic resource] Access mode: https://encyclopedia.kaspersky.ru/knowledge/years-1980s.

СЕКЦИЯ 5.5
ГЕОИНФОРМАЦИОННЫЕ СИСТЕМЫ

УДК 912.43

И. И. АБСАЛЯМОВА
absalyamchik13@gmail.com
Науч. руководв. – канд. техн. наук, доц. А. Х. АБДУЛЛИН

Уфимский государственный авиационный технический университет

ПРОСТОЕ ПОЛУЧЕНИЕ ПРОСТРАНСТВЕННЫХ ДАННЫХ OPENSTREETMAP

Аннотация. В статье кратко рассматривается веб-ресурс Geofabrik для получения (загрузки) векторных пространственных данных OpenStreetMap. Обосновываются преимущества использования Geofabrik для актуализации собственных веб-карт и слоев.
Ключевые слова: OpenStreetMap; OSM; ГИС; карты.

Одним из наиболее популярных источников пространственных данных для широкого применения являются картографические данные OpenStreetMap (OSM) – открытого некоммерческого проекта по картографированию земной поверхности, появившегося в 2004 году благодаря инициативе IT-инженера Стивена Коста [1]. В веб-картографии и ГИС этот проект обрел мировую известность и получил всеобщее одобрение и поддержку. Популярности OpenStreetMap способствуют не только открытость и свободное использование данных, но также простота их получения и использования.

С получением (загрузкой) данных OSM так или иначе приходится сталкиваться практические каждому разработчику картографических приложений или аналитику, использующему в своем исследовании картографические данные. Легко и быстро получить данные OSM – это один из первых этапов составления собственной карты, отвечающей индивидуальным требованиям. При создании ГИС-проектов автором статьи используется веб-ресурс Geofabrik (http://www.geofabrik.de/) – немецкий проект, предоставляющий простой и быстрый способ загрузить локально данные OSM в формате, удобным для последующей работы в ГИС-пакетах ESRI ArcGIS или QGIS [2]. Следует отметить, что ресурсов, предоставляющих данные OSM для загрузки на собствен-

ный компьютер довольно много, но по совокупности качеств Geofabrik является одним из наиболее полезных:

– разнообразие форматов файлов для загрузки;

– возможность извлечь историю правок объектов на карте OSM;

– актуальность предлагаемых к загрузке данных почти не отличается от исходных данных OSM, как заявляют авторы проекта, разница составляет не более двух дней;

– различные уровни обработки данных OSM, начиная от необработанных данных OSM для бесплатной загрузки (raw OSM data) до предварительно обработанных данных за небольшую однократную плату или постоянный доступ по подписке;

– наличие простого API (Overpass API) для извлечения данных по тэгам и создания скриптов для сценариев обработки данных;

– интуитивно ясная модель разграничения наборов данных OSM по региональному признаку: часть света – страна – регион страны;

– “бережное” обращение с тэгами и с содержанием слоев;

– сравнительно высокая скорость загрузки данных.

Типичный сценарий использования данных OSM заключается в первоначальной загрузке всего набора данных для выбранного региона, оформления и стилизации карты, обогащения карты, создания какого-либо производного картографического продукта (карты или картографического приложения). Для актуализации карты целесообразно обновлять только измененные объекты на карте, если дизайн ГИС-проекта предусматривает такую возможность. Geofabrik способствует именно такому подходу в разработке карты, что выгодно отличает его от других ресурсов.

СПИСОК ЛИТЕРАТУРЫ

1. Зачем миру нужен OpenStreetMap /пер. с англ. статьи “The World Cares About OpenStreetMap” Serge Wroclawski, 05.01.2014// ресурс https://habr.com/ru/post/217291/, 28.03.2014.
2. Ресурс https://learnosm.org/en/osm-data/geofabrik-and-hot-export/, дата обращения 15.09.2021.

УДК 004

Е. А. АТАРСКАЯ
arskaya25@mail.ru
Науч. руководов. – канд. техн. наук, доц. А. Ф. АТНАБАЕВ

Уфимский государственный авиационный технический университет

ПРИМЕНЕНИЕ ТЕХНОЛОГИЙ ГЕОИНФОРМАЦИОННЫХ СИСТЕМ В ПРОМЫШЛЕННОСТИ

***Аннотация*.** Целью исследования является повышение эффективности работы промышленного предприятия за счет использования ГИС технологий. В статье рассматривается применение ГИС технологий в сфере промышленных предприятий для решения различных прикладных задач.
***Ключевые слова*:** геоинформационные технологии; промышленность.

Актуальность работы обусловлена широким использованием геоинформационных систем (ГИС) для создания, хранения, манипулирования, визуализации и анализа пространственно распределенных данных, характеризующих ход технологического процесса на промышленном предприятии.

Огромное количество пространственно распределеннной информации на производстве требует интерпретации и анализа для дальнейшего использования.

Объект исследования – применение ГИС технологии в производственных организациях.

Предмет исследования – технологии геоинформационных систем для промышленных предприятий.

Цель работы: повышение эффективности промышленного предприятия за счет использования ГИС технологий.

Задачи:

– исследование промышленного объекта и технологических процессов его функционирования;

– анализ промышленного объекта в задаче применения ГИС технологий.

Современные геоинформационные системы (ГИС) предоставляют цифровые инструменты для организации и оперирования пространственными данны-

ми, моделирования географических (происходящих в пространстве) процессов, визуализации этих данных, моделей и процессов с помощью развитых компьютерных средств, специализированных инструментов обработки и анализа геоданных.

Пространственные исследования дают возможность превратить статические и географические данные в имеющую глубокий смысл и одновременно простую для восприятия информацию, используемую в процессе принятия решений.

У предприятий различного профиля имеется ряд задач, для которых ГИС жизненно необходима и используется в настоящее время [1].

Например, компании, обеспечивающие коммунальные услуги, являются активными пользователями ГИС. Геоинформационные системы в данном случае используются для построения базы данных о трубопроводах, кабелях, насосных и распределительных станциях. ГИС обеспечивает возможность полного моделирования коммунальных сетей, таких как сети, поставляющие воду, электроэнергию и телекоммуникации большому количеству потребителей. Такая система может работать в различных масштабах, моделируя подключения к потребителям, районы обслуживания, а также подробные перечни и схемы расположения объектов, таких как трансформаторы, арматура, трубопроводы и принципиальные схемы [2].

ГИС может использоваться промышленными объектами для управления пространством, его визуализацией, планированием, а также для реагирования на чрезвычайные ситуации и стихийные бедствия. Его можно использовать на протяжении всего жизненного цикла объекта от принятия решения о том, где строить, до планирования пространства.

ГИС технологии на промышленных предприятиях применяются для решения различных прикладных задач:

– принятие решений на всех уровней управления,

– оптимальное проектирование объектов промышленного назначения,

– совершенствование функций учета и рационального использования ресурсов,

– получение достоверной информации о местоположении и эксплуатации инженерных сетей и измерительных датчиков.

Широко используется также моделирование процесса использования различных прокладываемых коммуникаций в условиях их отклонений от требований инструкций. Наибольшее применение в этой области находят системы автоматизации картографирования (АК) и управления основными средствами (УОС). Функции АК и УОС используются для поддержания процессов прокладки коммуникаций [2].

Благодаря однозначной идентификации объектов промышленных предприятий, имеющих территориальную привязку, появляется возможность осуществлять по запросам выборку по объектам из разрозненных БД и выполнять управление (автоматизация процесса инвентаризации основных фондов, складской учет и т.д.) [3].

Предложенный в статье [4] набор данных АСУ ТП собран в ходе испытанной реальной АСУ ТП и дополнен результатами программно-аппаратного моделирования генерации энергии паровой турбиной и процесса гидроаккумулирования энергии.

Стенд состоит из котла, турбины, водоподготовительного узла и HIL-симулятора. Процесс, происходящий в котле, – это процесс водяного теплообмена с низким давлением и умеренными температурами. Процесс в турбине включает использование испытательного стенда комплекта ротора, который точно имитирует поведение реального устройства с вращающимися частями. Процесс водоподготовки включает закачку воды в верхний резервуар и последующий сброс ее в нижний резервуар с использованием модели выработки гидроэлектроэнергии с гидроаккумулятором во время HIL-симуляции.

Реальные процессы контролируются тремя различными типами контроллеров. Технологический процесс на испытательном стенде показан на рисунке

4 и может быть разделен на четыре основных процесса: процесс котла (P1), процесс турбины (P2), процесс водоподготовки (P3) и HIL-моделирование (P4). HIL-моделирование усиливает корреляцию между тремя реальными процессами на уровне сигнала, моделируя сценарии выработки тепловой энергии и генерацию гидроаккумулирования энергии.

Процессы котла и турбины используются для моделирования тепловой электростанции, а процесс очистки воды используется для моделирования гидроаккумулирующей электростанции.

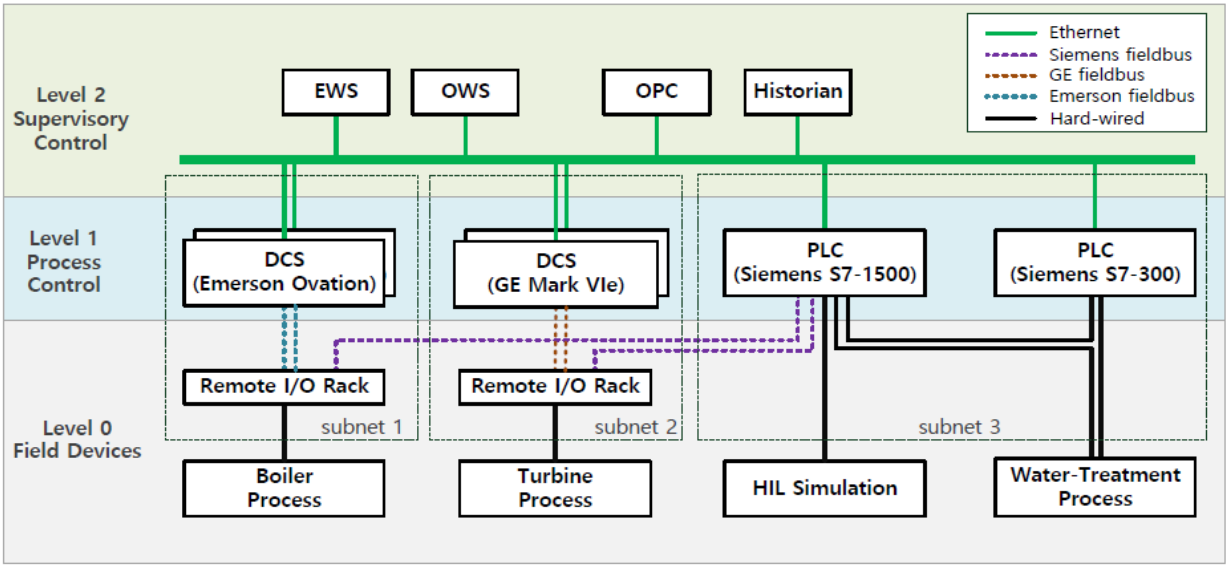


Рис. 1. Тестируемые компоненты и поток данных

Реальные процессы контролируются тремя различными типами контроллеров. Уровень воды, расход, давление, температура, насос подачи воды и управление нагревателем в котле контролируется системой DCS Emerson Ovation. Для управления скоростью и мониторинга вибрации в процессе турбины используется DCS Mark VIe компании General Electric. Процесс обработки воды контролируется ПЛК Siemens S7-300, который управляет уровнем воды и насосом. В испытательном стенде HAI моделирование HIL проводилось с использованием системы dSPACE® SCALEXIO, соединенной с реальными процессами с помощью ПЛК S7-1500, ПЛК (Siemens) и с устройствами удаленного ввода-вывода ET200 [4].

Для представленного испытательного стенда ГИС технологии могут предложить новое качество в описание объектов и новые функции для работы с ними:

– информацию о положении объектов (датчиков, контроллеров, коммуникации) в пространстве;

– пространственные связи объектов, выражаемые через топологические отношения (тестируемые компоненты и потоки данных);

– визуальное представление объектов, которое может изменяться в зависимости от изменения состояния параметров объектов (открытие/закрытие клапанов, изменение уровня воды, положение поршня);

– пространственный анализ.

Цикл работы с ресурсами и средствами предприятия теперь может быть дополнен:

– учетом и паспортизацией объектов, включающая в себя выявление объектов, описание их точного местоположения, пространственных, технологических и иных характеристик;

– установлением технологических связей и правил функционирования отдельных элементов и системы в целом;

– оценкой состояния объектов;

– мониторингом состояния объектов (периодическое обновление параметров системы);

– анализом состояния и функционирования объектов;

– планированием деятельности (планирование работ по обслуживанию и т.д.);

– управлением объектами: принятие и реализация решений.

ГИС технологии могут применяться для повышения эффективности выполнения задач по управлению инфраструктурой предприятия. Обеспечение служб предприятия актуальной и полной информацией об инженерно-технических сооружениях и оборудовании предприятия, их текущем состоянии

и взаимном расположении позволяют обеспечить своевременное обслуживание системы и снизить риск отказа оборудования, планировать и проводить капитальные ремонты и работы по реконструкции. Также ГИС используется для проведения инвентаризации и учета, получения электронных и печатных выкопировок генплана предприятия [1].

СПИСОК ЛИТЕРАТУРЫ

1. Применение геоинформационных технологий в промышленности [Электронный ресурс]. – Режим доступа: https://cyberleninka.ru/article/n/primenenie-geoinformatsionnyh-tehnologiy-v-promyshlennosti/viewer
2. Гиниятуллина О. Л., Хорошева Т. А. Геоинформационные системы: учебное пособие / Кемерово : КемГУ, 2018. – 122 с. [Электронный ресурс]. – Режим доступа: https://e.lanbook.com/book/120040 (дата обращения: 22.09.2021).
3. Производственные геоинформационные системы [Электронный ресурс]. – Режим доступа: https://arcreview.esri-cis.ru/2001/08/15/production-geoinformation-systems/
4. HAI Security Dataset | Kaggle [Электронный ресурс]. – Режим доступа: https://www.kaggle.com/icsdataset/hai-security-dataset

УДК 004

А. И. АЮПОВА
adelina-ayupova-00@mail.ru
Науч. руководит. – канд. техн. наук, доц. О. А. ЕФРЕМОВА

Уфимский государственный авиационный технический университет

ПРИМЕНЕНИЕ ГЕОИНФОРМАЦИОННЫХ СИСТЕМ ДЛЯ ИНФОРМАЦИОННОЙ ПОДДЕРЖКИ ДЕЯТЕЛЬНОСТИ СОТРУДНИКОВ, ОТВЕТСТВЕННЫХ ЗА ПОЖАРНУЮ БЕЗОПАСНОСТЬ ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ

Аннотация. Объектом исследования является ФГБОУ ВО «Уфимский государственный авиационный технический университет». Предметом исследования является пространственная информация об объектах ФГБОУ ВО «УГАТУ». Тема исследования посвящена разработке подсистемы информационной поддержки деятельности службы обеспечения пожарной безопасности в составе ГИС «УГАТУ».
Ключевые слова: геоинформационные системы; ГИС УГАТУ; ГИС ИнГео; обеспечение пожарной безопасности; образовательное учреждение.

Введение

Обеспечение пожарной безопасности в университете является - составной частью системы комплексной безопасности, направленной на сохранение жизни и здоровья работников и студентов в повседневной жизнедеятельности и при возникновении чрезвычайных ситуаций.

Организация, координация и контроль работы по обеспечению пожарной безопасности в университете осуществляется отделом по охране труда. Все помещения образовательной организации закрепляются за ответственными лицами согласно утвержденным руководителем спискам. Ответственные лица должны следить за чистотой помещений, противопожарной и электробезопасностью.

Деятельность сотрудников университета, ответственных за пожарную безопасность тесно связана с пространственной и атрибутивной информацией (сведения о датчиках пожарной сигнализации, огнетушителях, звуковых оповещателях, пожарных кранах, эвакуационных выходах и т.д.).

Актуальность

На основе опросов руководителей технических служб образовательного учреждения были сделаны выводы о большом количестве устаревших и неактуальных материалов, с которыми приходится сталкиваться службам в своей работе. Разработка подсистемы должна обеспечить ввод учета актуальности тех или иных технических документов, а также сортировку и проверку пригодности новых поступающих данных о техническом состоянии таких объектов как датчики пожарной сигнализации, огнетушители, звуковые оповещатели, пожарные кранаы, эвакуационных выходы и т.д.

Эксплуатируемые в образовательном учрежднии информационные системы не решают следующих задач:

– ввод, хранение и предоставление пространственной и атрибутивной информации об объектах ответственности сотрудников, отвечающих за пожарную безопасность по различным критериям (сведения о датчиках пожарной сигнализации, огнетушителях, звуковых оповещателях, пожарных кранах, эвакуационных выходах и т.д.);

– актуализация и обновление пространственных и атрибутивных данных об объектах ответственности подразделения по обеспечению противопожарной безопасности;

– предоставление пространственной и атрибутивной информации в различных форматах для создания отчетной документации подразделения по обеспечению противопожарной безопасности.

Пожарная безопасность и ее основные принципы

Пожарная безопасность подразумевает надлежащее состояние объекта с исключением возможности возникновения очага возгорания (пожара) и его распространения в пространстве.

Пожарная безопасность объекта - возможность предотвращения возникновения пожара и его развития на объекте, воздействия на граждан и имущество его опасных факторов. Ее должны обеспечивать системы предотвращения пожара, а также противопожарной защиты.

Меры пожарной безопасности — действия по обеспечению пожарной безопасности, в том числе по выполнению требований пожарной безопасности.

Общие правовые, экономические и социальные основы обеспечения пожарной безопасности в Российской Федерации определяет Федеральный закон от 21 декабря 1994 г. №69-ФЗ “О пожарной безопасности”. Нормативными правовыми документами в области пожарной безопасности также служат “Правила противопожарного режима в Российской Федерации”, государственные стандарты системы стандартов безопасности труда, строительные нормы и правила, нормы пожарной безопасности и др.

Целью создания систем противопожарной защиты является защита людей и имущества от воздействия опасных факторов пожара и (или) ограничение его последствий. Защита людей и имущества от воздействия опасных факторов пожара и (или) ограничение его последствий обеспечиваются снижением динамики нарастания опасных факторов пожара, эвакуацией людей и имущества в безопасную зону и (или) тушением пожара.

Обеспечение пожарной безопасности

Обеспечение пожарной безопасности – приоритетная задача для любого предприятия, организации, учреждения, офиса и частного дома.

Порядок обеспечения пожарной безопасности включает в себя следующие направления:

– Соблюдение всех правил противопожарного режима;

– Наличие необходимой документации об установлении противопожарного режима;

– Исключение факторов, влияющих на возникновение пожара;

– Выполнение норм и требований по содержанию эвакуационных путей и выходов;

– Соответствие архитектурных и конструктивно-плановых решений установленным требованиям;

– Установка в зданиях, сооружениях, помещениях систем автоматической защиты от пожара;

– Техническое обслуживание подсистем автоматической защиты;

– Контроль над работой коммуникаций здания;

– Всестороннее обеспечение работы структурных подразделений пожарной охраны;

– Проведение спасательных работ.

Разработка подсистемы для сопровождения деятельности по обеспечению пожарной безопасности

Архитектура взаимодействия пользователя с подсистемой обеспечения пожарной безопасности. Данная подсистема функционирует согласно архитектуре, изображенной на рисунке ниже (Рисунок 1).

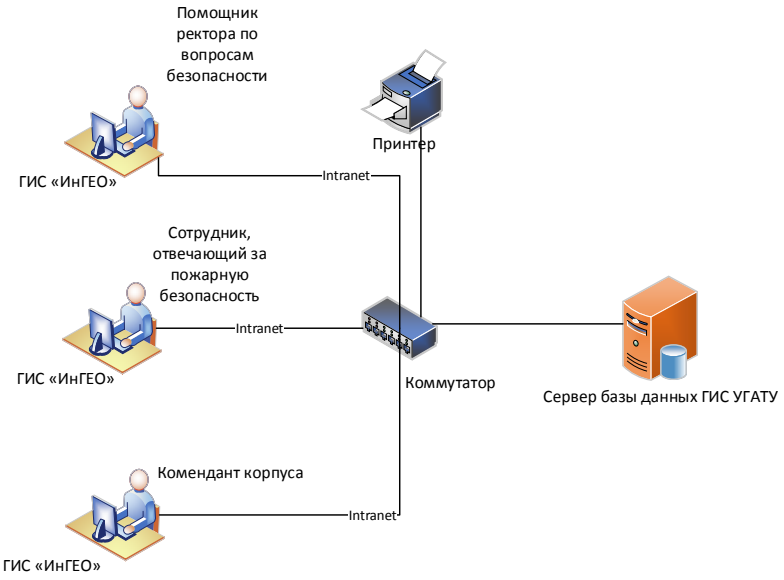


Рис. 1. Архитектура взаимодействия пользователя с подсистемой

Был определен набор информации, которая будет использоваться в ходе реализации разрабатываемой ГИС.

Исходная информация была взята из следующих источников:

1) Оцифрованный ген.план УГАТУ;
2) План коммуникаций УГАТУ;
3) Официальный сайт УГАТУ;
4) Физический сбор информации о средствах пожаротушения.

В подсистеме представлен ряд инструментов, реализующих заданные функции:

1. Настройка отображения и создание тематической карты. На главной форме представлен инструмент настройки слоев для отображения базовой карты и специализированный информации (Рисунок 2).

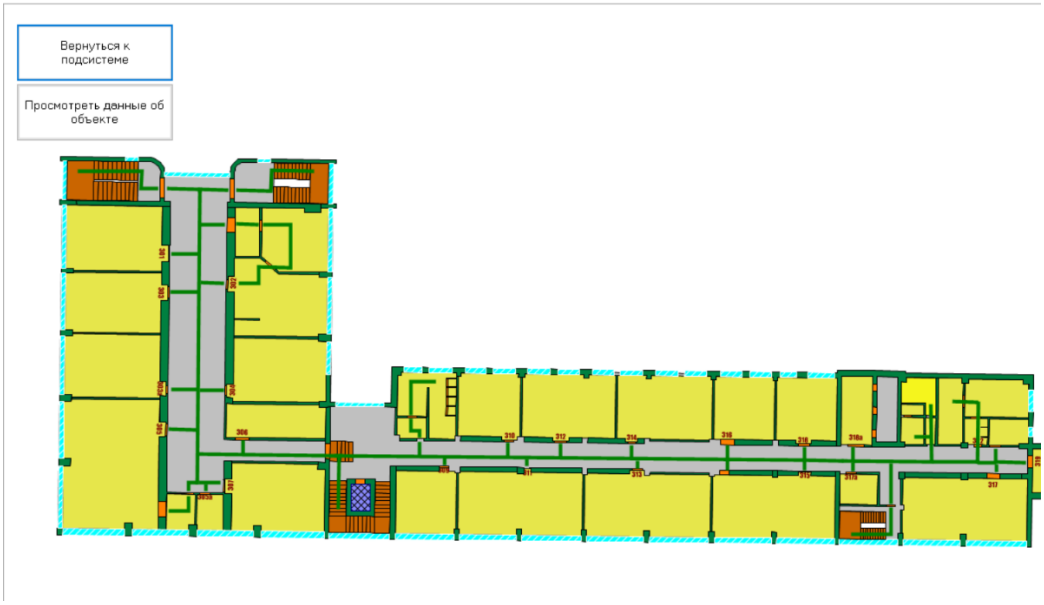


Рис. 2. Настройка отображения и создание тематической карты

2. Информационно-поисковый запрос. Данный инструмент позволяет пользователю произвести поиск объектов по заданным критериям атрибутивных данных при работе с активным слоем. Запрос строится на логическом выражении, а его результатом будет являться набор данных, которые удовлетворяют критериям поиска по ключевому слову (Рисунок 3).

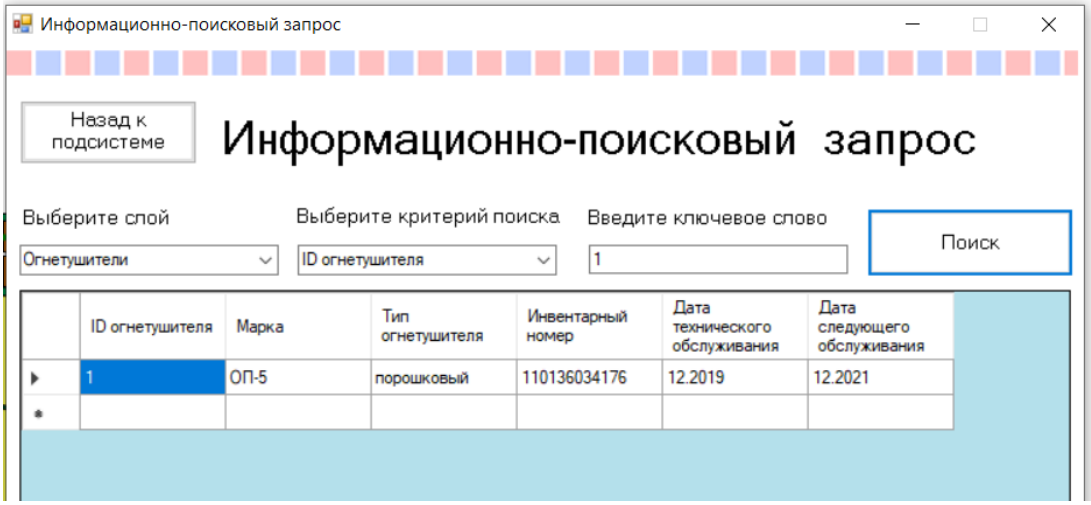


Рис. 3. Пример информационно-поискового запроса по ключевому слову

Заключение

В результате исследования была создана система противопожарной защиты людей и имущества от воздействия опасных факторов пожара и ограничение его последствий. Защита людей и имущества от воздействия опасных факторов пожара и ограничение его последствий обеспечиваются снижением динамики нарастания опасных факторов пожара, эвакуацией людей и имущества в безопасную зону и тушением пожара.

Внедрение разработанной подсистемы обеспечит информационную поддержку сотрудников управления пожарной безопасности, а также позволит актуализировать пространственные и атрибутивные данные об объектах ответственности подразделения управления пожарной безопасности.

СПИСОК ЛИТЕРАТУРЫ

1. Приказ ФГБОУ ВО УГАТУ от 26 декабря 2016 г. №2272 - О «Об утверждении инструкции по оформлению выпускных квалификационных работ обучающихся по образовательным программам высшего образования - программам бакалавриата, программам специалитета и программам магистратуры»;
2. ГОСТ 2.104-2006 Единая система конструкторской документации. Основные надписи;
3. ГОСТ 19.701-90. «Схемы алгоритмов, программ, данных и систем. Условные обозначения и правила выполнения»;
4. Методические указания для выполнения выпускной квалификационной работы для студентов специальности 230201 «Информационные системы и технологии» [Текст] / Сост.: С.В. Павлов, Г.М. Сайфутдинова, О.И. Христодуло, Р.А. Шкундина. – Уфимск. гос. авиац. техн. ун-т. – Уфа, 2008 –72 с.;
5. Рябышева, И. В. Сравнительный анализ подходов к проектированию информационных систем. Доклад в секции информационные технологии [Текст]/ Всероссийская конференция молодых ученых по математическому моделированию и информационным технологиям с участием иностранных ученых 1-3 ноября, г. Новосибирск, Россия. – 2008. – 8 с.
6. Гаврилов А.В. Использование современных CASE-средств структурного проектирования при обучении студентов по направлению подготовки «прикладная информатика» [Текст]/Открытое образование. – 2015. − №4(111). − с: 22-27.
7. Коломец Н. В. О методах и средствах проектирования программного обеспечения (обзор и примеры)[Текст]/ Ростовский научный журнал. – 2017. – №4. – с. 249-265.
8. Ципилева Т.А. Геоинформационные системы [Текст]: учебное пособие − Томск: Томский межвузовский центр дистанционного образования, 2004.− 162 с.
9. Рыбанов А.А. Инструментальные средства автоматизированного проектирования баз данных: Учебное пособие и варианты заданий к лабораторным работам по дисциплине «Базы данных» [Текст]/ВолгГТУ, Волгоград, 2007. – 96 с.

УДК 5.5

И. И. ВИТВИНОВА, В. А. МАЛИНСКАЯ
Inna.Vitvinova@yandex.ru
Науч. руководв. – канд. техн. наук, доц. А. Ф. АТНАБАЕВ

Уфимский государственный авиационный технический университет

МОНИТОРИНГ МАРШРУТА СЛЕДОВАНИЯ ТРАНСПОРТНОГО СРЕДСТВА

Аннотация. В статье описаны основные причины рассматриваемой темы, концепция процесса мониторинга, некоторые возможные решения, помогающие реализовать данную задачу.

***Ключевые слова*:** критерии выбираемого оборудования; приемники спутниковых сигналов; система транспортного мониторинга.

Введение

Актуальность рассматриваемой темы подтверждается тем, что в современном мире транспортное средство выступает в роли важного элемента. Без него не представляется возможным перемещение между городами и внутри населенных пунктов. Кроме того, транспорт помогает решить такие вопросы как перемещение различных грузов. По мере роста сети дорог и увеличения населения в городах с каждым годом перемещение становится все большей проблемой.

Отличным способом повышения безопасности на дорогах является мониторинг транспорта. Обычно это трекинговый мониторинг: на транспортное средство устанавливается GPS-трекер. Это устройство может следить за действиями водителя, собирать данные о техническом состоянии и о количестве топлива, с помощью теплодатчиков и датчиков скорости не дает двигателю перегреться и помогает контролировать его скорость. Такой трекинг помогает диспетчеру или оператору решать вопросы, связанные с графиками рейсов, а также отправляет ему актуальную информацию о местоположении транспортного средства. Кроме того, данный прибор может обеспечить связь с водителем при определенных случаях.

Проведение анализа предметной области

Мониторинг маршрута следования представляет собой контроль объекта наблюдения в режиме реального времени. Большое распространение в этой предметной области получили «онлайн приборы», которые объединяют гео-

данные, полученные спутниковым приемником и преобразованные в цифровую форму, обрабатывают с помощью GPRS-технологий и передают пользователю для последующей обработки.

К критериям, позволяющим выбрать это оборудование, можно отнести: приемники спутниковых сигналов, количество входов/выходов, различные типы входных сигналов и их возможность обработки бортовым оборудованием, возможность перепрограммировать встроенный контроллер в дистанционной форме, устойчивая работа в местах со слабой сотовой связью, а также размер генерируемого трафика.

Система транспортного мониторинга – это аппаратно-программный комплекс, основанный на использовании таких информационно телекоммуникационных технологий [1] как спутниковое позиционирование ГЛОНАСС и GPS, сотовая связь GSM, УКВ-связь, интернет, вычислительная техника и микроэлектроника [2].

Специальное навигационное GPS оборудование (GPS-маячок, GPS-трекер, бортовой терминал, GPS-контроллер) устанавливается на транспортное средство. Используя приемник спутниковых навигационных систем ГЛОНАСС или GPS, терминал автоматически определяет местоположение, скорость, направление движения автотранспорта, а также маршрут автомобиля и состояние подключенных датчиков [3].

Терминал передает собранную информацию по беспроводным каналам связи автоматически или по запросу пользователя. В качестве собранной информации может выступать как сотовый канал системы GSM стандарта GPRS/SMS, так и УКВ канал. Вся информация об этом процессе отправляется на сервер системы слежения ГЛОНАСС/ GPS, там она обрабатывается и сохраняется в базе данных [4].

Чтобы диспетчер мог видеть текущее местоположение и перемещение объекта, на его рабочем месте установлено специальное программное обеспечение, в котором с высокой точностью отображаются электронные векторные многослойные карты местности [5].

Анализ ПО для решения задачи

В данной задаче веб-приложение обеспечивает просмотр большого числа картографических слоев, накладываемых на базовую карту в качестве информа-

ции, передаваемой диспетчеру или оператору. В качестве базовой карты могут выступать общегеографические карты, космические снимки, рельеф.

Системы линейных координат — ключевой компонент приложений для транзитных перевозок, способствующий такой деятельности как: планирование и анализ маршрутов; автоматическое отслеживание положения транспортных средств; реестр автобусных остановок; управление железнодорожными объектами; обслуживание дорог, линий связи и сигналов; составление отчетов о происшествиях и их анализ; транспортное планирование и другим видам деятельности [6].

Для мониторинга маршрута транспорта существует множество программ. Из них наиболее известны: *Ставтрэк Онлайн, ArcGIS, Wialon, Fort Monitor, СКАУТ Онлайн, ГЛОНАССSoft.*

Ставтрэк Онлайн – программное обеспечение, с помощью которого можно осуществлять ГЛОНАСС/GPS мониторинг транспорта. Сервис позволяет узнавать место работы ТС, текущий и прошлые маршруты перемещения, полную информацию по топливу, а также информацию о качестве вождения. Собранные данные на сервере онлайн-мониторинга конвертируются, в результате чего информация выводится в виде таблиц и графиков.

Система *ArcGIS* позволяет собирать, организовывать и анализировать географическую информацию. Совместная обработка и обмен данными осуществляется с помощью поддержки серверов и облачных платформ. ArcMap – приложение семейства программных продуктов ArcGIS Desktop, используемое для всех картографических задач, в том числе создание и анализ карт, а также редактирование данных [7].

Wialon – приложение, упрощающее работу с маршрутами. Контролировать прохождение маршрута можно в реальном времени, реагируя на отклонения и незапланированные остановки. У приложения есть возможность получения уведомлений при отклонении от маршрута. При планировании маршрута в данном приложении можно использовать: создание маршрутов вручную или из геозоны; несколько источников адресной информации из геозон; отправку маршрута из контрольных точек с помощью команды; автоматическое создание рейсов по расписанию; автоматическое назначение объектов на рейс. Для анализа информации в приложении могут быть использованы: история маршрута с данными по опозданиям; отчетность по рейсам для объекта и маршрута; по-

строение и трассировка треков; расчет пробега по платным дорогам; отчет по выполненным заявкам; треки, маркеры и геозоны в отчетах [8].

Программная платформа *Fort Monitor* в реальном времени отслеживает движение ТС, получает информацию со всех установленных на ТС датчиков, оповещает о нарушениях скорости и критических событиях, анализирует поступившие данные путем построения графиков. Кроме того, существует возможность контролировать сроки прохождения технического обслуживания ТС, идентифицировать водителей и проводить анализ качества вождения.

СКАУТ Онлайн – программа мониторинга, позволяющая осуществлять поиск по любым данным (полям) объекта, узнать текущее местоположение и состояние объекта, увидеть историю движения объекта. Интерфейс приложения позволяет получать уведомления, просматривая журнал событий, строить отчеты полученной информации в PDF и Excel форматах, просматривать информацию о расходе топлива и о сотрудниках.

ГЛОНАССSoft – система, осуществляющая мониторинг транспортных средств в реальном времени, отслеживает изменения определенных параметров объектов, позволяет получать уведомления об активности объектов, получать информацию о состоянии датчиков объекта, контролировать уровень расхода топлива, формировать отчеты, интегрировать данные в существующие системы. Кроме того, на платформе предоставляется выбор картографических сервисов (OpenStreetMap, Yandex Maps, Google Maps, MapQuest, Bing).

Результаты анализа существующего ПО представлены в таблице 1.

Таблица 1

Анализ возможностей ПО

Возможности	Ставтрэк	СКАУТ	Wialon	ArcGIS	Fort Monitor	ГЛОНАССSoft
Контроль местоположения и истории движения	+	+	+	+	+	+
Контроль скорости объекта	+	+	+	+	+	+
Контроль расхода топлива	+	+	+	-	-	+
Формирование табличных и графических отчетов	-	+	-	-	+	+
Автоматическая генерализация запланированных маршрутов, событий, уведомлений и их отправка	+	+	+	+	+	+

Получение информации о работе механизмов ТС	+	-	+	-	+	-

Выявление информации для решения задачи

На транспортном средстве установлено оборудование, которое передает информацию на сервер. Разрабатываемое ПО должно анализировать эту информацию и выводить результат на экран диспетчеру. Обмен информацией о текущем состоянии транспортного средства происходит на протяжении всего маршрута. Если передаваемые показатели отклоняются от нормы, информация должна состоять из предупреждения и текущего местоположения транспортного средства. Диспетчер выходит на связь с водителем в случае отклонения транспорта от маршрута. Так план работы транспорта может быть скорректирован в зависимости от причины отклонения. На рисунке 1 рассматривается процесс мониторинга движения автотранспорта. Более детально процесс мониторинга рассматривается на рисунке 2.

Рис. 1. Алгоритм контроля маршрутного плана

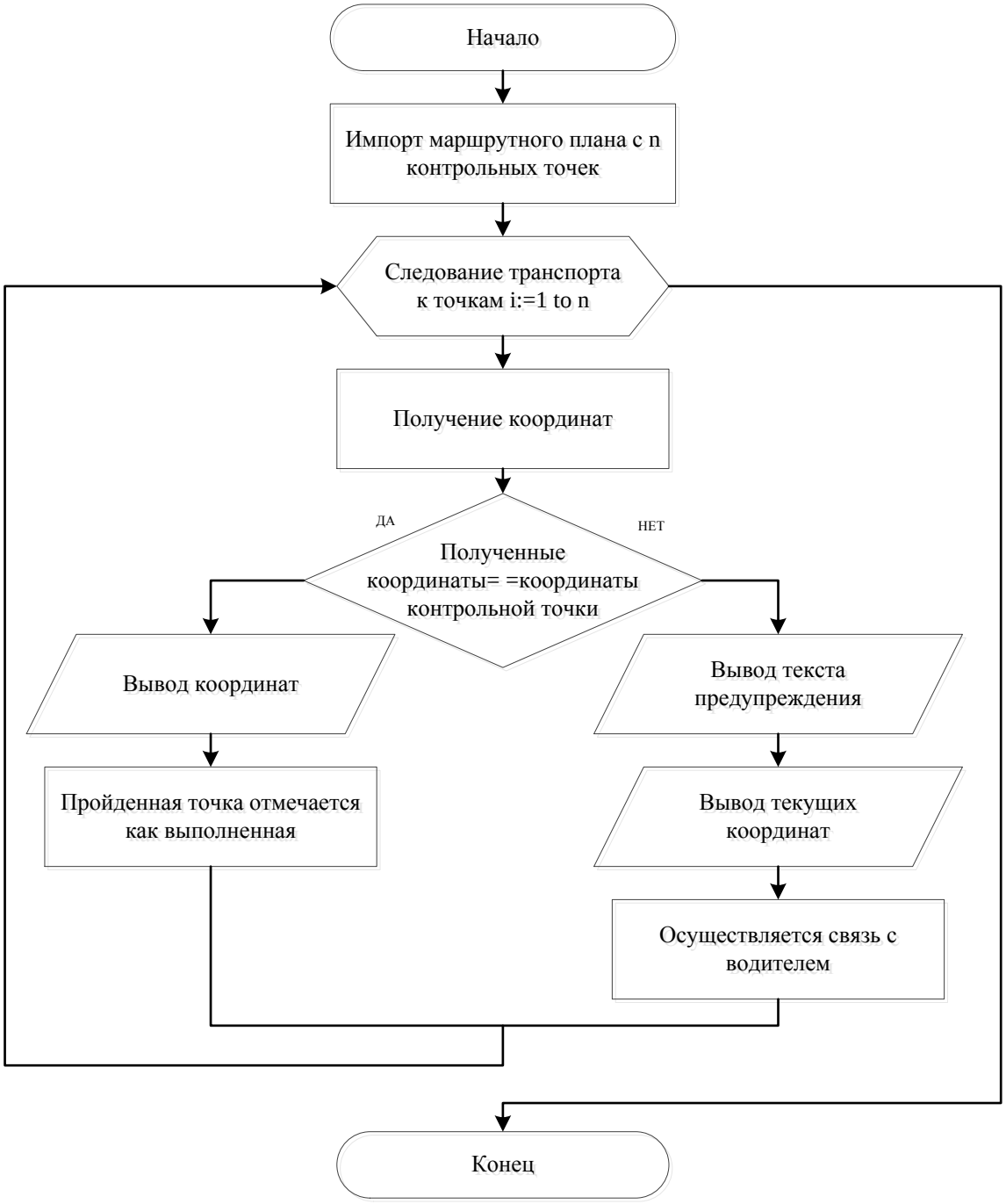


Рис. 2. Алгоритм контроля маршрута следования

Варианты решения задачи

При проектировании вариантов решения задачи следует рассмотреть несколько алгоритмов реализации процессов построения линейного объекта из точек маршрута, сравнения координат пройденных точек с координатами маршрута, вывода текста предупреждения при условиях отклонения. При автоматизации этих процессов с помощью скрипта на языке программирования, алгоритм скрипта должен учитывать такие определенные условия, как количество

отклоняющихся точек от запланированного маршрута. От этого зависит чувствительность алгоритма. При чувствительном алгоритме процесс сравнения координат состоит из условия: если 1 точка не соответствует координатам запланированного маршрута, то необходимо вывести текстовое предупреждение о несоответствии и текущие координаты (рисунок 3). При несущественных отклонениях от маршрута, таких как объезд препятствий, данный алгоритм может присылать текстовые предупреждения, и может возникнуть перегруженность ненужной информацией. Это является недостатком сильной чувствительности алгоритма. Чтобы устранить этот недостаток, чувствительность алгоритма можно понизить до 2-3 точек отклонения от маршрута. В этом случае текстовые предупреждения об отклонении будут выводиться только если координаты трех идущих друг за другом точек прохождения не будут совпадать с координатами маршрута. Альтернативой такому алгоритму является алгоритм, в котором после построения линии по заданным точкам маршрута строится буфер, имеющий ширину больше, чем ширина линии дороги. В данном алгоритме чувствительность зависит от разницы в ширине дороги и буфера, так как сравнение в этом случае будет проводиться не с координатами заданного пути, а с координатами буфера. При этом не следует строить буфер намного шире дороги, так как чувствительность алгоритма сильно понизится, текстовые предупреждения будут отправляться поздно и возможность быстрого реагирования на отклонения от пути следования будет исключена.

Алгоритм, представленный на рисунке 3, использует массив b для получения координат точек маршрута, затем строит линию дороги шириной L на основе полученных данных. Пока транспортное средство движется, координаты пройденных точек считываются в массив a, который может понадобиться при построении отчета о пройденном маршруте в дальнейшем. Так же в цикле идет сравнение координаты пройденной точки с координатами точек построенного линейного объекта.

Рис. 3. Чувствительный алгоритм

Алгоритм на рисунке 4 осложнен использованием дополнительного массива *c*. При сравнении координат пройденных точек в цикле каждая несовпадающая с маршрутом точка попадает в этот массив. После выполняется проверка количества элементов в этом массиве. Если количество больше или равно трем, то массив *c* должен обнулиться, после чего выводится предупреждение об отклонении.

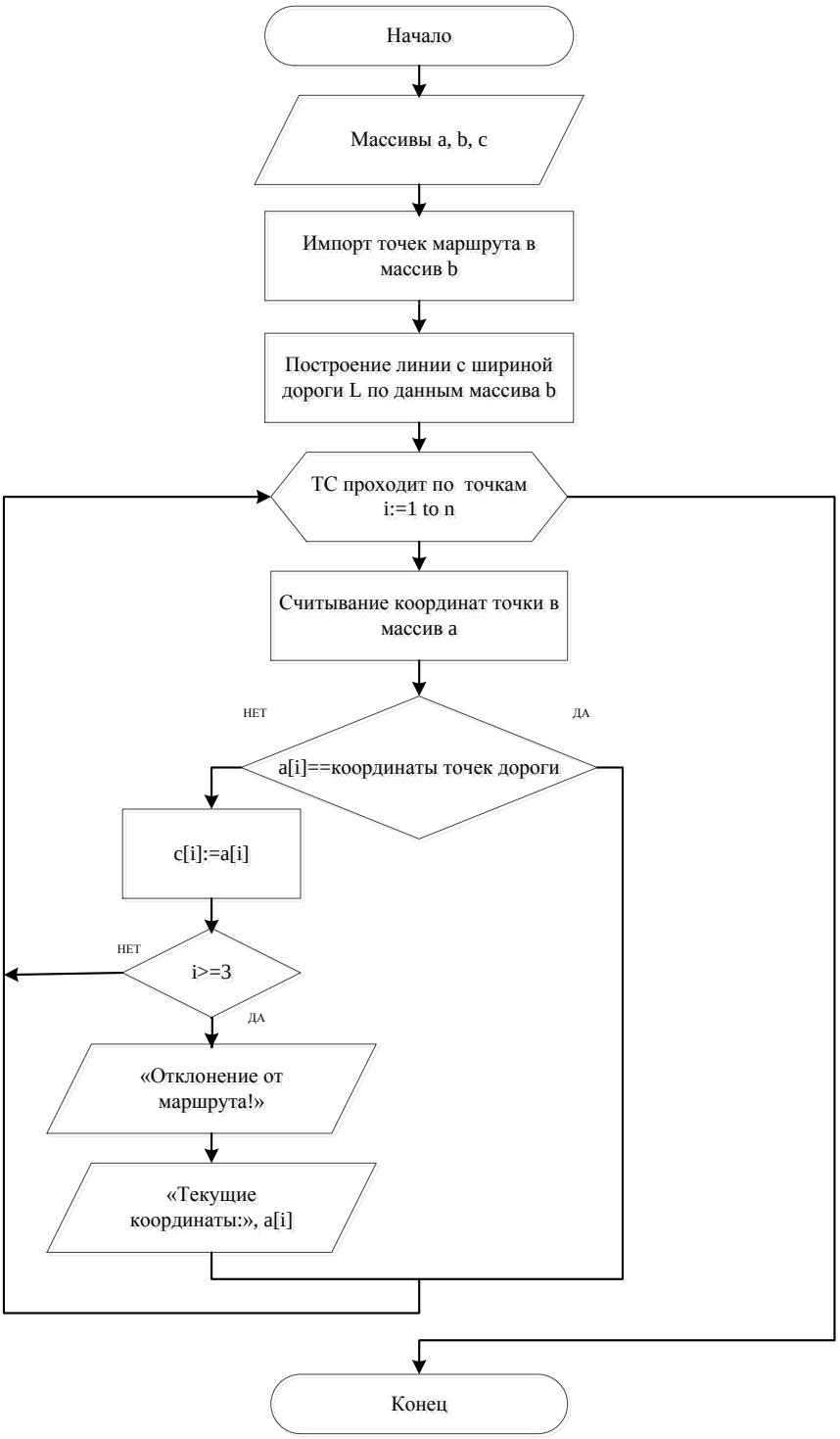


Рис. 4. Менее чувствительный алгоритм

Алгоритм на рисунке 5 вместо дополнительного массива *c* использует построенный буфер с толщиной *m* вокруг линейного объекта. При реализации такого алгоритма в приложении ArcMap инструмент построения линии по данным точек строит линию с шириной 1. Для возможности автоматизации процесса построения маршрута и буфера в Мастере построения моделей при ис-

пользовании инструмента, создающего буфер, нужно указать ширину буфера, которая будет учитывать ширину дороги ($m>L$).

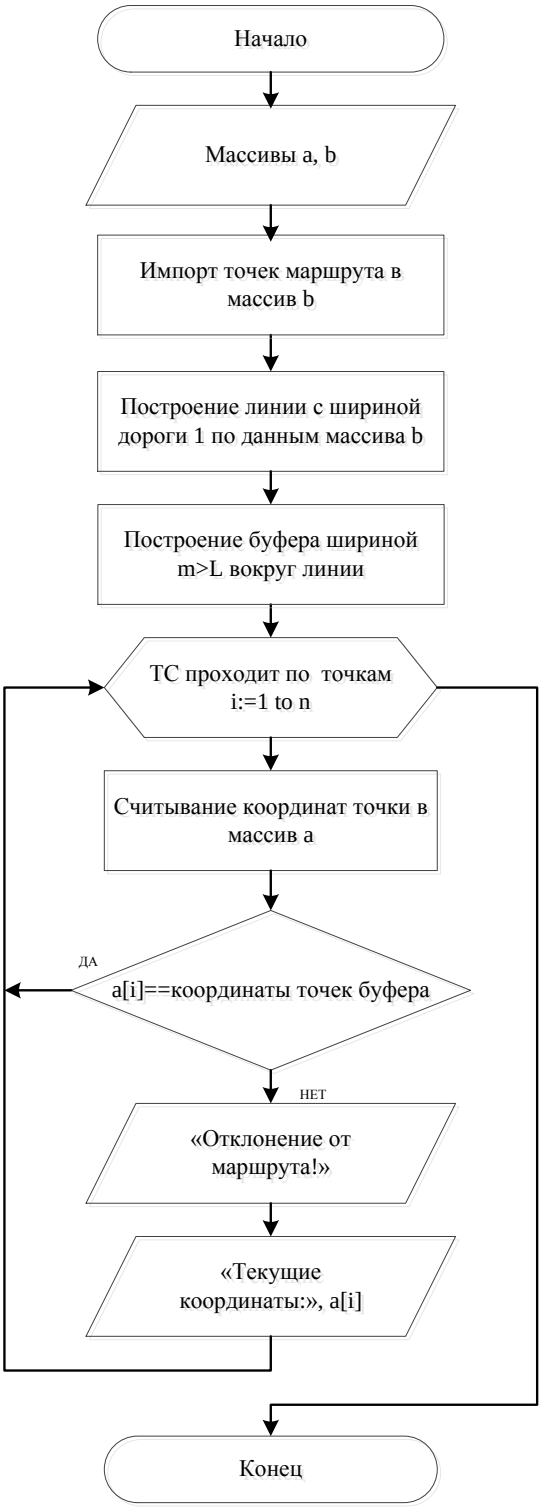


Рис. 5. Алгоритм с использованием буфера

Если смоделировать движение транспорта по этому алгоритму, можно увидеть 3 ситуации (рисунок 6). В первом случае диспетчеру видны точки прохождения по маршруту, которые также могут отображаться в таблице. Координ-

наты этих точек сравниваются с диапазоном координат построенного полигонального объекта (буферной зоны вокруг дороги). Во втором случае от маршрута отклонилась сначала 1 точка, координаты следующей точки совпали с буфером, затем отклонились 2 точки подряд. При этом сообщения диспетчеру не приходят с учетом чувствительности алгоритма. В третьем случае, на рисунке видны 3 точки, отклонившиеся от буферной зоны. В такой ситуации диспетчеру приходит сообщение об отклонении от маршрута. Осуществив связь с водителем, после выяснения причины отклонения диспетчер может передать водителю скорректированный маршрут и продолжить наблюдение за выполнением.

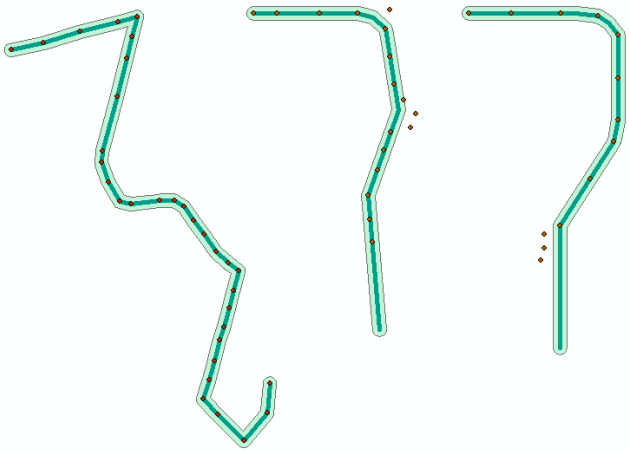


Рис. 6. Смоделированные ситуации

В процессе следования транспорта по определенному маршруту может возникнуть ряд различных затрудняющих путь ситуаций. Если транспортное средство, например, попадает в пробку, возникает потребность в алгоритме, который учитывает непрерывность получения данных. Используемое программное обеспечение может давать возможность просматривать в этом случае отображающиеся данные, которые поступают непрерывно, в таблице. В этой таблице также может отображаться и время получения пройденных координат. При появлении задержки диспетчер связывается с водителем для установления причины задержки. Возможно, водитель проинформирует диспетчера о причине как только попадет в пробку. Чтобы скорректировать маршрут, учитывающий пробки на пути, понадобится информация о пробках в районах, связанных с маршрутом, а также правильная обработка этой информации при построении.

Если такая информация у диспетчера окажется перед началом мониторинга следования, попадания в пробку можно будет избежать путем передачи возможных изменений в маршруте. Таким образом, программному обеспечению для мониторинга не помешает функция анализа запланированного маршрута с учетом данных о пробках. Кроме того, анализ маршрута может происходить и в процессе мониторинга следования. Если результаты анализа будут известны диспетчеру так же как и данные о пройденных координатах, он сможет оповещать водителя о пробке на определенном участке маршрута. Эта информация помогла бы выбрать диспетчеру или водителю возможное отклонение от маршрута. Алгоритм анализа запланированного маршрута начинает свою работу с получения маршрута и данных о пробках. По полученной информации о пробках строятся полигоны, после чего идет сравнение координат маршрута с координатами этих полигонов (рисунок 7).

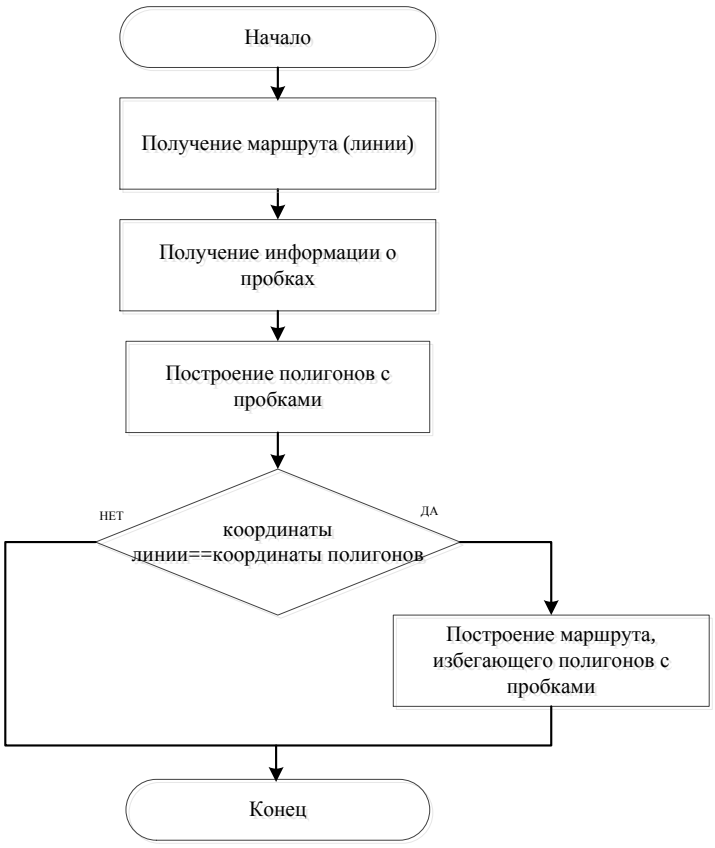


Рис. 7. Алгоритм анализа

Если смоделировать движение по этому алгоритму, можно увидеть 2 ситуации. В первом случае маршрут не пересекается с обнаруженным полигоном

пробки (рисунок 8). Во втором случае в маршруте встречается полигон пробки (рисунок 9). При обнаружении совпадений маршрута с пробкой строится аналогичный маршрут, не пересекающийся с найденным полигоном.

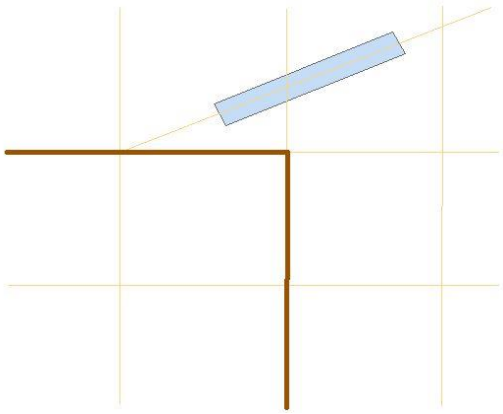


Рис. 8. Смоделированная ситуация

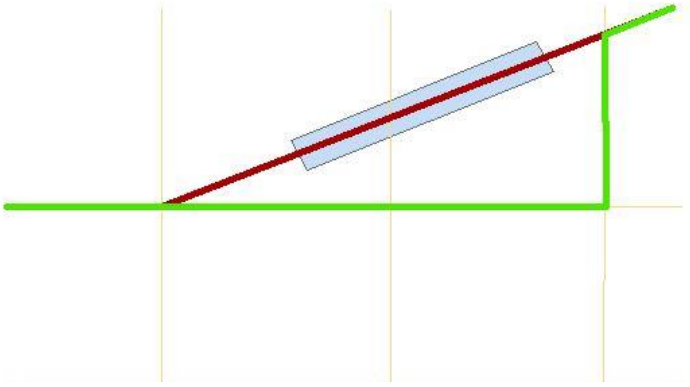


Рис. 9. Смоделированная ситуация

Помимо пробок на пути транспорта могут возникнуть и проблемы, связанные с погодными условиями. Если такой проблемой будет сильная заснеженность дорог, транспортное средство может значительно замедлить передвижение или вовсе застрять. Эту проблему может решить алгоритм анализа маршрута. В данном случае вместо информации о пробках алгоритм будет учитывать данные об осадках на дороге, а также понадобится информация об очищенных дорогах для выбора возможных маршрутов. При правильной обработке такой информации можно оперативно справиться с данным препятствием.

Не исключена также возможность ремонтных работ на дорогах. По этой причине некоторые пути проезда могут быть перекрыты. В такой ситуации лучше анализировать маршрут с учетом информации о ремонтных работах. Ес-

ли в запланированном маршруте в процессе анализа будут выявлены участки ремонта, понадобится построить аналогичный маршрут с теми же точками назначения, но без участков ремонта. Полученный результат можно будет использовать при мониторинге следования: если диспетчер, связавшись с водителем, узнает эту причину, то передаст результат водителю для дальнейшего передвижения. Возможно и такое решение, в котором водителю и диспетчеру уже будет известен результат анализа. При этом, столкнувшись с этим препятствием, водитель уже будет знать правильный маршрут, а диспетчеру будет видно, что транспортное средство перешло на альтернативный маршрут.

Транспортное средство может также перевозить различные грузы, возможно товары. В таких случаях могут возникать попытки нападения на водителя ТС. Это может зависеть от уровня преступности в районах или ряда других показателей той местности, через которую проходит маршрут. В целях предотвращения таких ситуаций транспортное средство не должно делать никаких остановок в этих местах. В данном случае программное обеспечение просто отображает полигоны неблагоприятных мест для остановок, чтобы диспетчер смог предупредить водителя о наличии этих районов в маршруте.

Заключение

Одним из способов повышения эффективности мониторинга следования ТС по указанному маршруту является использование в качестве результатов анализа маршрута сразу несколько типов полигонов. В данном случае каждый тип возможных препятствий на пути транспорта может отображаться в виде полигона с единым цветом. При этом алгоритм анализа будет искать в маршруте наличие всех таких полигонов, и строить аналогичный маршрут, избегающий полигоны, если их найдет. Таким образом, программное обеспечение, позволяющее анализировать маршрут с учетом информации о пробках, количестве осадков, происшествиях, ремонтных работах, может сделать процесс мониторинга движения эффективным.

СПИСОК ЛИТЕРАТУРЫ

1. Иванов, В.В. Государственное и муниципальное управление с использованием информационных технологий / А.Н. Коробова. М.: ИНФРАМ, 2014. 383 с.
2. Быховский, М.А. Развитие телекоммуникаций. На пути к информационному обществу. Развитие радиолокационных систем: Учебное пособие для вузов / М.: Гор. линия-Телеком, 2015. 402 с.
3. Пласкова, Н.С. Финансовый анализ деятельности организации: учебник / М.: Вузовский учебник: ИНФРА-М, 2017. 368 с.
4. Сакалема Д.Ж. Подвижная радиосвязь / Под ред. О.И. Шелухина. М.: Гор. линия-Телеком, 2015. 512 с.
5. Федотова, Е.Л. Прикладные информационные технологии: Учебное пособие / Е.М. Портнов. М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2015. 336 с.
6. Сайт *ArcGIS* компании *ESRI*. URL: https://desktop.arcgis.com/ru/arcmap/10.3/guide-books/linear-referencing/linear-referencing-sample-applications.htm (дата обращения: 05.11.2020)
7. Сайт пошагового руководства выполнения действий в *ArcGIS* компании *ESRI*. URL: https://learn.arcgis.com/ru/ (дата обращения: 15.11.2020)
8. Сайт Wialon: URL: https://wialon.ru/kontrol-marshrutov (дата обращения: 21.11.2020)
9. Мавлютов А.Р., Атнабаев А.Ф., Мавлютов А.Р. МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ДЛЯ АВТОМАТИЧЕСКОГО РАСЧЕТА КОЭФФИЦИЕНТА ЗАТРАТ НА ПОЕЗДКИ // Вестник науки и образования. 2019. № 2-2 (56). С. 9-13.
10. Мавлютов А.Р., Атнабаев А.Ф. ВНЕДРЕНИЕ ГЕОИНФОРМАЦИОННЫХ СИСТЕМ НА ПРЕДПРИЯТИЕ // Modern Science. 2020. № 1-2. С. 298-303.

УДК 004

Н. А. ГАЛИМОВА
nelligalimova77@gmail.com
Науч. руководов. – д-р техн. наук, проф. О. И. ХРИСТОДУЛО

Уфимский государственный авиационный технический университет

МОНИТОРИНГ И АНАЛИЗ ДЕМОГРАФИЧЕСКИХ И СОЦИАЛЬНО-ЭКОНОМИЧЕСКИХ ПОКАЗАТЕЛЕЙ В РЕСПУБЛИКЕ БАШКОРТОСТАН С ИСПОЛЬЗОВАНИЕМ ГЕОИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Аннотация. В статье приведена необходимость и актуальность разработки геоинформационной системы (ГИС) мониторинга и анализа демографических и социально-экономических показателей в Республике Башкортостан. Представлена архитектура, алгоритм работы и функционал ГИС.
***Ключевые слова*:** геоинформационная система; ГИС; демографические показатели; социально-экономические показатели.

Введение

На сегодняшний день общей тенденцией демографических процессов в Республике Башкортостан и по всей России в течение последних нескольких лет является сокращение численности населения [1].

Основные причины падения численности населения – это уменьшение числа рождаемости [2] и увеличение миграционного оттока населения.

Проблема повышения численности населения в Республике Башкортостан является важной и поэтому ГИС для мониторинга и анализа демографических и социально-экономических показателей является актуальной. Система позволяет оценить МО на привлекательность для жизни людей, поддерживать развитие территорий МО и улучшать уровень жизни в тех МО, которые имеют низкие показатели, с целью привлечения мигрантов в Республику Башкортостан, а также удержания текущего населения.

Актуальность

Анализ существующих ГИС и ИС (информационных систем) [6, 7] в предметной области демографического и социально-экономического развития в Республике Башкортостан позволил сделать выводы об уникальности создава-

емой системы. Систем, подобных той, что описывается в данной статье, нет по Республике Башкортостан. Также нет систем по Российской Федерации в открытом доступе, позволяющих анализировать статистические демографические, миграционные, социально-экономические данные с целью определения уровня привлекательности территорий для миграционного переселения.

Таким образом, создание ГИС мониторинга и анализа демографических и социально-экономических показателей в Республике Башкортостан является актуальной задачей, система позволит: упростить получение информации по МО в Республике Башкортостан, благодаря интерактивной карте со всплывающими окнами, содержащими статистические данные для каждого МО; оценить данные во временном промежутке и сделать выводы о тенденции развития демографического и социально-экономического развития по гистограммам; редактировать существующие и вносить новые данные в базу данных из интерфейса пользователя; определить наиболее привлекательные для жизни территории.

Разработка ГИС мониторинга и анализа демографических и социально-экономических показателей в Республике Башкортостан

Целью создания ГИС мониторинга и анализа демографических и социально-экономических показателей в Республике Башкортостан является повышение эффективности процессов мониторинга, анализа, редактирования и внесения демографических и социально-экономических показателей в Республике Башкортостан, что позволит упростить работу потенциальных пользователей системы – сотрудников Минэкономразвития Республики Башкортостан. Для достижения данной цели необходимо решить следующие задачи:

– визуализация границ и муниципальных образований Республики Башкортостан на карте;

– поиск МО на карте Республики Башкортостан;

– отображение атрибутивных данных по МО Республики Башкортостан;

– отображение динамики атрибутивных данных по демографическим и социально-экономическим показателям Республики Башкортостан в виде гистограмм;

– редактирование и добавление новых атрибутивных данных в БД ГИС для мониторинга и анализа демографических и социально-экономических показателей в Республике Башкортостан;

– районирование территории Республики Башкортостан по значениям коэффициента привлекательности.

ГИС мониторинга и анализа демографических и социально-экономических показателей в Республике Башкортостан имеет клиент-серверную архитектуру (Рис. 1). Со стороны клиента к ГИС обращаются потенциальные пользователи: это специалисты Минэкономразвития Республики Башкортостан (Министерство экономического развития и инвестиционной политики Республики Башкортостан). Клиенты получают доступ к системе через запрос к веб-серверу по протоколу HTTP, веб-сервер, обращаясь к базе данных (БД), возвращает пользователю по сети запрашиваемую веб-страницу.

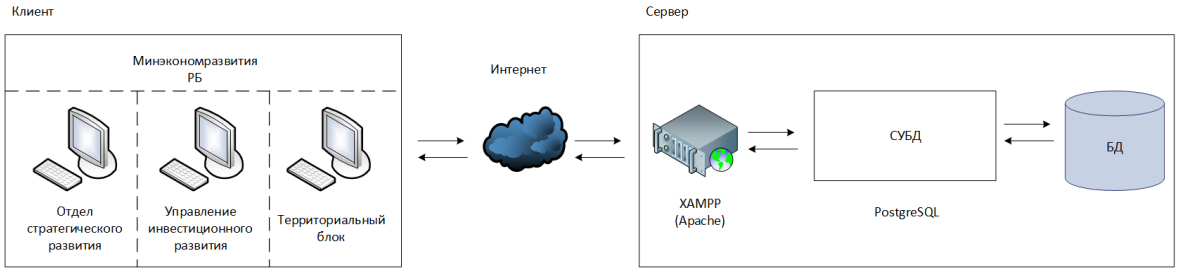


Рис. 1. Архитектура ГИС мониторинга и анализа демографических и социально-экономических показателей в Республике Башкортостан

Далее рассмотрим алгоритм работы ГИС мониторинга и анализа демографических и социально-экономических показателей в Республике Башкортостан (Рис. 2). Работа с системой начинается с загрузки интерфейса веб-страницы, далее пользователю необходимо сделать выбор следующего действия: «Работа отдельно с МО», чтоб в дальнейшем работать с атрибутивными данными: просмотр или редактирование, «Открыть панель для формирования

графиков», «Открыть панель для районирования территории», «Открыть панель для поиска МО на карте». Блок «Работа отдельно с МО» отображен на рис. 3.

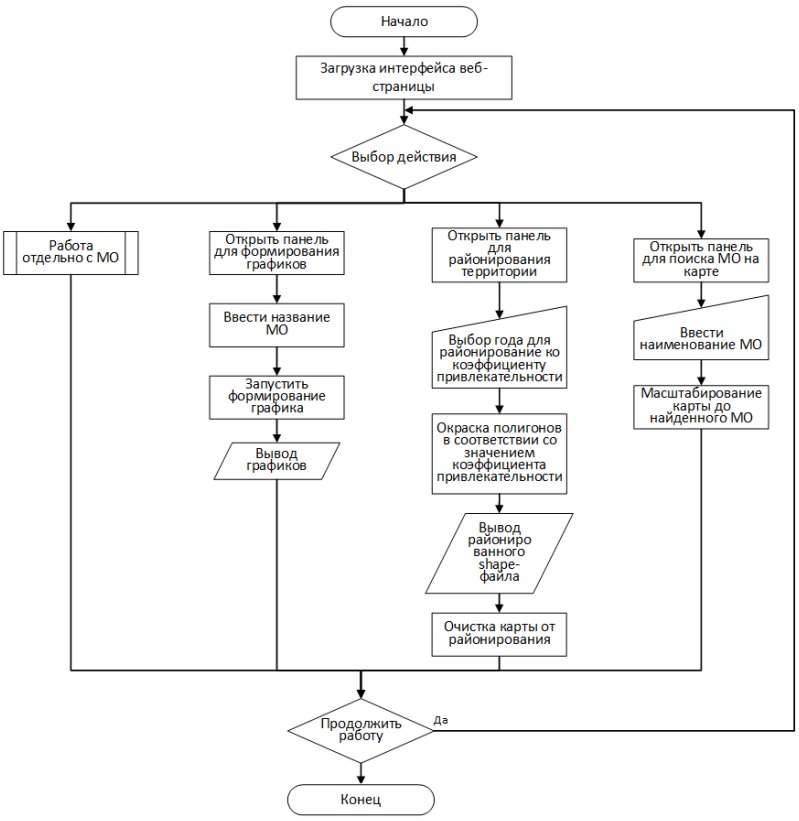


Рис. 2. Алгоритм функционирования ГИС мониторинга и анализа демографических и социально-экономических показателей в Республике Башкортостан

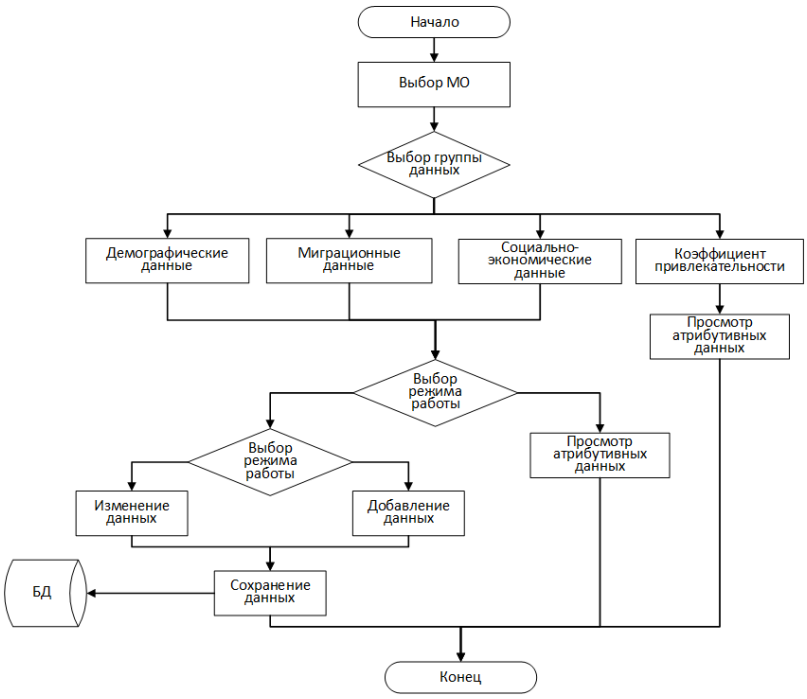


Рис. 3. Алгоритм «Работа отдельно с МО»

Рассмотрим некоторые функции ГИС мониторинга и анализа демографических и социально-экономических показателей в Республике Башкортостан.

Функция отображение атрибутивных данных [8] по каждому МО Республики Башкортостан отображена на рис. 4. Для отображения атрибутивных дан-

ных пользователю необходимо выбрать МО. По щелчку на карту открывается всплывающее окно, содержащее четыре вида вкладок: демографические данные, миграционные данные, социально-экономические данные, коэффициент привлекательности. В каждой вкладке имеется два режима работы с данными: просмотр и редактирование. Режим работы «Редактирование» дает возможность вносить изменения или создавать новые данные в БД с пользовательского интерфейса.

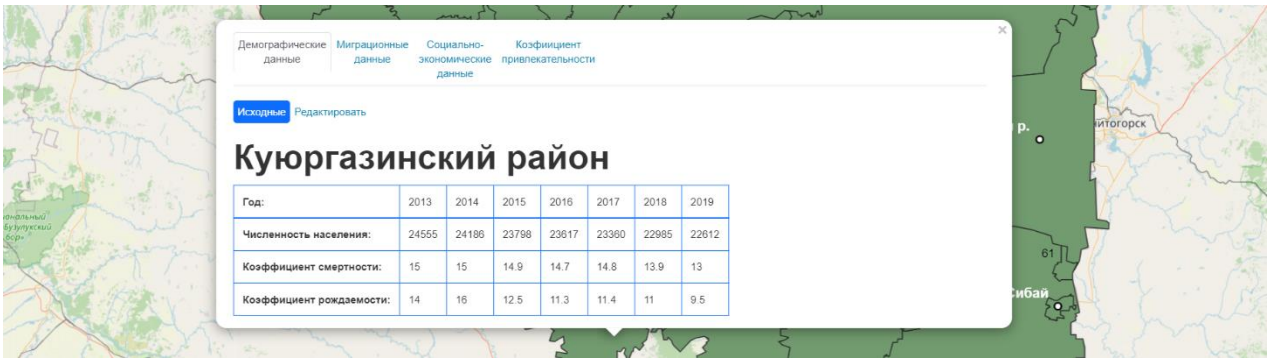


Рис. 4. Отображение атрибутивных данных по демографическим показателям для Куюргазинского района за 2013-2019 года

Районирование – это деление территории Республики Башкортостан посредством окрашивания полигонов в цвета, соответствующие кластерам коэффициентов привлекательности [4, 5]. По результатам районирования можно определить как МО отделены друг от друга, определить их коэффициенты привлекательности. Таким образом функция районирования дает возможность выполнять оценку работы органов местного самоуправления и проводить сценарные прогнозы для увеличения привлекательности территории МО для иммиграции в них. На рис. 5 отображена функция районирования территории Республике Башкортостан по коэффициенту привлекательности. В 2013 году толь-

ко Стерлитамак имеет набольшее значение коэффициента привлекательности и попадает в первый (зеленый) кластер МО.

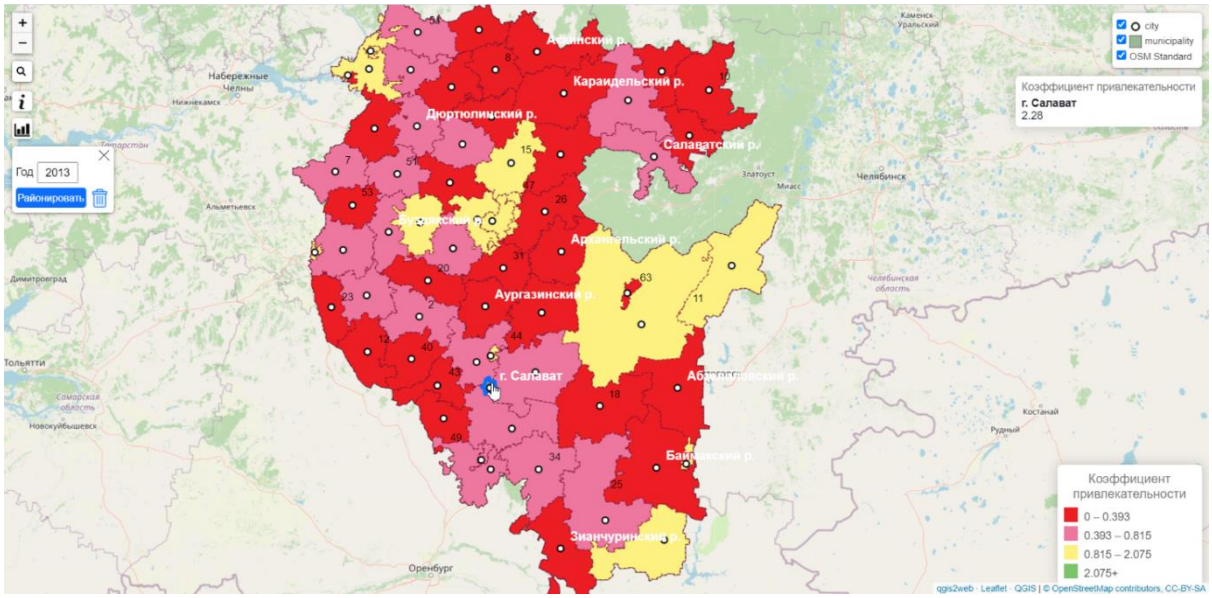


Рис. 5. Районирование территории Республики Башкортостан по коэффициенту привлекательности за 2013 год

Для функции построения графиков (Рис. 6) имеется панель, которая раскрывается по клику на пиктограмму инструмента. Перед тем как запустить построение графика необходимо выбрать МО и или демографический, или миграционный, или социально экономический показатель. Перечень показателей включает: численность населения, коэффициент смертности, коэффициент рождаемости, численность выбывших, численность прибывших, сальдо миграции, среднесписочная численность занятых в экономике, среднемесячная заработная плата, выбросы в атмосферу (загрязняющих веществ, отходящих от стационарных источников), объем инвестиций в основной капитал, объем отгруженной продукции, коэффициент привлекательности.

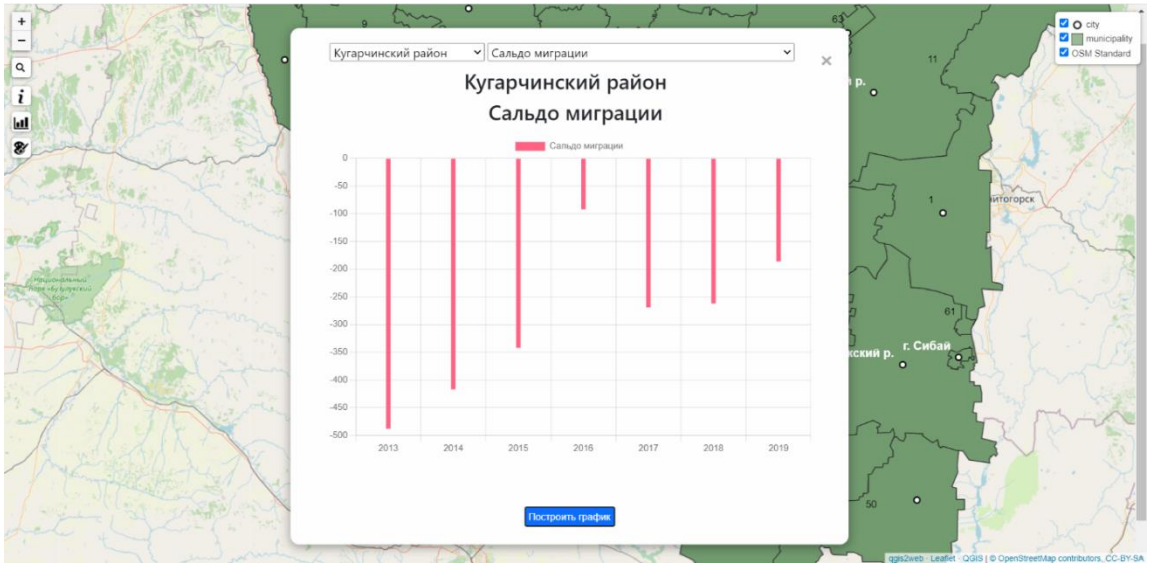


Рис. 6. График по показателю сальдо миграции для города Кугарчинский район за 2013-2019 года

Заключение

В данной статье была описана архитектура и алгоритмы работы ГИС мониторинга и анализа демографических и социально-экономических показателей в Республике Башкортостан, а также частично рассмотрен ее функционал. Дальнейшая работа над ГИС мониторинга и анализа демографических и социально-экономических показателей в Республике Башкортостан будет направлена на оптимизацию работы программы, расширение функционала системы и выполнение исследований, посвященных прогнозированию уровня миграции, что позволит повысить качество принятие решений в органах, ответственных за миграционное развитие Республики Башкортостан.

СПИСОК ЛИТЕРАТУРЫ

1. [Электронный ресурс] // Территориальный орган Федеральной службы государственной статистики по Республике Башкортостан URL: https://bashstat.gks.ru/ (Дата обращения: 21.06.2019);
2. Зайцева Н.В. и др Методические подходы к прогнозированию суммарного коэффициента рождаемости на основе исследования закономерностей очередности рождений / Н.В. Зайцева, Д.А. Кирьянов, С.В. Бабина, Л.А. Сичихина / Проблемы социальной гигиены, здравоохранения и истории медицины. 2020. Т. 28, №4. С. 548-554.
3. Дегтярева А.Н., Кузнецовой А.Р., Ахметовой Г.Ф. Республика Башкортостан. Демографический доклад // Институт стратегических исследований Республики Башкортостан. 2020. №4. 252 с.
4. Ахметзянова М.И., Атнабаева А.Р. Исследование привлекательности муниципальных районов и городов Республики Башкортостан с применением компонентного и кластерного анализов // Вестник Евразийской науки. 2020. №5.

5. Атнабаева А. Р., Ахметзянова М. И. Концепция агент-ориентированной модели миграционных потоков в Республике Башкортостан // Проблемы функционирования и развития территориальных социально-экономических систем: материалы 13-й всероссийская научной интернет-конференции –Уфа: ИСЭИ УФИЦ РАН, 2019. С.58-63.
6. Павлов, С. В. Разработка метода объединения данных из различных информационных систем в единую информационную систему Минэкологии РБ / С. В. Павлов, О. И. Христодуло // Вестник Уфимского государственного авиационного технического университета. 2011. Т. 15. № 2 (42). С. 3-7.
7. Павлов, С. В. Геоинформационная система для управления водными ресурсами на территориальном уровне (на примере Республики Башкортостан) / С. В. Павлов, С. А. Абрамов, Р. А. Шкундина, О. И. Христодуло // Геоинформатика. 2008. № 4. С. 14-20.
8. Христодуло О. И. Совместное описание пространственных и атрибутивных данных на основе многомерных информационных объектов // Программные продукты и системы. 2011. №3. С. 11.

УДК 332.14:004.9

Э. Р. ГАЛИМЗЯНОВА
galimzyanova02@inbox.ru

Уфимский государственный авиационный технический университет

ИСПОЛЬЗОВАНИЕ WEB-КАРТОГРАФИИ В ИНТЕРНЕТЕ

Аннотация. В последнее время Internet-технологии все более стремительно развиваются и могут предоставлять пользователям различные виды информации, в том числе и пространственную. Доставкой этой пространственной информации занимается такая область технологий как web-картография, которая в свою очередь является частью геоинформационных систем. Web-картография выполняет безусловно важные для нас пользователей задачи. Она визуализирует пространственные данные, делает представление информации более понятным для понимания, облегчает поиск и сортировку данных.
Ключевые слова: web-картография; интернет; технологии; пространственные данные; информация; геоинформационные системы.

"Рождение" web-картографии

Многие пользователи интернета думают, что вся история с представлением пространственных данных началась с продуктов компании Google, но в реальности же зачинателем этой эры картографических web-приложений был web-сервис Xerox PARC Mar Viewer, выпущенный в 1993 году. Данный сервис позволял пользователям отправлять запросы из браузера к серверу и получать нужные им части карт в формате GIF. Именно эта функциональная концепция стала основополагающей большинства других, более поздних версий web-ГИС.

Популяризация web-ГИС

Большая часть сервисов в начале становления web-картографии отличались своей локальностью и были направлены на узкую область тем изучения, что сужало их группу потенциальных пользователей. От данных недостатков надо было избавляться, и этим занялись британские разработчики, которые в 1998 году запустили сайт www.streetmap.co.uk. Выпущенный сервис использовал простейшую топографическую информацию, но в то же время охватывал всю территорию Великобритании. Из-за этого данный сервис был хорошо принят людьми и использовался большим количеством пользователей, т.к. они

могли без особых усилий определить местоположение нужных им объектов. Запуск этого сайта стал первым шагом к популяризации web-ГИС.

Важным моментом в истории развития web-картографии стал запуск двух картографических сервисов – Google-Maps и Google-Earth (2005 год). Данные сервисы можно смело назвать масштабными или глобальными, т.к. ничто из того, что выпускалось ранее, не могло похвастаться настолько "широкой" географией.

Следующие года показывали и показывают какое большое внимание уделяется к web-картографии и ее способностям, т.к. число сервисов, использующих web-технологии, увеличивается с каждым новым годом.

Заключение

Стремительное развитие и огромное разнообразие современных картографических web-систем является показателем все более массового использования электронных картографических данных в различных предметных областях. Именно благодаря этому, вероятнее всего, мы станем свидетелями дальнейшего развития и процветания географических информационных систем.

СПИСОК ЛИТЕРАТУРЫ

1. Абдуллин Р.К., Пономарчук А.И. Технологии интернет – картографирования, 2020. – Ст. 136.
2. Быков А.В., Пьянков С.В. Web – картографирование, 2015. – Ст. 110.
3. Лебедев П.П. Картография, 2017. – Ст. 157.
4. Воробьев А.В., Пилипенко В.А., Еникеев Т.А., Воробьева Г.Р., Христодуло О.И. Система динамической визуализации геомагнитных возмущений по данным наземных магнитных станций Научная визуализация, 2021. Т. 13. № 1. С. 162-176.
5. Воробьев А.В., Пилипенко В.А., Еникеев Т.А., Воробьева Г.Р. Геоинформационная система для анализа динамики экстремальных геомагнитных возмущений по данным наблюдений наземных станций Компьютерная оптика, 2020. Т. 44. № 5. С. 782-790.
6. Воробьев А.В., Пилипенко В.А., Решетников А.Г., Воробьева Г.Р., Белов М.Д. Веб-ориентированная визуализация геофизических параметров в области аврорального овала Научная визуализация, 2020. Т. 12. № 3. С. 108-118.
7. Воробьев А.В., Воробьева Г.Р. Визуализация геомагнитных вариаций в частотно-временной области информационного сигнала Научная визуализация, 2019. Т. 11. № 2. С. 143-155
8. Воробьев А.В., Воробьева Г.Р. Подход к оценке относительной информационной эффективности магнитных обсерваторий сети intermagnet Геомагнетизм и аэрономия, 2018. Т. 58. № 5. С. 648-652.
9. Воробьев А.В., Воробьева Г.Р. Веб-ориентированная 2d/3d-визуализация параметров геомагнитного поля и его вариаций Научная визуализация, 2017. Т. 9. № 2. С. 94-101.

10. Воробьев А.В., Пилипенко В.А., Сахаров Я.А., Селиванов В.Н. Статистические взаимосвязи вариаций геомагнитного поля, аврорального электроджета и геоиндуцированных токов Солнечно-земная физика, 2019. Т. 5. № 1. С. 48-58.

УДК 004

Ф. А. МАГЕР
Lafenix123@yandex.ru
Науч. руководитель – ст. преп. О. С. САУБАНОВ

Уфимский государственный авиационный технический университет

ПРИМЕНЕНИЕ ГЕОИНФОРМАЦИОННЫХ СИСТЕМ ДЛЯ ИНФОРМАЦИОННОЙ ПОДДЕРЖКИ ДЕЯТЕЛЬНОСТИ РАБОТНИКОВ ПОДРАЗДЕЛЕНИЯ УПРАВЛЕНИЯ БЕЗОПАСНОСТИ ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ

Аннотация. Объектом исследования является процесс обеспечения внутриобъектовой безопасности высшего учебного заведения. Предметом исследования методы сбора, хранения и обработки данных об объектах ответственности подразделения управления безопасности. Тема исследования посвящена разработке подсистемы информационной поддержки деятельности сотрудников подразделения управления безопасности УГАТУ. Был произведен анализ предметной области, а также аналитический обзор программных продуктов для решения сбора, хранения, обработки, анализа и графического представления пространственных и атрибутивных данных об объектах ответственности подразделения управления безопасности.
***Ключевые слова*:** геоинформационные системы; ГИС УГАТУ; ГИС ИнГео; управление безопасности; обеспечение внутриобъектовой безопасности; образовательное учреждение.

Обеспечение функционирования надежной системы безопасности является одной из первостепенных организационных задач. Вне зависимости от масштаба или характера рассматриваемого заведения, построение внутриобъектовой безопасности — это необходимый фактор, влияющий на его нормальное функционирование. Поддержание высокой результативности напрямую зависит от методик и применяемых технологий в т. ч. коммуникационных систем связи, навигационных спутниковых систем, справочников и статистических данных и т. д. На практике внедрение технологий ограничивается как отсутствием ресурсов аппаратного обеспечения, так и специализированных программных продуктов для создания, организации и использования в работе информационных систем. Большая часть деятельности на данный момент автоматизирована только частично и по-прежнему выполняется на бумаге. Вследствие этого информация зачастую является неактуальной и малодоступной, что значительно сокращает оперативную значимость полученных данных

Информационные технологии и разработка систем заданной предметной области являются главной задачей процесса оптимизации любого сложного процесса, а в частности структур образовательного учреждения.

Безопасность – это некоторое положение конкретного объекта или сложно устроенной системы, при котором отсутствуют угрозы внешнего или внутреннего характера. Это статус защищенности, при котором негативные или разрушительные воздействия не представляют опасность для обеспечения нормального процесса функционирования. Разработка системы безопасности – это комплексный и многоплановый процесс. Прежде всего обеспечение безопасности в организации — это создание и осуществление администрацией нормативных документов и рекомендаций, а также системы мер и правил взаимодействия объектов внутри нее. Их исполнение подразумевает устойчивость системы к неправомерным действиям злоумышленника либо ее защищенность и стабильное функционирование в случае возникновения непредвиденной чрезвычайной ситуации.

Обеспечение внутриобъектовой безопасности ВУЗа — это набор регулирующих правил, рекомендаций и нормативных документов, а также организационных и технических мероприятий направленных на создание безопасных условий деятельности студентов и сотрудников университета; сохранение внутреннего порядка; обеспечение личной и государственной тайны информации; материального имущества и т. д.

Общие понятия и принципы безопасности, а также меры и правила построения системы безопасности и ее функции определяет Федеральный законом от 28.12.2010 № 390-ФЗ «О безопасности». Согласно данному правовому документу, можно выделить основные принципы, на которых основывается система управления безопасности:

– Принцип соблюдения и защиты прав и свобод гражданина – базируется на второй статье Конституции Российской Федерации и подразумевает обязательство государства признание их высшей ценностью

– Принцип законности – соблюдение равного исполнения субъектами правового законодательства для обеспечения общенациональной безопасности.

– Принцип системности и комплексности применения федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, другими государственными органами, органами местного самоуправления политических, организационных, социально-экономических, информационных, правовых и иных мер обеспечения безопасности. Данный принцип характеризуется понятиями системность и комплексность. Системность — это рациональное и оптимальное представление, распределение обязанностей внутри многоуровневой системы. Комплексность обозначает завершенность деятельности, координацию и построение взаимосвязи между частями данной системы.

– Принцип приоритета превентивных мер в области обеспечения безопасности. Превентивные меры направлены на прогнозирование и предупреждения возможных угроз безопасности.

– Принцип взаимодействие федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, других государственных органов с общественными объединениями, международными организациями и гражданами в целях обеспечения безопасности. Под функциями взаимодействия следует понимать стабильный обмен информацией и организацию коллективной деятельности и мероприятий структурных подразделений по обеспечению безопасности.

Данные принципы должны послужить основой при разработке подсистемы обеспечения внутриобъектовой безопасности в составе ГИС УГАТУ.

Применение геоинформационных систем положительно отразится на выборке существенной информации из большого массива данных. В настоящее время цифровые карты сочетают в себе точность и исчерпывающее количество разнообразных справочных материалов.

В соответствии с письмом Министерство образования и науки России от 30 августа 2005 года № 03-1572 обозначена совокупность мероприятий по обеспечению безопасности, которая включает в себя разработку мер и внутренних правил учреждения; обучение сотрудников и учащихся в рамках курса Безопасности жизнедеятельности; инструктажи по поведению в чрезвычайных ситуациях, разработка и пояснение методических указаний и техники безопасности; меры противодействия угрозе террористических актов; установка технического оборудования управления безопасности (громкоговорителей, систем оповещения, противопожарной безопасности), а также сотрудничество и взаимодействие с правоохранительными структурами.

На данный момент существует глобальная тенденция применения ГИС для автоматизации и повышения эффективности процессов в различных сфера деятельности человека. Подобные системы уже находят свое применение в образовательных учреждения по всему миру. ГИС предоставляет администрации учебного заведения широкий инструментарий для организации, мониторинга, управления, анализа и графического представления данных, что помогает в решении задач планирования и оперативного принятия решений.

Система рассматривается как набор аппаратно-программного обеспечения и информационных средств для реализации возможностей работы с актуализированными пространственно-распределенными данными и относящейся к ним атрибутивной информации. Это предлагает руководству университета большой спектр ресурсов и функциональных возможностей для совершенствования управления и организации учебного процесса и рабочей среды в учреждении. ГИС в образовательной организации может быть использован для мониторинга безопасности в кампусах и предотвращения кризисных ситуаций; позволит упростить процессы административно-хозяйственной деятельности, а также построения логистических путей и маршрутов передвижения транспортных средств по всей территории учреждения; создания тематических карт инфраструктуры университета, а также объектов интереса и ответственности его

структурных подразделений. Помимо этого, ГИС «УГАТУ» должен предоставлять сотрудникам и учащимся, а также лицам и организациям, заинтересованным в развитии деловых отношений, свободный доступ к открытой и актуальной информации о разных направлениях и видах деятельности, которыми занимается ВУЗ.

На данный момент администрацией и руководством УГАТУ было вынесено решение о необходимости разработки общей геоинформационной системы университета, которая должна стать инструментов повышения производительности и эффективной работы его подразделений, а также предоставления набора актуальных данных для решения задачи планирования и поддержки принятия решений для руководства и сотрудников учреждения. В рамках информационной системы должна быть реализована подсистема, которая поможет в решении поставленного вопроса по обеспечению внутриобъектовой безопасности образовательной организации и объектов интереса и ответственности специализированных подразделений.

ГИС УГАТУ реализуется на нескольких платформах одной из которых является ГИС «ИнГео».

«ИнГео» является набором программ, который позволяет построить систему «клиент-сервер» только третьей технологической схемы работы с пространственными данными. Основой системы является сервер данных собственной разработки, который взаимодействует с программой-клиентом через локальную сеть или сеть «интернет». При необходимости возможна установка всех компонентов системы на одном компьютере, имитирующем локальную работу одного пользователя без использования сети и выделенного сервера данных.

Сервер данных «ИнГео» хранит как пространственные, так и семантические данные внутри внешней СУБД, в качестве которой могут быть использованы файловая СУБД Borland Paradox (через BDE), а также SQL сервера Microsoft SQL Server и Oracle SQL Server. Данные о пространственных объек-

тах хранятся во внутреннем двоичном формате, разбитыми на большие блоки, внутренняя структура которых разработчиком не раскрывается. Доступ к пространственным данным возможен только через внутренние функции системы.

Заключение

Геоинформационные системы являются важным инструментом, а также необходимым связующим компонентом для структур различного уровня крупной компании или федерального учреждения.

Внедрение разработанной подсистемы обеспечит информационную поддержку сотрудников управления безопасности, а также позволит актуализировать пространственные и атрибутивные данные об объектах ответственности подразделения управления безопасности.

СПИСОК ЛИТЕРАТУРЫ

1. Приказ ФГБОУ ВО УГАТУ от 26 декабря 2016 г. №2272 - О «Об утверждении инструкции по оформлению выпускных квалификационных работ обучающихся по образовательным программам высшего образования - программам бакалавриата, программам специалитета и программам магистратуры»;
2. Письмо Министерство образования и науки России от 30 августа 2005 года № 03-1572
3. ГОСТ 19.701-90 (ИСО 5807-85) "Единая система программной документации. Схемы алгоритмов программ, данных и систем. Условные обозначения и правила выполнения";
4. Методические указания для выполнения выпускной квалификационной работы для студентов специальности 230201 «Информационные системы и технологии» [Текст] / Сост.: С.В. Павлов, Г.М. Сайфутдинова, О.И. Христодуло, Р.А. Шкундина. – Уфимск. гос. авиац. техн. ун-т. – Уфа, 2008 –72 с.;
5. Рябышева, И. В. Сравнительный анализ подходов к проектированию информационных систем. Доклад в секции информационные технологии [Текст]/ Всероссийская конференция молодых ученых по математическому моделированию и информационным технологиям с участием иностранных ученых 1-3 ноября, г. Новосибирск, Россия. – 2008. – 8 с.
6. Гаврилов А.В. Использование современных CASE-средств структурного проектирования при обучении студентов по направлению подготовки «прикладная информатика» [Текст]/Открытое образование. – 2015. − №4(111). − с: 22-27.
7. Коломец Н. В. О методах и средствах проектирования программного обеспечения (обзор и примеры) [Текст]/ Ростовский научный журнал. – 2017. – №4. – с. 249-265.
8. Ципилева Т.А. Геоинформационные системы [Текст]: учебное пособие − Томск: Томский межвузовский центр дистанционного образования, 2004.− 162 с.
9. Рыбанов А.А. Инструментальные средства автоматизированного проектирования баз данных: Учебное пособие и варианты заданий к лабораторным работам по дисциплине «Базы данных» [Текст]/ВолгГТУ, Волгоград, 2007. – 96 с.
10. Горбаченко В. И. Проектирование информационных систем с CA ERwin Modeling Suite 7.3 [Текст]: учебное пособие / В. И. Горбаченко, Г. Ф. Убиенных, Г. В. Бобрышева – Пенза: Изд-во ПГУ, 2012. – 154 с.

УДК 332.14:004.9

Л. М. МАЗГАРОВА
98lillitlu13@gmail.com
Науч. руководов. – канд. техн. наук, доц. А. В. ИВАНЦОВ

Уфимский государственный авиационный технический университет

РЕАЛИЗАЦИЯ СИСТЕМЫ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА С ФУНКЦИЕЙ ТЕРРИТОРИАЛЬНОГО ОТСЛЕЖИВАНИЯ ДОКУМЕНТОВ

Аннотация. Рассматривается задача территориального отслеживания документов в системе документооборота, в том числе их состояние, места создания и хранения. Изучается предметная область, а также актуальность системы электронного документооборота в современности. Предлагаются инструменты для решения задачи отслеживания документов
Ключевые слова: электронный документооборот; бизнес-процессы; СЭД.

ИЗУЧЕНИЕ ПРЕДМЕТНОЙ ОБЛАСТИ

Главный источник информации в любой организации — это документы, которые создаются и существуют в рамках бизнес-процессов. Контент появляется на разных стадиях процесса: в начале, когда происходит согласование договора, или в конце, когда производится выдача справок, подготовка маркетингового материала.

Для удобства работы с документами в предприятия внедряются СЭД.

Система электронного документооборота (СЭД) — это программное обеспечение для работы с электронными документами на всех стадиях их жизненного цикла: создание, редактирование, хранение. Современные системы поддерживают возможности маршрутизации документов и, конечно, такие базовые функции, как поиск, классификация и т.п. Документы и бизнес-процессы неразрывны, поэтому современные системы автоматизации должны включать набор инструментов для работы как в поле процессов, так и в поле информации.

Изначально СЭД создавались как инструмент автоматизации делопроизводства, однако сегодня развились в многофункциональные, комплексные продукты. Система электронного документооборота имеет следующие полезные функции:

1. Обеспечение процесса создания и перемещения внутрифирменной документации в электронном виде;

2. Обработка поступающей корреспонденции и внешних нормативно-распорядительных документов;

3. Упрощение контроля над документопотоками;

4. Помощь в эффективном управлении отношениями с партнерами и клиентами и многое другое.

В компании СЭД обеспечивает работу со всеми документами в электронной форме — любым набором информации, сохраненном или переданном на ПК. Их необходимо сопровождать атрибутами на своеобразных «карточках», которые идентифицируют единицу.

Документооборот в электронной форме — это способ централизованно организовать работу с бумагами, где большинство регистров и операций представлены в электронном виде. Соответственно, система, управляющая им, представляет собой решение с инструментарием – комплексом сервисов электронного документооборота - для осуществления всех процедур по созданию, изменению, поиску документов и поддержке взаимодействия между сотрудниками компании.

В процессе собственной эволюции СЭД постепенно «научились» сопровождать и обеспечивать бизнес-логику всего жизненного цикла документа, а потом – автоматизировать сквозные бизнес-процессы, связанные с документооборотом, частично принимая на себя функции BPM-систем (Business Process Management).

Реализация СЭД

С 2017 года развивается концепция CSP (Content Service Platform), для которой характерен отказ от монолитной архитектуры систем прежних поколений в пользу платформы, которая поставляется в виде набора сервисов. Современные СЭД, представляют собой CSP-платформы, которые объединяют и поддерживают работу сервисов, необходимых для конкретной компании на данном этапе ее жизненного цикла и с учетом специфических задач. При этом

платформа оставляет возможность в любой момент добавить новый сервис, обновить или доработать отдельный модуль.

Документы имеют много форм, ими могут быть как простые письма, договора, проектные документы, так и формализованные документы, структура которых определена законодательством. Организации, обменивающиеся документами как правило территориально распределены, поэтому документооборот также территориально распределен. Это объясняет, почему важно предусмотреть возможности организации единой СЭД в географически удаленных друг от друга подразделениях компании.

Для реализации этого возможно привлечение элементов геоинформационных систем, или компонентов веб-интерфейсов, в которых применяются элементы геоинформационных систем.

Например:

– Отслеживание перемещения документов в режиме онлайн с добавлением элемента мультипликации

– Перечень документов в точке на определенной территории

– Визуальное отображение статусов документов, их изменение.

Функция территориального отслеживания документов в режиме реального времени должна быть оснащена удобными инструментами настройки, локализации, карта должна хорошо масштабироваться.

Для реализации этой функции существуют различные инструменты и библиотеки JavaScript, предназначенные для создания карт и работы с ними.

1. Leaflet. Считается одной из лучших для создания «дружелюбных» интерактивных карт. Она относительно маленькая, но при этом имеет множество функций и плагинов, простой API и работает во всех браузерах и на всех платформах.

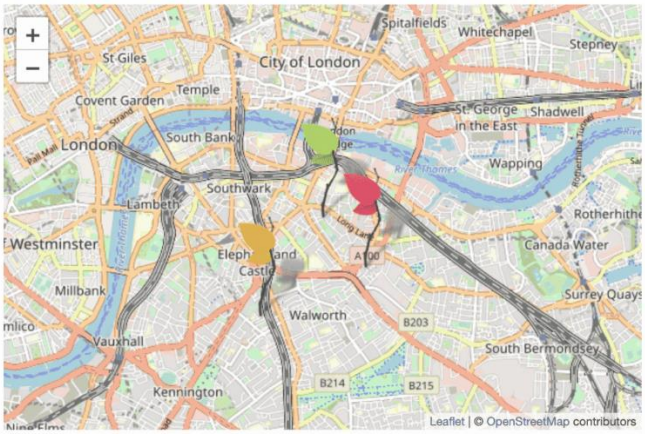


Рис. 1

2. OpenLayers - JavaScript-фреймворк с открытым исходным кодом, предназначенный для создания интерактивных карт при помощи различных сервисов. Одним из достоинств можно считать возможность использования CSS для изменения внешнего вида карты под нужны разработчика. OpenLayers также подходит для рендеринга векторных данных из GeoJSON, TopoJSON, KML, GML и других географических форматов данных.

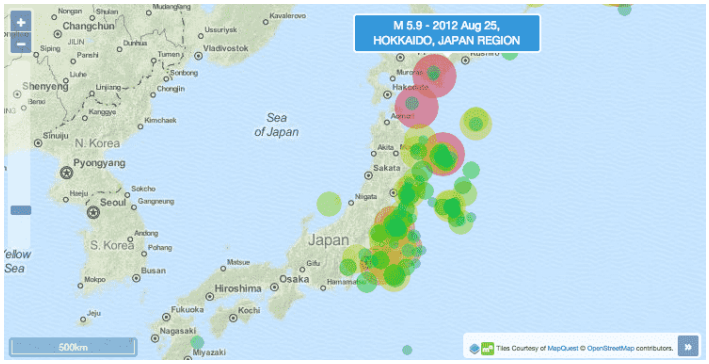


Рис. 2.

3. Google Maps.

Наиболее известная библиотека, имеющая множество поклонников. Ее преимуществом является то, что JavaScript API значительно облегчает интеграцию в любое приложение, сервис или сайт.

Рис. 3.

СПИСОК ЛИТЕРАТУРЫ

1. Бобылева М.П. Управленческий документооборот: от бумажного к электронному. Вопросы теории и практики. М.: Изд-во «ТЕРМИКА», 2016. – 360 с
2. Майкл Дж. Д. Саттон. Корпоративный документооборот. Принципы, технологии, методология внедрения. СПб. : Азбука : БМикро, 2002. - 448 с.
3. Алтухова Н.Ф. , Дзюбенко А.Л. , Лосева В.В., Чечиков Ю.Б. Системы электронного документооборота. (Бакалавриат). Учебное пособие. Изд-во: КноРус 2021 г. – 202 с.

УДК 004

Е. О. МАКАРОВ, А. Р. ФАРХУТДИНОВ, Т. А. ВАСИЛЬЕВ
makarov.e1999@ynadex.ru
Науч. руководов. – д-р техн. наук, проф. О. И. ХРИСТОДУЛО

Уфимский государственный авиационный технический университет

РАЗРАБОТКА ГЕОИНФОРМАЦИОННОЙ СИСТЕМЫ ДЛЯ ПРОГНОЗИРОВАНИЯ УРОВНЕЙ ВОДЫ НА СТАЦИОНАРНЫХ ГИДРОЛОГИЧЕСКИХ ПОСТАХ

Аннотация. В статье описывается процесс разработки ГИС для прогнозирования уровней воды на стационарных гидрологических постах, обосновывается ее актуальность, представлена схема базы данных, архитектура, алгоритм работы ГИС для прогнозирования уровней воды на стационарных гидрологических постах.
Ключевые слова: геоинформационная система; прогнозирование уровней воды; стационарные гидрологические посты; паводок.

Экстремальные природные явления гидрометеорологического происхождения, к которым относятся катастрофический паводок, сопутствуют человеческому обществу с древнейших времен. Катастрофический паводок, выдающийся по величине и редкий по повторяемости, может вызвать жертвы и разрушения [1].

В России паводки могут приобретать характер наводнения, которые наносят гигантский ущерб людям и территориям. Так в 1994 году в Башкирии произошло одно из самых страшных наводнений за последние 20 лет, произошел прорыв плотины Тирлянского водохранилища и вместе с этим сброс 8,6 млн куб метров воды. В ходе этой катастрофы погибли 29 человек, 786 остались без жилья. В зоне затопления оказалось 4 населенных пункта, 85 жилых домов было полностью разрушено. При ликвидации чрезвычайной ситуации были задействованы 1500 человек спасателей, 240 единиц техники. В ходе ликвидации последствий аварии восстановлены 12 километров дорог, 18 километров теплотрассы, два километра водопровода, пять километров линий электропередач, три разрушенных моста.

Прогнозирование уровней воды способствует оперативному принятию мер по снижению ущерба при чрезвычайных ситуациях, которые обусловлены

гидрологическими явлениями. Этим обуславливается актуальность разработки ГИС [2] для прогнозирования уровней воды на стационарных гидрологических постах.

Была разработана следующая информационная модель прогнозирования уровней воды на стационарных гидрологических постах (Рис. 1.).

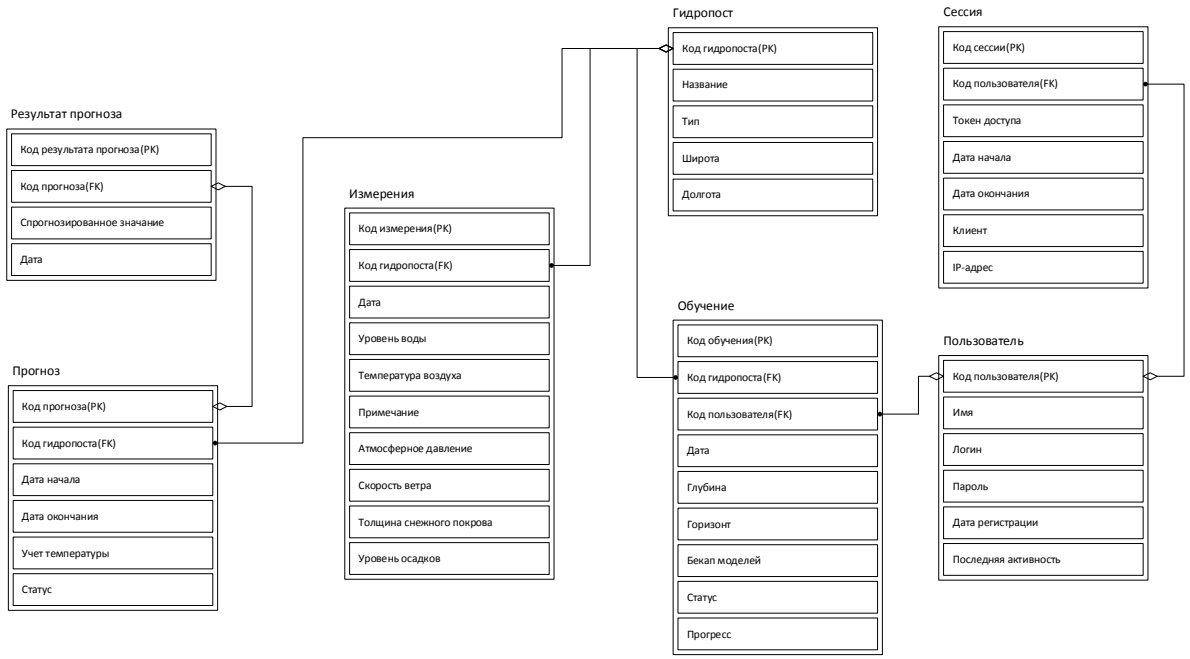


Рис. 1. Информационная модель прогнозирования уровней воды на стационарных гидрологических постах

Основной сущностью в данной модели является «Гидропост» так все фактические и спрогнозированные значения уровней воды хранятся для конкретного стационарного гидрологического поста, а также для каждого гидропоста создается своя модель нейронной сети и размещается на сервере. Хранение данных кардинально отличается от ГИС для водных ресурсов [3].

ГИС состоит из следующих компонентов: *Web*-интерфейс на *Angular* [4], *API* на языке *PHP* [5], СУБД *MySQL*, искусственная нейронная сеть на языке *Python* с применением библиотеки *Tensorflow* [6], планировщик задач *Cron*. API [4], разработанное на PHP является прослойкой между web-интерфейсом пользователя и искусственной нейронной сетью, которая выполняет прогнозы. Прогнозирование осуществляется следующим образом. Клиентское приложение на Angular отправляет запрос на инициализацию прогноза, затем API на PHP, воз-

вращает результат со статусом прогноза, если прогнозов в очереди нет, то планировщик задач Cron запускает искусственную нейронную сеть, которая возвращает по окончанию работы прогноз и записывает результат в БД, все это время клиентское приложение отправляет запросы с равными интервалами времени (5 с.), и в тот момент, когда результат прогноза запишется в БД, API вернет результат клиенту. Архитектурная схема приложения представлена на Рис. 2.

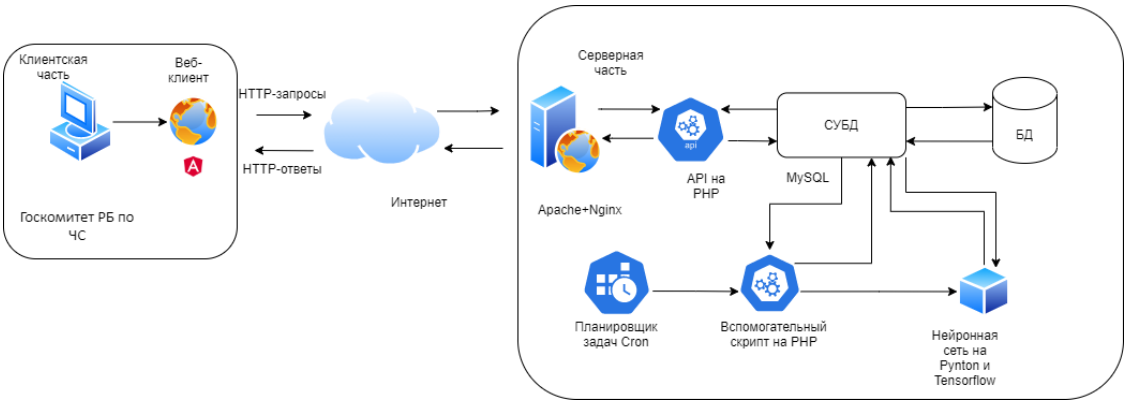


Рис. 2. Архитектурная схема ГИС для прогнозирования уровней воды

Основной функцией, данной ГИС является выполнение прогнозирования уровней воды на стационарных гидрологических постах. Алгоритм модуля, реализующего данную функцию, можно представить следующим образом: в самом начале происходит загрузка базовой карты, гидропостов на карте, загрузка данных о гидропостах, после чего пользователю необходимо осуществить выбор гидропоста для дальнейшего прогнозирования. Затем необходимо выбрать следующие параметры прогноза: дни прогноза, с учетом температуры или без него, выполнения прогноза по текущему гидропосту или по всем постам одновременно. Затем запускается цикл, в котором с интервалом в 5 секунд отправляются запросы к серверу на проверку статуса прогноза, если же его выполнение завершилось возвращается результат прогноза и происходит выход из цикла, если же выполнение прогноза не завершилось, то продолжается отправка запросов, после достижения лимита отправка запросов, после чего возвращается текст и код ошибки. Для дальнейшей работы со спрогнозированными дан-

ными может быть применен комбинированный алгоритм при расчете и построении зон затоплений при разливах рек [7].

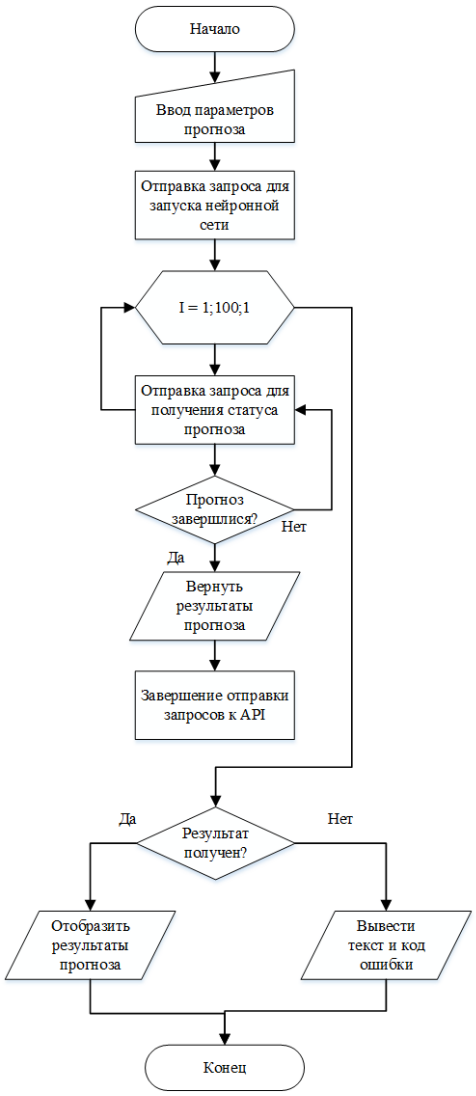


Рис. 3. Алгоритм модуля для прогнозирования

В данной статье были описаны основные аспекты разработки ГИС для прогнозирования уровней на стационарных гидрологических постах, данная система обеспечивает оперативное получение спрогнозированной информации об опасных уровнях воды основных пользователей системы, одним из которых является Госкомитет РБ по ЧС [8]. Данная система может помочь пользователям снизить экономический ущерб от паводка, а также обеспечить своевременное оповещение населения. Дальнейшее развитие данной системы заключается в моделирование зон затопления на основе модели речной сети [9].

СПИСОК ЛИТЕРАТУРЫ

1. Министерство Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий [Электронный ресурс] URL: https://02.mchs.gov.ru/deyatelnost/poleznaya-informaciya/vnimanie-polovode/chto-takoe-polovode-pavodok-navodnenie, свободный – (Дата обращения: 09.09.2021).
2. Крымский В.Г., Павлов С.В., Христодуло О.И. Информационное обеспечение оценки состояния водных объектов и управления ими на основе геоинформационных технологий. Москва, 2010. ООО «Дата+», 284 с.
3. Павлов С.В., Абрамов С.А., Шкундина Р.А., Христодуло О.И. Геоинформационная система для управления водными ресурсами на территориальном уровне (на примере республики башкортостан) // Геоинформатика. 2008. № 4. С. 14-20
4. Официальная документация Angular [Электронный ресурс] URL: https://angular.io/docs – (Дата обращения: 09.09.2021).
5. Официальная документация PHP [Электронный ресурс] URL: https://www.php.net/manual/ru/ – (Дата обращения: 09.09.2021).
6. Официальная документация Tensorflow [Электронный ресурс] URL: https://www.tensorflow.org/api_docs/python/tf – (Дата обращения: 09.09.2021).
7. Христодуло О.И., Шарафутдинов Р.Р. Использование комбинированного алгоритма при расчете и построении зон затоплений при разливах рек// геоинформационные технологии в проектировании и создании корпоративных информационных систем. Уфа, 2008. С. 183-191.
8. Государственный комитет Республики Башкортостан по чрезвычайным ситуациям [Электронный ресурс] URL: https://gkchs.bashkortostan.ru/about/ – (Дата обращения 07.09.2021)
9. Павлов С.В., Христодуло О.И., Шарафутдинов Р.Р. Разработка геоинформационной модели речной сети с учетом картографической, гидрологической и морфометрической информации для определения границ зон затоплений при изменении уровня воды в водных объектах // Вестник Уфимского государственного авиационного технического университета. 2008. Т. 11. № 1. С. 18-27.

УДК 5.5

В. А. МАЛИНСКАЯ
malina26020015@gmail.com

Уфимский государственный авиационный технический университет

ОТСЛЕЖИВАНИЕ МЕСТОПОЛОЖЕНИЯ И ПОСТРОЕНИЕ МАРШРУТА СЛЕДОВАНИЯ ТРАНСПОРТНОГО СРЕДСТВА

Аннотация. В данной статье рассматривается понятие мониторинга маршрута следования и его значение в современном мире. Также проводятся анализ и сравнение современных программных обеспечений, специализирующиеся в данной области. В ходе анализа предметной области мы делаем вывод о количестве передаваемых данных, необходимом оборудовании и необходимости применения ГИС технологий для решения данной задачи.
Ключевые слова: водитель; мониторинг маршрута; ГЛОНАСС; GPS; контрольные точки; веб-приложение; отслеживание.

Введение

Современное информационное общество стремительно развивается во всех сферах информационных систем. Сегодня процесс развития приобрел глобальный характер и уже охватывает практически все развитые страны мира, в том числе и Россию. Система мониторинга не осталась в стороне.

Всего существует два способа определения местоположения. Первый – это система мониторинга построенная на основе систем спутниковой навигации, оборудования и технологий сотовой(радио) связи, вычислительной техники и цифровых карт. Она позволяет отследить положение такси и автобусов, грузовых и легковых автомобилей, а также водного, воздушного и железнодорожного транспорта. Благодаря этому транспортные компании могут гарантировать безопасность как пассажиров и водителя, так и перевозимого груза. Кроме того, технология отслеживания выявляет недобросовестных водителей и способствует повышению дисциплины.

Основные спутниковые приемники передачи данных

В основном, система мониторинга построена на основе приемников спутникового сигнала *Глонасс* и *GPS.*

Глонасс

Глобальная Навигационная Спутниковая Система разработана в 1982 году по заказу Министерства обороны России. Терминал устанавливается на транс-
портном средстве. В дальнейшем он позволяет определить местоположение по географическим координатам передаваемыми от спутниковых систем.

GPS

Global Positioning System – система глобального позиционирования разработанная в 1973 году Министерством обороны США. Основным принципом использования данной системы является определение местоположения путем измерения моментов времени приема синхронизированного сигнала от навигационных спутников антенной потребителя.

Их основное различие в том, что *GPS* спутники располагаются на 6 плоскостях по 4 аппарата в каждой плоскости, а *ГЛОНАСС* располагает 8 своих спутников всего в 3 плоскостях.

Системы *ГЛОНАСС* и *GPS* имеют схожую архитектуру, тем самым, можно сделать вывод, что они работают по следующей *схеме мониторинга транспорта:*

1. *GPS* с помощью сотовой связи связывается с центром данных, тем самым определяя локация ТС.

2. Трекер, установленный на ТС, информирует о своем местоположении каждые 5-10 секунд (время может изменяться).

3. Одновременно с пунктом 2 происходит обработка данных, которые в последствии попадают на терминал.

4. Собранные данные отправляются на сервер, где происходит их анализ и систематизация при помощи специализированного ПО.

5. Поступление данных клиенту.

От чего зависит точность передачи данных?

Степень точности(погрешность) вычисления координат зависит от ряда факторов, таких как:

– Смещение показания *GPS*-часов;

– Положение спутника относительно *GPS*-приемника;

– Задержка распространения;

– Искажение данных (чаще используется в военных целях);

– Погодные условия;

– Прохождение радиоволн в тропосфере;

– Распространение радиоволн в тропосфере;

– Расхождение шкал времени различных спутников;

– Расстояние от ТС до спутника.

В настоящее время ведутся работы по улучшению передачи данных, показателей доступности и целостности систем ГЛОНАСС и *GPS*. Но, тем не менее, эти навигационные системы полностью удовлетворяют требованиям точности при определении местоположения гражданских потребителей.

Основные программные продукты для решения данной задачи

Существует множество программ для мониторинга маршрута транспорта. Сейчас проведем анализ наиболее известных в нашей стране:

Таблица 1

Название	Страна происхождения	Основные возможности
Ставтрэк Онлайн	Россия	– Мониторинг в режиме онлайн – Детальный контроль топлива – Модуль контроля качества вождения – Отчет о пройденном маршруте за любой период – Визуализация данных в графиках и диаграммах
Wialon Local	Белоруссия	– Мониторинг стационарных и подвижных объектов – Мониторинг скоростного режима – Мониторинг непрерывной работы двигателя
Omnicomm	Россия	– Мониторинг уровня топлива – Мониторинг транспорта на основе *GPS* и ГЛОНАСС
Fort Monitor	Россия	– Мониторинг транспорта на основе спутников – Построение отчетов – Оповещение о нарушениях
СКАУТ Онлайн	Россия	– Мониторинг маршрута следования – История маршрута следования – Построение отчетов
ГЛОНАССсофт	Россия	– Мониторинг маршрута следования – Контроль топлива – Контроль скоростного режима

Произведя анализ известных ПО для построения маршрута следования, можно сделать вывод, что их функционал мало чем отличается друг от друга и они являются конкурентами на рынке по предоставлению необходимого ПО.

Принцип работы

Так как рассмотренные нами ранее программные продукты работают на системе ГЛОНАСС и GPS, мы можем сделать общий алгоритм работы мониторинга маршрута следования:

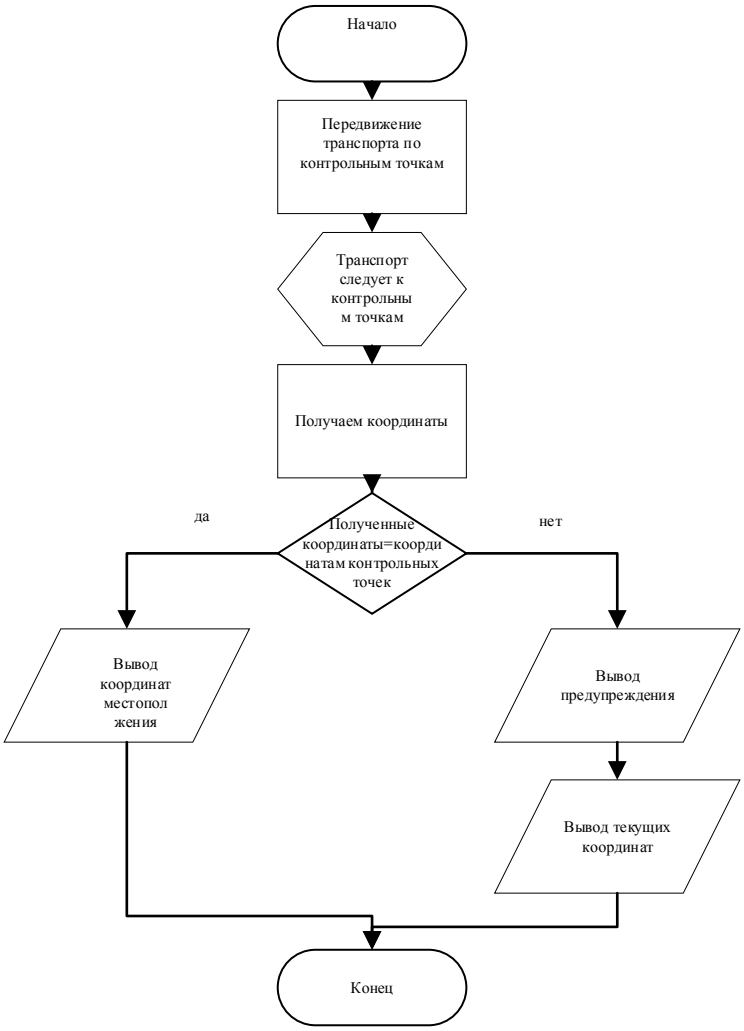


Рис. 1. Алгоритм работы мониторинга

Реализация программного обеспечения для отслеживания маршрута следования

Для реализации программного обеспечения я выбрала приложение *ArcGIS.*

ArcGIS – это программное обеспечение для построения ГИС любого уровня. *ArcGIS* позволяет собирать, организовывать, управлять, анализировать, обмениваться и распределять географическую информацию.

Система *ArcGIS* позволяет создавать надежную географическую информацию ГИС-сообществом, легко и просто использовать ее заинтересованным

людям. Данная система включает в себя программное обеспечение, интерактивную

облачную инфраструктуру, профессиональные инструменты, настраиваемые ресурсы. Поддержка серверов и облачных платформ позволяет выполнять совместную обработку и обмен данными.

Формирование маршрута в данном приложении может происходить как в режиме *OFFline* путем указания точек, которое должно пройти наше ТС, так и в режиме *Online* путем подключения *GPS*-приемника к устройству.

Так как у нас нет необходимых продуктов, мы строим маршрут по контрольным точкам.

Начинаем с указания начальной точки, далее последовательно отмечаем другие пункты по ходу движения и задаем интервал времени, за которое ТС должно добраться из начальной точки в конечную.

Рис. 2. Созданная карта с контрольными точками

Транспортные сети, например, дорожные, лучше всего строить в ArcGIS при помощи наборов сетевых данных. Для работы с наборами сетевых данных и выполнения их анализа необходим дополнительный модуль ArcGIS Network Analyst.

При введении каждой из точек, мы указываем следующую информацию:

– Название контрольной точки;

– Радиус контрольной точки(погрешность);

– Время отправления;

– Время прибытия.

После введения всех необходимых данных мы можем наблюдать графический указатель, построенный на указанных нами ранее контрольных точках.

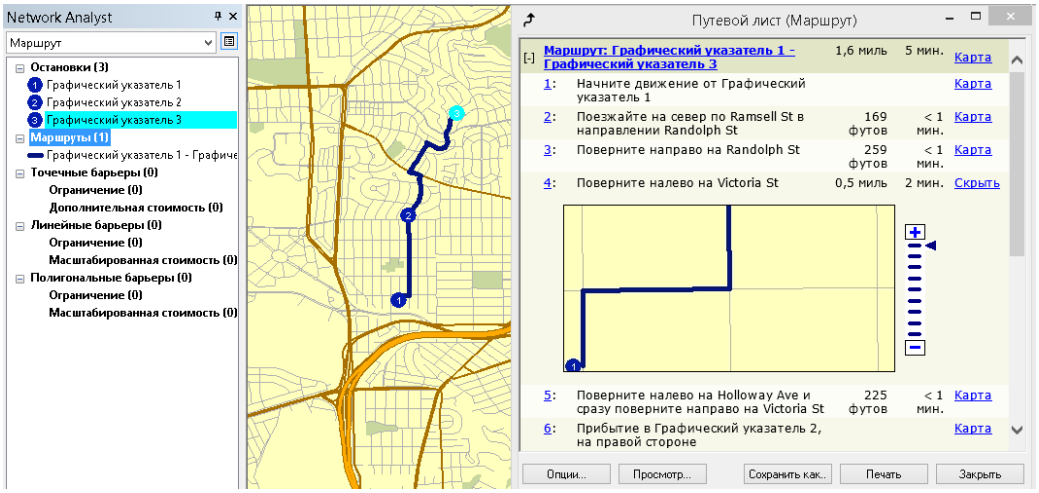


Рис. 3. Созданный графический указатель

Для лучшего отображения маршрута пути и наглядного выявления схода с маршрута мы применяем создание буферной зоны вокруг объекта. Бирюзовым цветом отмечен маршрут следования, красным – крайние зоны.

Рис. 4. Созданные буферные зоны

После введения необходимой информации система мониторинга будет отслеживать прохождение ТС по указанному маршруту и оповещать о сбоях, отклонениях по маршруту и ошибках навигационного устройства.

Заключение

В ходе написания статьи мы пришли к выводу, что мониторинг маршрута следования стал неотъемлемой частью современной жизни. Так же были рассмотрены основные программные обеспечения и компоненты, необходимые для решения данной задачи.

Список литературы

1. Сайт *ArcGIS* компании *ESRI.* – Режим доступа: https://desktop.arcgis.com/
2. Сайт пошагового руководства выполнения действий в *ArcGIS* компании *ESRI.* – Режим доступа: https://learn.arcgis.com/ru/
3. Сайт Wialon: https://wialon.ru/kontrol-marshrutov
4. Быховский, М.А. Развитие телекоммуникаций. На пути к информационному обществу. Развитие радиолокационных систем: Учебное пособие для вузов/ - М.: Гор. линия-Телеком, 2015. - 402 с.

УДК 551.509.51

А. В. МАЛЫШЕВ
agerasx@gmail.com
Науч. руководитель – канд. техн. наук, доц. А. Ф. АТНАБАЕВ

Уфимский государственный авиационный технический университет

ПОЛУЧЕНИЕ МЕТЕОРОЛОГИЧЕСКИХ ДАННЫХ И ИЗУЧЕНИЕ СОЛНЕЧНОГО ИЗЛУЧЕНИЯ ДЛЯ ТЕРРИТОРИИ РЕСПУБЛИКИ БАШКОРТОСТАН

Аннотация. Объектом исследования является процесс сбора и обработки данных о солнечном излучении. Предметом исследования являются методы сбора метеорологических данных, обработка и визуализация солнечного излучения для территории Республики Башкортостан.
Статья посвящена проектированию и разработке программного продукта, решающего задачи сбора и обработки метеорологических данных для изучения солнечного излучения для территории Республики Башкортостан. В работе приводятся результаты анализа предметной области, а также аналитического обзора программных решений, необходимых для сбора, обработки и визуализации метеорологических данных.
***Ключевые слова*:** метеорологические данные; СУБД; программный продукт; солнечное излучение; инсоляция.

Ни для кого не секрет, что метеорологические явления сильно влияют на всю планету, в том числе и на Республику Башкортостан. Плохая видимость, облачность, сильный ветер, гололед, метель, ливень и т.д. — все это может оказаться опасным, если не принимать специальные меры для предотвращения серьезного ущерба в тех или иных отраслях.

Наша страна и Республика имеют обширные территории и существуют отдаленные территории, которые нуждаются в электроэнергии. Имеются множество устаревших тепловых электростанций с низкими экологическими стандартами, которые дороги в ремонте. И при передаче электроэнергии на больших расстояниях из других регионов, происходят сетевые потери.

Исходя из этого становится ясно, что имея метеорологические данные в структурированном виде – это поможет решить множество прикладных задач и в том числе они могут помочь в расчетах солнечного излучения.

Солнечная энергетика – это перспективная и развивающаяся отрасль. Постепенно увеличивается КПД и снижается стоимость оборудования. При переходе на солнечную энергию снижаются вредные выбросы.

Также стоит отметить, что без развития возобновляемых источников электроэнергии будет расти стоимость электроэнергии в целом, так как добыча энергоресурсов становится сложнее, а сами технологии сжигания топлива не имеют дальнейшего потенциала снижения стоимости.

Существует не мало отдельных районов, которые не электрифицированы, или имеют проблемы со старыми источниками электроэнергии, иногда выходит эффективнее построить собственную солнечную электростанцию, которая будет способна обеспечить энергией этот отдаленный район. Например, поселок Северный в Абзелиловском районе нашей Республики в 2015 году перешел на автономное электроснабжение на основе возобновляемых источников энергии.

Отдельно хочется отметить Закон о микрогенерации, так называемый «Зеленый тариф». Это Федеральный закон от 27 декабря 2019 г. N 471-ФЗ. Суть его заключается в том, что частное лицо, имея объект микрогенерации, мощностью до 15 кВт. Имеет право реализовывать лишнюю выработанную электроэнергию, которая им не была потреблена в общую электрическую сеть. Не платя при этом налоги на доход, получаемый при продаже.

Таким образом установив солнечные панели, мы обеспечиваем свой дом электроэнергией, при излишке, мы ее продаем. В ночное время, когда электроэнергии не хватает мы приобретаем у поставщика электроэнергии. Двунаправленный счетчик считает и по истечении месяца, если мы отдали больше электроэнергии, чем потребили, то мы получим оплату по среднеоптовой цене в регионе. Тем самым быстрее окупим оборудование.

Исходя из этого была поставлена цель разработать программный продукта получения метеорологических данных и изучение солнечного излучения для территории Республики Башкортостан. Чтобы достичь эту цель были поставлены следующие задачи: анализ предметной области и обзор существующих решений, проектирование функциональной и информационной модели проекта, разработка алгоритма работы, выбор средств разработки, реализация программного продукта.

У нас есть несколько способов получения метеорологических данных. Первый способ — платить коммерческим компаниям, которые специализируются на этом. Например, если обратиться к прайсу на 2021 год компании Баш-

кирское управление по гидрометеорологии и мониторингу окружающей среды. То там мы увидим информацию, что нужные нам данные мы можем получить приблизительно за 12 тыс. рублей в месяц.

Второй способ получить метеорологические данные в структурированном виде — это обратиться на специальный сайт OpenWeather. Он предоставляет данные пригодные для дальнейшей работы с ними, но в бесплатном тарифе у нас есть множество ограничений, такие как 60 запросов в минуту и 1000 вызовов API в день, что нас не очень устраивает. Есть стандартный тариф, который все еще имеет некоторые ограничения. А тот тариф, который нас полностью устроит будет стоить 180$ в месяц.

Есть несколько источников данных, где можно найти данные о солнечном излучении. Самый простой способ — это просмотр статических карт солнечной инсоляции. Далее можно обратиться к коммерческим сервисам предоставляющие услуги по консультации и продаже оборудования для солнечных электростанций. И также существует сервис NASA POWER Data Access Viewer. Это обширный сервис, который предоставляет информацию по различным явлениям на всей планете. Однако имеет ряд недостатков.

Таким образом было принято решение разрабатывать собственный программный продукт получения метеорологических данных и изучения солнечного излучения для территории Республики Башкортостан. Нужно было определиться с формулой, по которой будет рассчитываться солнечное излучение, имея метеорологические данные. Самый главный показатель, который влияет на солнечное излучение, достигаемое земли — это облачность.

Множество сервисов представляют данные о солнце, не учитывая облачность. Тот же самый сервис NASA POWER Data Access Viewer преимущественно предоставляет данные о солнечном излучении в ясные дни, по которым можно просмотреть месячную статистику. Этот показатель был взят для дальнейших расчетов.

Мой расчет солнечного излучения происходит по формуле Тамары Григорьевны Берлянд, которая была описана в книге Сивкова Сергея Ивановича «Методы расчета характеристик солнечной радиации»:

$$Q_{\text{обл}} = Q * (1 - (a + b * n) * n), \quad (1)$$

где Q – суммарное солнечное излучение без учета облачности (прямое, рассеянное и отраженное); a – коэффициент, зависящий от среды и от широты местности; b – коэффициент, который можно считать постоянным и равным 0,38 (выведен Берлянд при сравнении зависимости Q и n); n – коэффициент облачности, где 0 – ясно, а 1 – пасмурно.

После преобразований получаем следующую формулу для расчета:

$$Q_{\text{обл}} = Q * (1 - (0.38 + 0.38 * n) * n), \quad (2)$$

Остается получить Q и n. Суммарное солнечное излучение взято из статистической выдачи сервиса NASA Power Data Access Viewer. А параметр n берется из полученных метеорологических данных. Беря во внимание показатели облачности утром, днем и вечером.

При анализе предметной области были выделены потенциальные пользователи программного продукта: администрация Республики Башкортостан, электрогенерирующие компании, обычные жители региона и иные исследователи.

В процессе исследования предметной области были выделены требования к программного продукту: разрабатываемый программный продукт не должен нарушать законодательство РФ, получение метеорологических данных должно выполняться в автоматическом режиме, серверная часть проекта должна быть универсальна для различных задач, клиентская часть проекта должна быть представлена в виде веб-сервиса, предоставляемая информация должна быть достаточно точной для расчета солнечной системы, разрабатываемый проект должен иметь перспективу развития.

Разрабатываемая геоинформационная система представлена классической трехуровневой архитектурой, в которой пользователи с любого удобного для них устройства через интернет обращаются к веб-серверу, который реализован средствами Nginx, который в свою очередь через сервер приложений Apache Tomcat обращается к серверу базы данных PostgreSQL.

Язык программирования для серверной части программного продукта был выбран Java. Это объектно-ориентированный язык программирования, ко-

торый является простым, быстрым, надежным и безопасным. Хоть он был разработан достаточно давно, он до сих пор актуален и многие компании продолжают использовать его для своих разработок. При разработке клиентской части был выбран язык JavaScript. Который является неотъемлемой частью веб-разработки.

В результате выполнения работы серверной части программного продукта получаем структурированные метеорологические данные. Преимущества программного продукта: полная автоматическая работа, которая обновляет информацию 4 раза в сутки, каждое обновление происходит по 8 минут, максимальная экономия трафика и времени так как загружается только таблица с данными, нежели вся html страница целиком. Клиент-серверная архитектура позволяет использовать полученную базу данных в различных разработках. В СУБД написаны триггеры, которые мгновенно выполняют обработку полученных данных и рассчитывают солнечное излучение с учетом облачности в процессе получения данных.

В результате работы клиентской части разработан адаптивный веб-сервис, который доступен любому желающему. Можно выбрать интересующее время, район и получить информацию по солнечному излучению или рассчитать получаемую солнечную энергию.

Разработан программный продукт получения метеорологических данных и изучения солнечного излучения для территории Республики Башкортостан. В процессе были решены все поставленные задачи. Программный продукт имеет хорошие перспективы развития, как серверной части для решения различных прикладных задач, так и клиентской части для более точных расчетов и добавления нового функционала к изучению солнечного излучения.

СПИСОК ЛИТЕРАТУРЫ

1. Первая ветро-солнечная электростанция – сайт [Электронный ресурс], режим доступа – свободный, URL: https://ufa.mk.ru/articles/2015/01/21/v-bashkirii-zarabotala-pervaya-kommercheskaya -vetrosolnechnaya-elektrostanciya.html, (дата обращения: 20.09.2021);
2. Солнечная энергетика Башкортостана – сайт [Электронный ресурс], режим доступа – свободный, URL: https://solarb.ru/solnechnaya-energetika-bashkortostana, (дата обращения: 18.09.2021);
3. Сивков, С.И. Методы расчета характеристик солнечной радиации / С.И. Сивков – Ленинград: Гидрометеорологическое издательство, 1968. – 232с;

4. ArcGIS API for JavaScript – сайт [Электронный ресурс], режим доступа – свободный, URL: https://developers.arcgis.com/javascript/latest/, (дата обращения: 20.09.2021).

УДК 004.413.2

А. А. НОЗДРИН
anton.nozdrin.12@mail.ru
Науч. руководов. – канд. техн. наук, доц. А. Ф. АТНАБАЕВ

Уфимский государственный авиационный технический университет

МОНИТОРИНГ ТРАНСПОРТНОГО СРЕДСТВА. КОНТРОЛЬ РЕЖИМА ТРУДА И ОТДЫХА ВОДИТЕЛЯ

Аннотация. В статье описываются основные аспекты контроля режима труда и отдыха водителей на основе законодательных актов, а также описывается процесс программной реализации контроля РТО в виде приложения. В ходе решения задачи делаются выводы о программной составляющей приложения, определяются необходимые функции и их взаимодействие между собой в ходе мониторинга транспортного средства и водителя. Данная статья является аналитической проработкой предметной области, которая производится с целью оптимизации дальнейшего процесса разработки.
***Ключевые слова*:** водитель; режим труда и отдыха; тахограф; мониторинг.

Введение

Контроль режима труда и отдыха (далее РТО) водителя – это обязательное условие для любой компании, которая осуществляет транспортную деятельность. Данная мера предназначена для предотвращения ДТП на дорогах во время поездки, за счет обеспечения водителя достаточным количеством времени для отдыха.

Правовые источники, регламентирующие РТО, определяют минимальные и максимальные временные рамки в зависимости от различных условий: продолжительность безостановочного вождения, смены, рабочей недели и др. Время труда и отдыха может изменяться в пределах этих рамок, а за нарушение предписаны штрафы как для водителя, так и для работодателя.

Далее приведем основные акты, на основе которых делались выводы о составлении рабочего графика для водителей на разных предприятиях.

Пункт 26 Правил дорожного движения (далее – ПДД) [1] описывает нормы времени труда и отдыха. Указывается, что водитель может непрерывно управлять транспортом *не более* 4,5 часов, после чего обязан сделать перерыв длительностью *не менее* 45 минут. Данный перерыв можно разделить на две части, например 15 и 30 минут (пункт 26.1).

Более детализированным и направленным на конкретные виды перевозок является Приказ Минтранса №424 «Об утверждении Положения об особенностях режима рабочего времени и времени отдыха водителей автомобиля» [2] более полно описывает что считается за рабочее время, а что нет, а также определяет дополнительные факторы, которые могут влиять на изменение временных рамок РТО. Приказ распространяется на все виды транспортной деятельности, за исключением указанных в разделе 1 Приложения; раздел 13 Приложения, в целом, повторяет пункт 26.1 ПДД.

Регистрация времени труда и отдыха, ввиду законных предписаний, осуществляется с помощью специального устройства – тахографа. Устройство фиксирует скорость транспортного средства (далее ТС) и РТО водителей. Тахограф работает с одним или двумя водителями, которые вставляют в устройство личную карту водителя. Тахограф является обязательным условием для осуществления транспортных перевозок. Устройство настраиваемое и обеспечивает автономный и объективный сбор информации, что позволяет точно установить факт нарушения и назначить наказание.

В случаях, когда установка тахографа не обязательна, но работодатель все равно хочет получать информацию о водителе, предприятия находят различные решения в виде программного обеспечения, устанавливаемого на смартфон, где водитель фиксирует свой статус. Показатели может видеть и анализировать диспетчер. Задачей данной статьи является определить возможность качественного мониторинга РТО водителя без использования тахографа, используя приложение, которое будет заменять часть функций бортового самописца и давать более широкие возможности для анализа. Для этого необходимо рассмотреть существующие варианты мониторинга ТС, относящиеся к отдельным фирмам или направленные на самого широкого потребителя.

Существующие решения

Каждый работодатель устанавливает графики работ индивидуально и для каждого водителя на определенный срок, учитывая правовые ограничения, наложенные на его вид деятельности.

Компания, о которой рассказывается в статье [3], в рамках корпоративных нужд разработала собственное решение на основе Wialon SDK, которое позво-

ляет настраивать различные временные показатели для каждого водителя отдельно и получать отчет после завершения рабочего периода (смены). Параметры, которые мониторит приложение:

1. максимальная продолжительность вождения днем;
2. максимальная продолжительность вождения ночью;
3. минимальное время отдыха после продолжительного вождения днем;
4. минимальное время отдыха после продолжительного вождения ночью;
5. максимальное количество часов вождение в сутки.

Базовый функционал различных систем мониторинга ТС (ГЛОНАСС, Stavtrack, Wialon), относящийся к контролю РТО, обычно включает в себя возможность составления отчетов о количестве рабочих часов за определенный период, а также картографическое отображение текущего местоположения водителя (GPS, ГЛОНАСС) с отрисовкой пройденного маршрута и контрольных точек.

В разрабатываемом приложении предлагается объединить описанный в начале раздела функции с возможностями специализированных систем – это позволит отдельно устанавливать РТО каждого водителя и наглядно отображать пространственные данные. Для решения задач, связанных с пространственными данными, используются геоинформационные системы (далее – ГИС). ГИС – это комплекс средств, направленных на визуальное отображение различных объектов на местности и анализ параметров этих объектов. Возможности ГИС позволят диспетчеру или администратору системы наблюдать текущее местоположение водителя, контролировать его маршрут и находить более оптимальные пути передвижения. Далее мы рассмотрим более подробно каждый аспект задачи.

Описание возможных методов контроля РТО в приложении

Основной задачей приложения будет получение текущего статуса водителя с указанием времени, когда статус стал активен. От этой временной метки производится отсчет времени, по истечению которого будет выведено оповещение о превышении, например, периода непрерывного вождения. Для каждого водителя можно устанавливать индивидуальный рабочий график. В момент, когда водитель изменяет статус (например «В пути», «Перерыв») мы начинаем отсчет времени. Когда таймер будет приближаться к установленному ограниче-

нию, будет выводиться уведомление. Ограничения будут вручную вводиться диспетче-
ром в окне редактирования водителя.

Для наглядного отображения мест остановок подключается картографический сервис, который будет отображать маркеры водителей с их текущим местоположением. В момент, когда водитель останавливается на перерыв на карте появляется метка, обозначающая остановку. Для качественной идентификации, какому именно водителю принадлежит метка, она будет соотноситься по цвету с маркером водителя. При нажатии на метку откроется всплывающее окно, в котором будет отображаться вспомогательная информация, например – когда сделана эта остановка. На рисунке 1 показан макет, на котором есть маркер водителя и знак остановки, который появился, когда водитель изменил свой статус на «Перерыв».

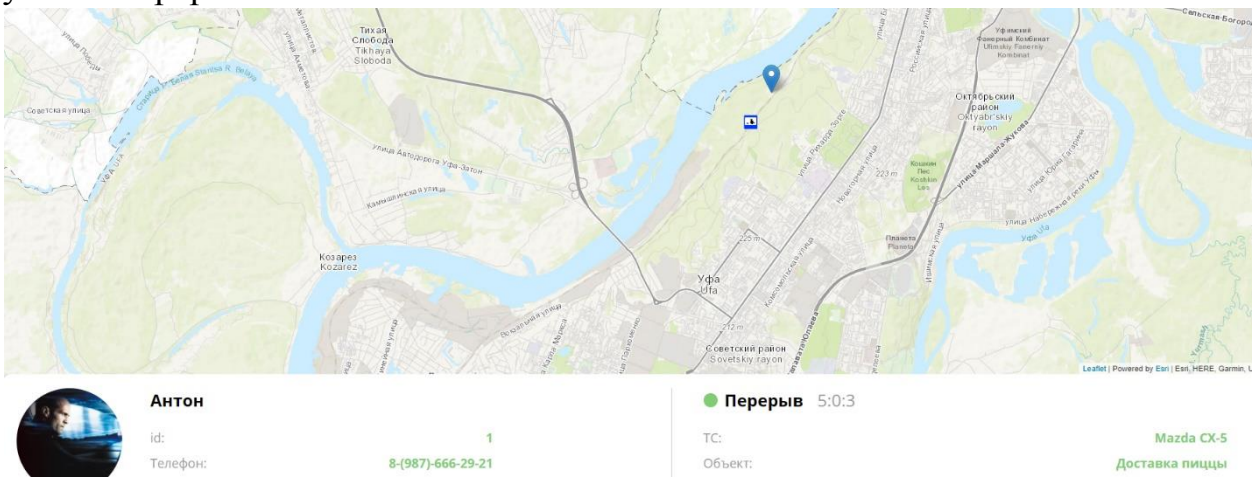


Рис. 1. Отображение данных о водителе

Также на карте мы можем отображать пройденный маршрут водителя, чтобы контролировать точное прохождение, или для последующего поиска более оптимальных путей.

На данный момент список функций, которые может реализовывать приложение следующий:

1. Индивидуальная настройка рабочего графика для каждого водителя
2. Контроль продолжительности управления ТС/отдыха водителя
3. Отображение местоположения водителя на карте
4. Отображение пройденного маршрута

Из данного списка видно, что все методы завязаны на одном объекте – водителе, и реализуют частично независимые разделы мониторинга водителя. Ис-
ходя из этого, описание структуры в базе данных (далее БД) можно представить в виде объекта со вложенностями, или в виде дерева (рис. 2).

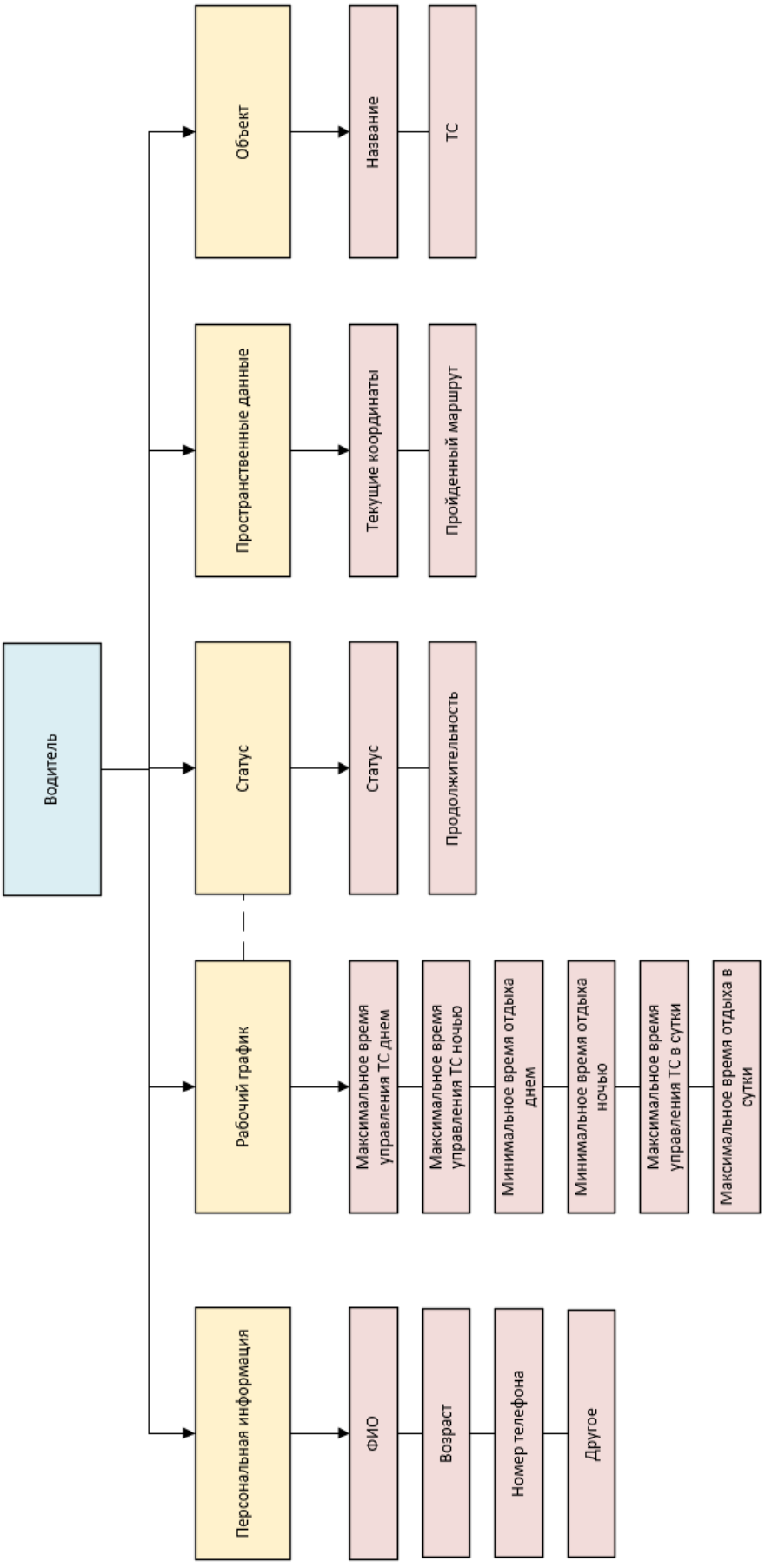


Рис. 2. Дерево объекта водителя в БД

Выше были описаны задачи, которые решаются в реальном времени. Данные в таком случае не накапливаются, а динамически изменяются. Для создания отчетов необходимо чтобы данные скапливались и сортировались по выбранным полям. Для выделения промежутка времени можно принять, что начало следующего статуса является окончанием предыдущего. Сохранять эти данные можно в виде дополнительной ветки объекта или создать отдельную сущность для каждого водителя и сохранять отчетные данные отдельно.

Функциональная блок-схема приложения показана на рисунке 3. На ее основе можно начать реализацию системы, первым этапом которой станет подбор подходящих инструментов разработки.

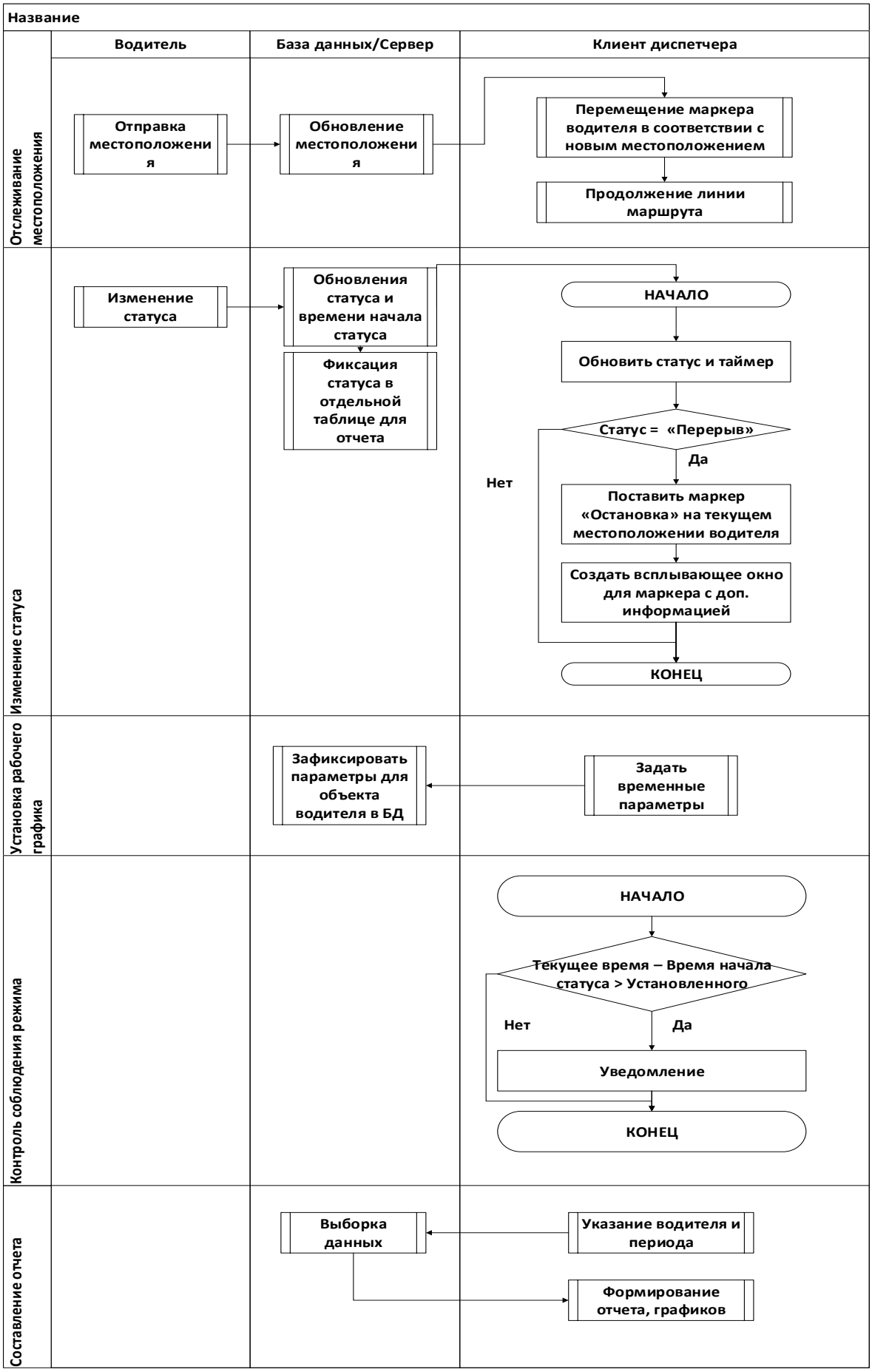


Рис. 3. Функциональная блок-схема

Заключение

Описанные выше функции можно реализовывать поэтапно, изолировав внутреннюю часть каждого метода от другого, что позволит ускорить процесс разработки и сократить количество ошибок. В совокупности приложение будет давать диспетчеру возможность контролировать водителя в течение всего периода работы благодаря пространственному отслеживанию положения ТС и учету времени статуса для предупреждения переработок, которые чреваты опасными случаями на дороге. Для анализа эффективности и дисциплины водителя диспетчер сможет создавать отчеты за определенный период.

В ходе аналитического разбора функций выявлено, что водитель будет отправлять малое количество данных (координаты) в короткие промежутки времени (2-5 секунд), а также периодически обновлять свой статус.

СПИСОК ЛИТЕРАТУРЫ

1. О Правилах дорожного движения (вместе с «Основными положениями по допуску транспортных средств к эксплуатации и обязанности должностных лиц по обеспечению безопасности дорожного движения»): постановление Правительства РФ от 23.10.1993 N 1090 (ред. от 31.12.2020)
2. Об утверждении Особенностей режима рабочего времени и времени отдыха, условий труда водителей автомобилей: приказ Министерства транспорта Российской Федерации от 16.10.2020 № 424
3. Войтихович О. Мониторинг режима труда и отдыха водителей с Wialon. [Электронный ресурс] 2019. URL: https://gurtam.com/ru/blog/wialon-lafargeholcim-az (дата обращения 20.01.2021)
4. Мавлютов А.Р., Атнабаев А.Ф. Внедрение геоинформационных систем на предприятие // Modern Science. 2020. № 1-2 с. 298-303.

УДК 004.413.2

Б. Р. РАМАЗАНОВ
bogdanramazanov2001@gmail.com
Науч. руководитель – канд. техн. наук, доц. А. Ф. АТНАБАЕВ

Уфимский государственный авиационный технический университет

МОНИТОРИНГ СКОРОСТНОГО РЕЖИМА ТРАНСПОРТНЫХ СРЕДСТВ

Аннотация. В данной статье описываются основные правила по контролю скорости транспортного средства, описывается принцип работы различных систем мониторинга транспортного средства, указаны ГИС-технологи, которые используются для контроля скорости. Также расписаны существующие компании, которые предоставляют услуги по мониторингу ТС
***Ключевые слова*:** контроль скоростного режима; водитель; скорость; ДТП; спидометр; GPS-спидометр; база данных; приложение; данные.

Введение

Мониторинг скорости транспортного средства является одной из основах функций, осуществляемых системами мониторинга транспортного средства ведь скорость, влияет как на риск аварии, так и на тяжесть травм, полученных при ДТП.

В соответствии с десятым разделом ПДД водитель должен вести транспортное средство со скоростью, не превышающей установленного ограничения, при этом он должен учитывать интенсивность движения, особенности и состояние транспортного средства и груза, дорожное и метеорологическое условия, в частности видимость в направлении движения, а при возникновении опасности для движения, которую водитель в состоянии обнаружить, он должен принять возможные меры к снижению скорости вплоть до остановки транспортного средства.

В населенных пунктах разрешается движение транспортных средств со скоростью не более 60 км/ч, на автомагистралях не более 110 км/ч а в жилых зонах, велосипедных зонах и на дворовых территориях не более 20 км/ч.

На грузовики, перевозящие пассажиров в кузове, накладываются самые большие ограничения. Их максимальная скорость - 60 км/ч. И в населенных пунктах, и на загородных трассах, и даже на автомагистралях.

Так контроль скорости транспортных не только поможет предотвратить аварию, но и существенным образом уменьшит тяжесть травм, получаемых жертвами ДТП.

В саму систему мониторинга транспорта входит комплекс датчиков, который устанавливают на транспорт. Они представляют из себя небольшие устройства, которые умеют собирать и передавать нужную для мониторинга информацию, а именно: скорость автомобиля, местоположение транспорта, уровень топлива в баке, температуру и.т.д.

Для измерения скорости автомобиля есть два вида приборов. Одни из них измеряют скорость непосредственно в автомобиле и называются спидометр, подобных приборов очень много и принцип их работы может сильно отличаться друг от друга. Другие приборы измеряют скорость автомобиля снаружи.

Основным прибором для измерения скорости в автомобиле является встроенный спидометр, но он выдает погрешность примерно 5 км/ч и скорость автомобиля может видеть только водитель.

Дополнительным прибором в автомобиле может являться *GPS* спидометр, который с большей точностью через спутники определяет скорость движения автомобиля, а также может транслировать данные о скорости на сторонние приборы.

Внешними приборами для регистрации скорости являются специальные радары, чей принцип действия основан на лазерном излучении, они фиксируют скорость движения автомобиля с минимальной погрешностью. В основном они используются сотрудниками ГИБДД.

Существующие системы мониторинга ТС

На сегодняшний день существует множество компаний, которые предоставляют оборудование для мониторинга транспортных средств, данная об-

ласть насчитывает сразу несколько ведущих поставщиков услуг, одним из которых является компания *Gurtam,* которая признана лидером в своей отросли. Важнейшим продуктом данной компании является *Wialon* — это многофункциональная платформа для ГЛОНАСС/*GPS* мониторинга транспорта, а также любых мобильных и стационарных объектов.

Arvento Mobile Systems – технологическая компания в Турции, специализирующаяся на программировании, разработке и производстве мобильных технологий отслеживания и интегрированных средств обработки и передачи данных.

Техноком – лидирующие позиции на рынке России в области разработки и производства систем ГЛОНАСС/GPS мониторинга транспорта, персонала, датчиков контроля топлива и программного обеспечения высшего уровня для любых компаний и отраслей транспорта, промышленности и сельского хозяйства.

Все вышеперечисленные системы объединяет то, что они используют в качестве спутниковой системы *GPS*-мониторинг (координаты автотранспорта вычисляются на основе данных со спутников системы *GPS*, запущенных и управляемых США) или ГЛОНАСС-мониторинг (определение координат осуществляется на основе российской системы позиционирования ГЛОНАСС). (Рисунок 1)

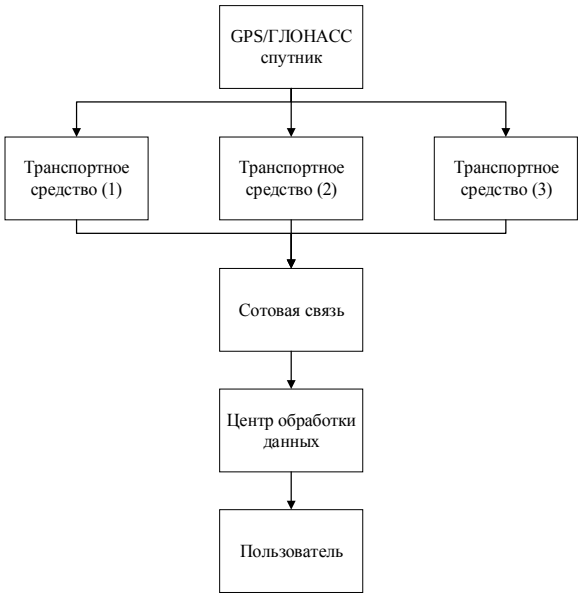


Рис. 1. Принцип работы GPS/ГЛОНАСС мониторинга

На сегодняшний день все оборудование работает с обеими системами, но считается, что *GPS*-мониторинг более точен по сравнению с ГЛОНАСС, благодаря меньшей погрешности при вычислении координат, но принцип работы в обоих системах одинаковый.

На рисунке 1 видно, как *GPS*/ГЛОНАСС спутник транслирует постоянный сигнал на транспортные средства, после чего полученный сигнал обрабатывается и по каналам сотовой связи передается в центр обработки данных, где аккумулируется и наносится на карту. В конечном итоге пользователь получает доступ к этим данным и может видеть траекторию транспортного средства, его скорость, запас топлива и.т.д.

В случае если нет возможности передать сигнал по линиям связи все данные будут записываться на накопитель, заранее встроенный в машину, который вмещает в себя огромный объем памяти и в случае появления сети может выгрузить большую часть данных. (Рисунок 2).

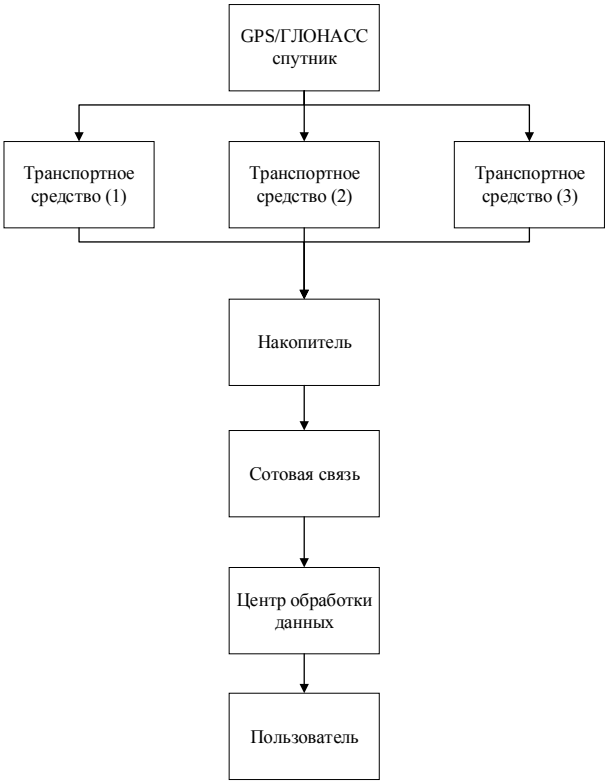


Рис. 2. Принцип работы GPS/ГЛОНАСС мониторинга без доступа к сети

Приложения для мониторинга скорости ТС

Все вышеперечисленные решения объединяет то, что контроль перемещений, скорости и топлива осуществляется при помощи специальной платформы для мониторинга транспортных средств по типу *Wiolan*, в качестве альтернативы предлагается специальное приложение *High-Speed*, в котором у пользователя будет доступ к данным водителя. Основной задачей данного приложения будет данных о скоростном режиме водителя и сопоставление этих данных с текущем ограничением по скорости на участке. Все эти данные будут фиксироваться в базу данных с указанием времени, места, ФИО водителя, марки автомобиля, номеров, возраста водителя. Дополнение существующей БД будет осуществляться каждые 5 минут.

Для наглядного отображения мест фиксирования скорости будут устанавливаться специальные маркеры, которые будут пронумерованы в порядке их создания. Также будет возможность просмотреть весть маршрут водителя. На рисунке 3 представлен общий интерфейс приложения для мониторинга скоростного режима ТС.

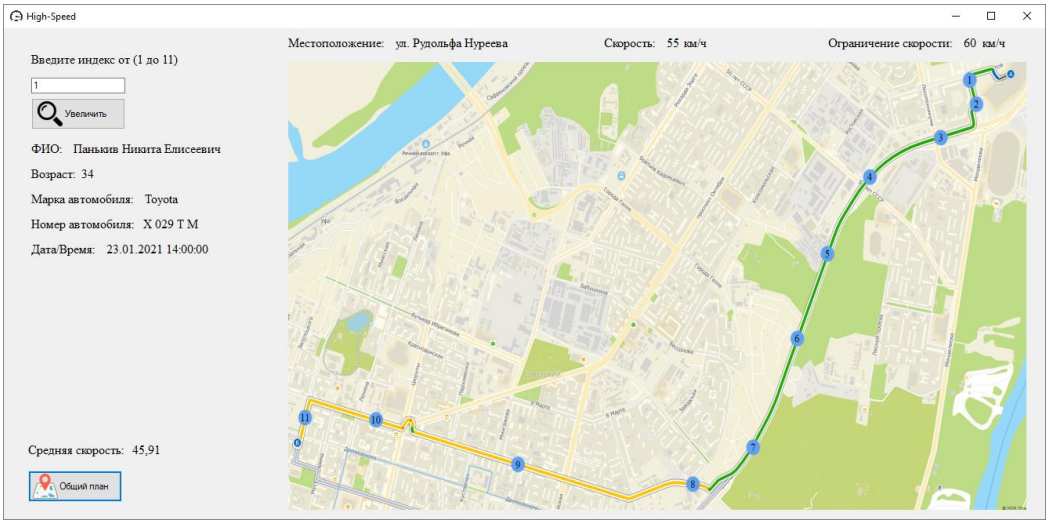


Рис. 3. Отображение пространственных данных водителя ТС

Также в приложении будет возможность увеличить местоположение фиксирования данных с помощью специального *textbox*, в который необходимо ввести индекс от 1 до 11. (Рисунок 4).

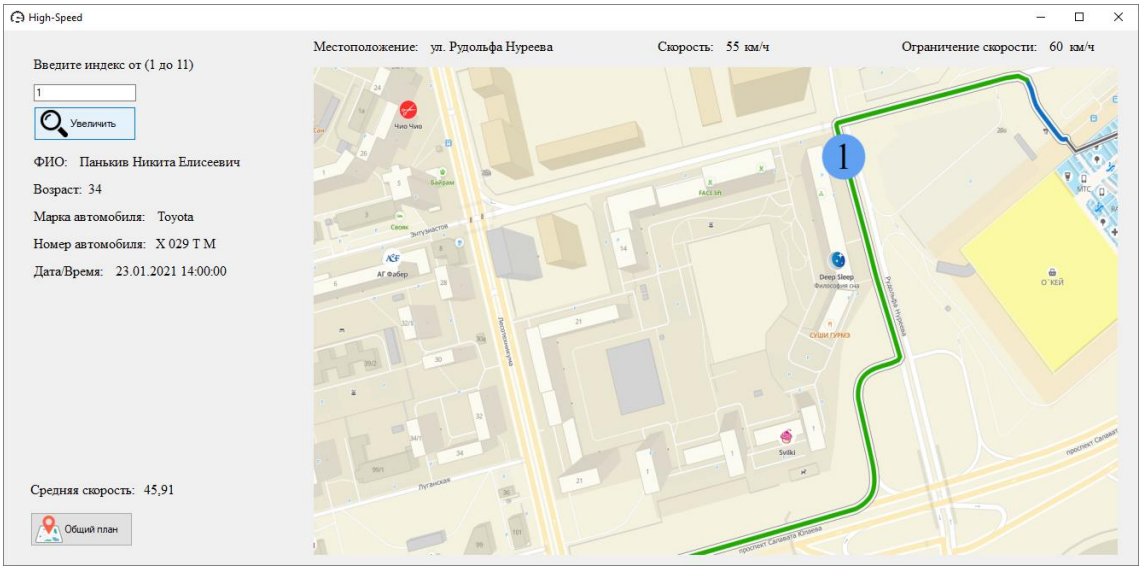


Рис. 4. Увеличенное отображение пространственных данных водителя ТС

Каждый раз после нажатия на данную кнопку происходит сопоставление скоростного режима водителя с действующим ограничением на данном участке. В случае если водитель превысил скорость на экране появится надпись, содержащая всю необходимую информацию о водителе, также будет рассчитано на сколько была превышена скорость на данном участке. Также будет указано место превышения скорости. На рисунке 5 представлен пример появления подобного уведомления.

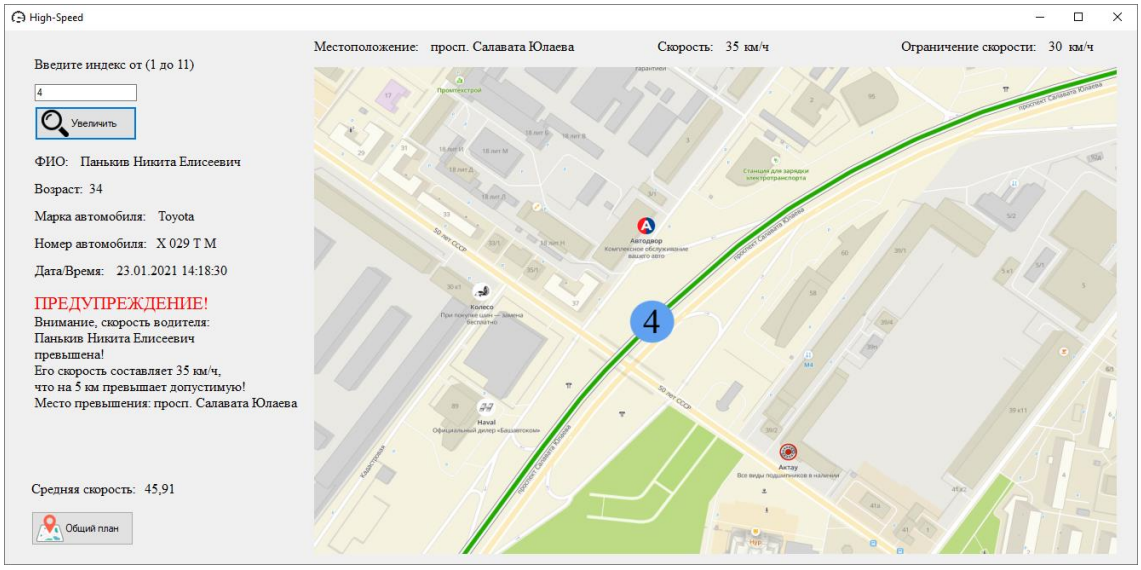


Рис. 5. Пример превышения скоростного режима

Список функций, которые на данный момент реализованы в приложении:

1. Мониторинг местоположения водителя;

2. Просмотр данных водителя ТС;
3. Определение превышения скоростного режима;
4. Просмотр всего маршрута;

На рисунках 6-7 представлена функциональные блок-схемы приложения.

Рис. 6. Определение местоположения

Рис. 7. Контроль скоростного режима

В дальнейшем данная система будет дополняться новыми функциями, будет добавлена возможность самому выбирать маршрут, по которому двигался водитель, для этого в БД будет внесено несколько новых маршрутов.

Также планируется добавить индикатор, оповещающий пользователя о том, что водитель в данный момент находится в пробке или попал в аварийную ситуацию. На рисунке 8 представлена блок-схема данной функции.

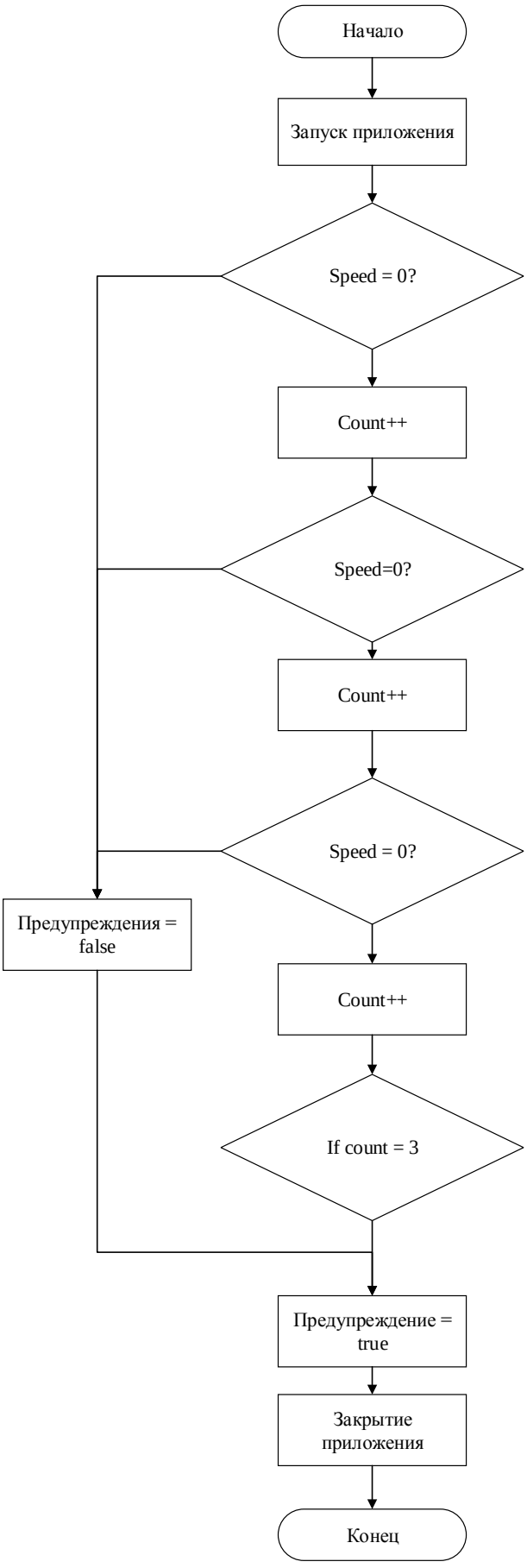


Рис. 8. Мониторинг аварийной ситуации

Заключение

Мониторинг скорости является одной из важнейших функций представимых системами мониторинга транспортного средства т. к. именно скорость сильнее всего влияет на риск возникновения аварийной ситуации.

Подобный подход может быть полезен для крупных систем мониторинга ТС, потому что все данные о водителях, маршрутах и нарушениях будут продолжительное время хранится на сервере, что может быть очень дорого для маленьких систем.

Подобный подход может быть полезен для крупных систем мониторинга ТС, потому что все данные о водителях, маршрутах и нарушениях будут продолжительное время хранится на сервере, что может быть очень дорого для маленьких систем.

Технологии ГИС в данной сфере является ключевой, потому что среди всех компаний, которые предоставляют услуги по мониторингу ТС наиболее успешными являются компании, которые предоставляют наилучшее ГИС-оборудование и чьи системы работают без задержек.

Также можно сделать вывод, что на данный момент самыми успешными системами мониторинга являются системы, которые строятся на основе спутниковой навигации *GPS*, а не ГЛОНАСС. Т.к современное оборудование поддерживает оба варианта, а задержка меньше при использовании *GPS*.

СПИСОК ЛИТЕРАТУРЫ

1. Мавлютов А.Р., Атнабаев А.Ф. Внедрение геоинформационных систем на предприятие // Modern Science. 2020. № 1-2 с. 298-303.
2. Алексеев, А.П. Правила дорожного движения 2019 с иллюстрациями / А.П. Алексеев. - М.: Эксмо, 2018. - 288 с.
3. Перов А.И., Харисов В.Н. ГЛОНАСС. Принципы построения и функционирования (4-е издание, 2010) // М.: Радиотехника, 2010. -801с.

УДК 004.78

Г. К. СУХАРЕВ
cteiiu08080@gmail.com
Науч. руководитель – канд. техн. наук, доц. А. Ф. АТНАБАЕВ

Уфимский государственный авиационный технический университет

МОНИТОРИНГ ТРАНСПОРТНОГО СРЕДСТВА. КОНТРОЛЬ РАСХОДА ТОПЛИВА

***Аннотация*.** В статье описывается, каким образом обеспечивается мониторинг расход топлива транспортного средства, описываются их нюансы, а также, зачем предприятиям нужны в таких задачах ГИС технологии. В ходе решения делаются выводы о технической части, которые связанные с тем, как и где хранятся данные, обрабатываются, какой используется метод создания приложения, обрабатываются, какие используются ГИС технологии.
***Ключевые слова*:** водитель; контроль расхода топлива; база данных; GUI приложение; Web-приложения; отслеживание; мониторинг; технологии; геоинформационные системы; ГИС.

Введение

Контроль расхода топлива – это контроль, позволяющий рассчитывать средний расход топлива на дистанции. Данный вид контроля нужен почти всем автомобилистам, а также и предприятиям для соблюдения отчетности. На момент 2021 года почти все новые автомобили мира оснащаются мини-компьютерами, которые высчитывают тот самый показатель – средних расход топлива.

Данный вид контроля имеет различные методы для мониторинга, например: расчетный метод. Данный метод хорош тем, что он является самым дешевым и походит для всех транспортных средств (далее ТС), которые не имею датчиков топлива. Но, этот метод имеет очень большую погрешность, так как в нем все считается «вручную» и расчеты происходят с учетом нормативным показателям расхода топлива ТС.

Также существуют и другие способы. Один из таких – измерение с помощью штатного датчика топлива. Это один из самых популярных методов на данный момент, так как почти все ТС имею датчики уровня топлива. Плюсы данного метода: низкая цена, меньше погрешность по сравнению с первым методом, не требует дополнительной установки оборудования. К минусам можно отнести: невысокая точность.

Далее идет более сложный метод, с использование уже дополнительного оборудования – погружного датчика. В данном случае устанавливается датчик прямо в бензобак, который напрямую подключен к системе дистанционного мониторинга. Данный метод также подходит к большинству ТС, имеет высокую точность данных. Из минусов: более дорогой из-за установки дополнительных модулей.

Похожий метод на предыдущий – использование проточных датчиков. Данный метод является самым точным из всех, которые были описаны. Имеет минимальную погрешность. Отличия с предыдущим лишь в оборудовании. Плюсы: как было отмечено – самая низкая погрешность. Минусы: более дорогой.

Последний метод – подключение *GPS* трекера к *CAN* шине автомобиля. Данный метод является самым технологичным. *CAN* – это стандарт промышленной сети, ориентированный на объединение в единую сесть различных исполнительных устройств и датчиков. В данном случае *GPS* трекер напрямую соединен с *CAN* шиной автомобиля, что позволяет считывать не только положения уровня топлива, но и положение педали газа, общий пробег, время работы двигателя и так далее.

Все эти методы работают вместе с различными приложениям. Они бывают двух видов: десктопные и *Web*-приложения, в большинстве случаев которых используются геоинформационные системы (далее ГИС). Они могут не только считывает данные с ТС, но и анализировать их и предоставлять различную и необходимую информацию диспетчеру.

Десктопные приложения

О сложном мониторинге расходе топлива для одного автомобиля, который находится в «бытовой» эксплуатации говорить бессмысленно, так как автомобиль один и владелец чаще всего этого автомобиля тоже один. Нет нужды выстраивать в таком положение какие-либо решения для мониторинга расхода топлива. Мониторинг в большинстве случаев нужен предприятиям. Предприятия должны учитывать данный фактор, потому что топливо – один из основных расходов предприятий, занимающиеся грузоперевозками.

К десктопным можно отнести базовые *GUI* приложения. Они могут подходить для всех компаний. Приложения удобны в плане того, что их не нужно арендовать, а это значит – иметь меньше издержек на предприятии и хранить свои данные у себя. То есть, команда программистов или определенная компания пи-

шет для вас такое приложения, и вы можете установить собственный сервер на предприятии, подключится к нему через приложения и следить за ТС. Один из таких примером может послужить решение одного студента, созданного на языке программирования *Python*.

При создании баз данных нужно учитывать все возможные факторы. В данном решения в базе данных существуют четыре колонки данных: время, пробег, объем топливного бака, заправка. Время служит идентификатором, так как оно уникально для таблицы и не может повторяться. Лист является днем. Название таблицы, это месяц и год.

Необходимые данные, такие как пробег и количество топлива в баке, для работы принимаются с *GPS* приемников установленные в ТС и записываются в базу данных. Для этого чаще всего используются сторонние приложения, либо дополнительные модули для *Python*. Заправка пишется вручную через стороннее приложения, либо также можно добавить функцию в *GUI* приложения.

В данном примере *GPS* не используются, так как автор данного приложения не обладает *GPS* приемниками, но интеграция его возможна.

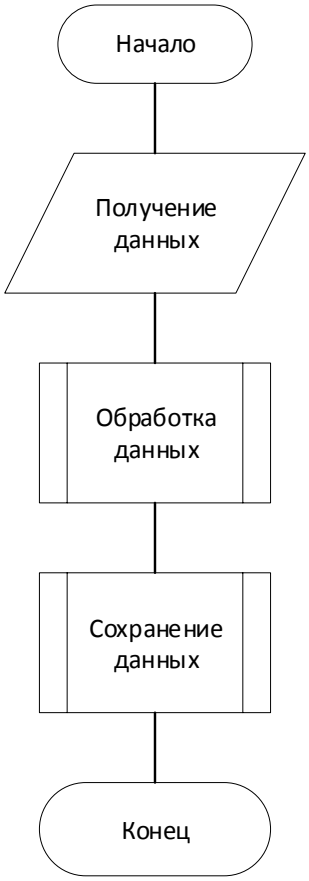


Рис. 1. Блок-схема получения данных.

Для более хорошего понимания представим данные в виде таблице (рис. 3). Существует 4 столбца: время, пробег автомобиля, объем топливного бака, заправка. Для большинства случаях этих данных будет достаточно, особенно для рядового пользователя.

Время	Пробег автомобиля	Объем топливного бака	Заправка
00;00;00	32000	500	0
00;30;00	32124	480	0
01;00;00	32240	460	0
01;30;00	32340	450	0
02;30;00	32340	450	0
02;30;00	32340	450	0
03;30;00	32400	420	0
03;30;00	32490	400	0
04;00;00	32560	380	0
04;30;00	32600	360	0
05;00;00	32624	340	0
05;30;00	32700	320	0
06;00;00	32800	300	0
06;30;00	32900	280	0
07;00;00	33000	260	0
07;30;00	33100	240	0
08;00;00	33200	220	0
08;30;00	33300	200	0
09;00;00	33400	500	330
09;30;00	33500	480	0
10;00;00	33600	469	0

Рис. 2. Данные в таблице

Как видно в данном приложении (рис. 4) мы можем выбирать дату и время, которое нас интересует. После ввода данных можно нажать на кнопку «Вывести данные». Отобразятся значения расхода, пробега и среднего расхода на 100 километров за то время, которое указал пользователь.

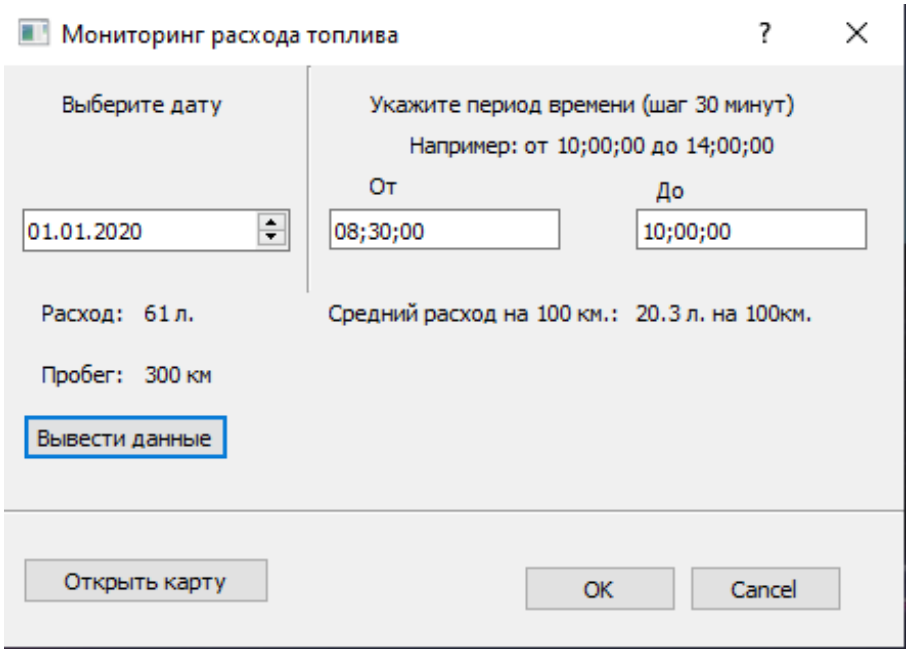


Рис. 3. Приложение мониторинга расхода топлива ТС

Также можно заметить, что внизу слева есть кнопка «открыть карту» (рис. 4). Существуют модули ГИС, позволяющие использовать карту для своих нужд. В данном случае карта служит для предприятий дополнительным контролем за передвижением ТС. Это позволяет лучше обеспечивать работу логистики предприятия, знать, где находиться ТС, где оно было в конкретные период времени.

В приложении был использован модуль *Folium*. Он добавляет возможность использовать карту, создавать объекты на карте. При нажатии на кнопку «открыть карту» можно увидеть карту (рис. 5). Что бы знать местоположения ТС, нужно подключать *GPS* модуль и работать с объектами.

Рис. 4. Встроенная карта в приложение

Часто используются методы, которые спроектировала компания *ESRI*. В их приложениях программного комплекса *ArcGIS* используется язык *Python*, а также есть свой модуль *Arcpy*. С его помощью можно создавать свои карты, имея полный контроль над ее структурой. Но для этого необходима программное обеспечение *ArcGIS* и квалификация в работе с ним.

Web-приложения

Самые популярные приложения для мониторинга ТС – это Web-приложения. Такие приложения имеют сложные структуры, но просты для использования клиентами. Они часто используются маленькими и средними компаниями, где количество ТС может варьироваться от 10 до 50 ТС. Один из основных минусов приложений: данные хранятся не у заказчика, а у владельца при-

ложения на их собственном сервере. Для некоторых компаний, особенно больших, это не приемлемо.

В Web-решениях почти всегда используются сложные технологии. Например, часто за СУБД используют комплекс *Oracle*. Но благодаря таким СУБД данные хранятся в надежном месте, имею целостность, удобство работы с большими данными, возможно хранить большие данные и высокую безопасность.

Что касается внедрения ГИС-технологий, которые необходимы для таких приложений, то иногда заказываю *API* ключи у различных компаний, таких как *Google* или *Yandex*. Но, также в таких проектах используют свои карты, помогает в этом уже знакомая компания *ESRI*.

Рассмотрим такое *Web*-приложение от компании «ТМ: Корпоративные поездки». Тут уже имеются множество разных функций (рис. 6), не только мониторинг расхода топлива.

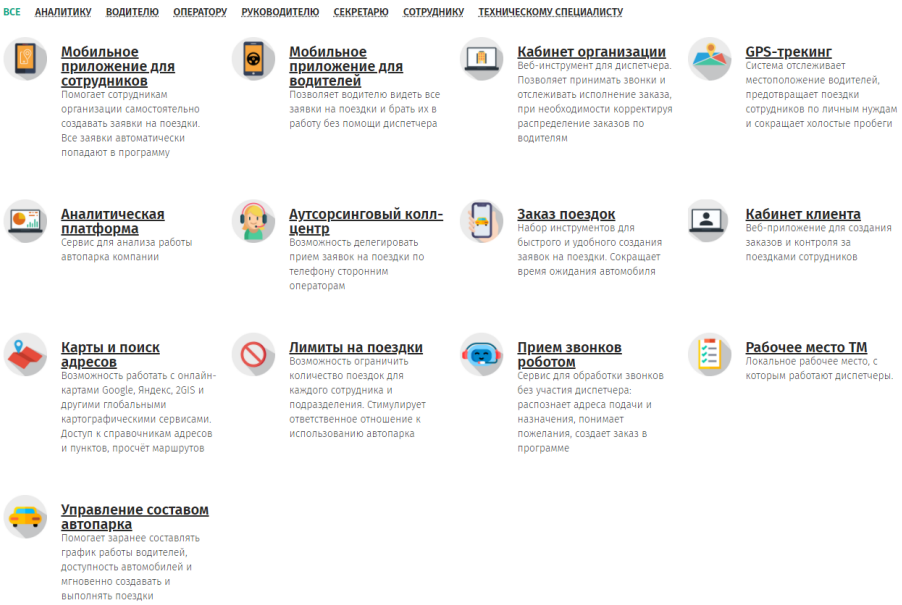


Рис. 5. Функциональные возможности приложения «ТМ: Корпоративные поездки»

Интерфейс имеет простую и эстетичную оболочку, а также можно заметить на больше количество функций (рис. 7). Например: добавить заказ, посмотреть водителей, посмотреть автомобили, посмотреть маршрут следования, посмотреть средний расход топлива, посмотреть пробег и так далее.

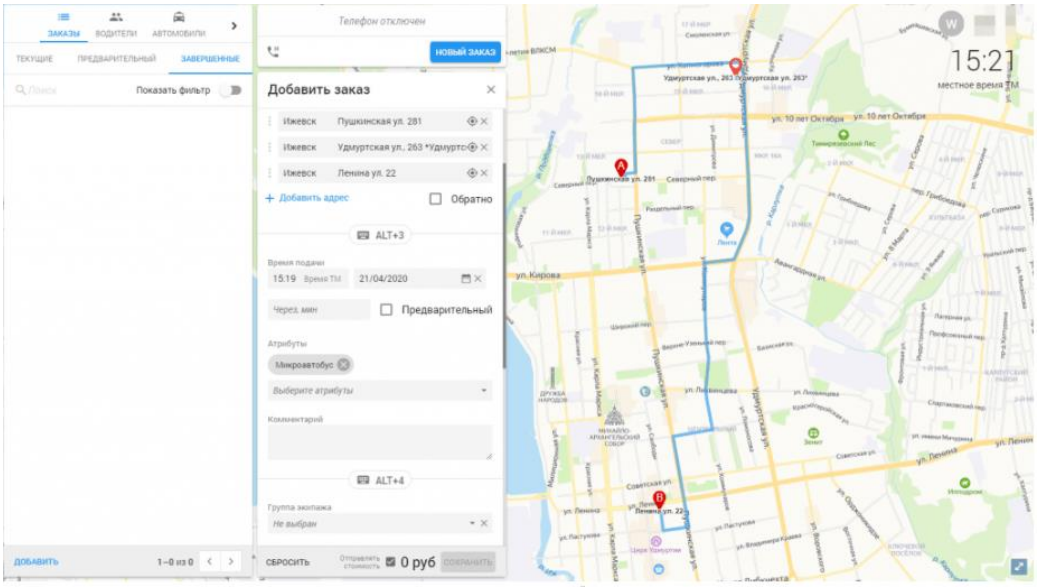


Рис. 6. Интерфейс приложения ТМ: Корпоративные проездки

Также есть еще одно решение от компании «АвтоГРАФ». На их сайте очень хорошо описаны их функциональные способности, в частности – мониторинг расхода топлива. Для этого они используют графики расхода топлива. Графики нужны для удобного просмотра для диспетчера, который может заметить какие-нибудь внештатные ситуации. Например: если за минуту было истрачено более 5 л бензина, то на графике это будет видно очень отчетливо и в базу данных такая информация может пойти как слив бензина. Будет записано, где это было сделано и в каком количестве топлива (рис. 8).

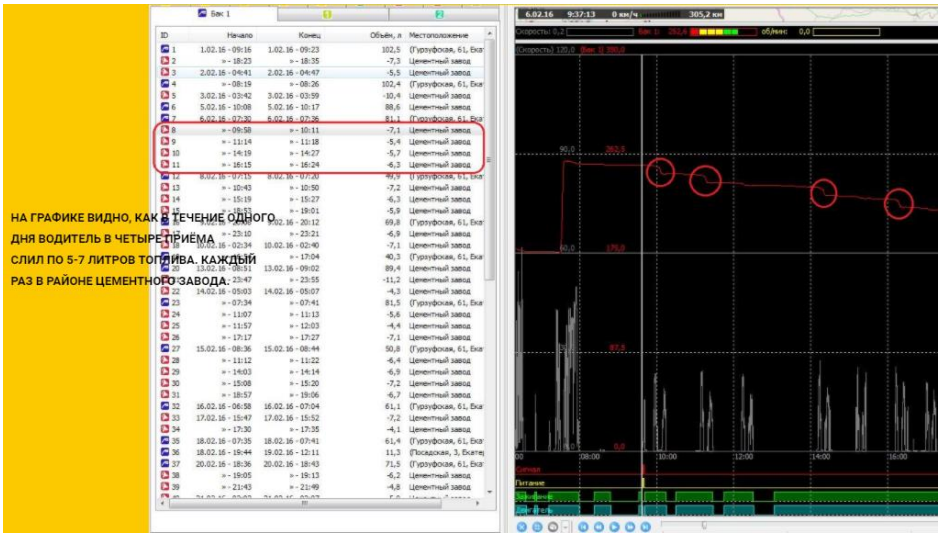


Рис. 7. График расхода топлива от компании «АвтоГРАФ»

Такой функционал служит для предотвращения кражи ресурсов на предприятиях, а также для выявления каких-то проблем с ТС. Водитель мог и не сливать бензин. Могла происходит утечка топлива. Диспетчер это видит и делает определенные выводы. Связывается с водителем и если есть определенная функция, то через приложение.

Можно задаться вопросом, а что, если наоборот произошла резкая прибавка бензина за короткий промежуток времени? Все очень просто. Это означает, что водитель заправил свое ТС и такие данные как место и количество прибавленных значений топлива пойдут в таблицу «Заправки».

У большинства из *Web*-приложений есть свои приложения для смартфона, которые естественно связаны между собой и является очень универсальным решением.

Чтобы пользоваться функциями приложений компаний таких как «ТМ: Корпоративные поездки» или «АвтоГРАФ», требуется приобретать у них подписки. Обычно предлагаются 3 варианта: на месяц, на полгода, на год. Стоимость таких приложения в разных компаниях зависти от функциональных возможностей системы и внутренних издержек компаний. Для выбора того или иного решения зависит от того, что конкретно нужно заказчику, какие функции ему наиболее важны, в каком городе расположена компания, как у них с безопасностью, как правильно считываются и считаются данные. После ответов на эти вопросы и делаются выводы и выбор в сторону конкретного решения приложений компаний.

Вывод

И так можно разобраться, что мониторинг транспортных средств, в частности расхода топлива, является необходимой для предприятий, так как это обеспечивает контроль, что позволяет лучше следить за экономикой компании. Мониторинг расхода топлива содержит в себе огромное количество нюансов, таких как: резкое потеря топлива за короткий промежуток, заправки ТС, которые нужно учитывать при создании или выбора приложений.

Десктопные решения подходят для компаний, которым необходима что бы был полный контроль над приложением, не имея сторонних лиц в управлении, а также полагаться на свои усилия в поддержке работы приложений.

Web-приложения являются самыми продуктивными и популярными в плане мониторинга ТС. Клиентам и работникам с такими приложениями работать намного легче и распространение таких приложений от создателей намного проще, нежели десктопные решения.

Неотъемлемой частью также является ГИС-технологии. Помогают в этом различные модули, например от компании *ESRI,* или приобретения *API* ключей. Благодаря встроенным картам диспетчер, сидя за приложением, может отслеживать местоположение ТС, смотреть его маршруты, заниматься логистикой движении, смотреть, где была произведена заправка ТС, где было утрачено большое количество топлива.

СПИСОК ЛИТЕРАТУРЫ

1. Мавлютов А.Р., Атнабаев А.Ф. Внедрение геоинформационных систем на предприятие // Modern Science. 2020. № 1-2 с. 298-303.
2. Мавлютов А.Р., Атнабаев А.Ф., Вестник науки и образования. 2019. № 2-2 (56). С. 9-13.
3. ТМ: Корпоративные поездки: официальный сайт – Ижевск. – URL: http://tmcorp.pro (дата обращение 10.01.2021). – Текст: электронный.
4. АвтоГРАФ Москва: официальный сайт – Москва. – URL: http://glonassgps.com (дата обращения 10.01.2021). – Текст: электронный.

УДК 004.055

Н. С. ФИЛИППОВ
Serfil1970@gmail.com
Науч. руководов. – канд. техн. наук, проф. О. И. ХРИСТОДУЛО

Уфимский государственный авиационный технический университет

ГЕОПАРКИ ЮНЕСКО. ЗНАЧЕНИЕ ГЕОПАРКОВ В ГИС

Аннотация. В статье описывается, какие ГИС задачи решаются геопарками, описываются возможности интерактивных карт, а также, доказывается нужность в таких задачах ГИС технологий. В ходе решения делаются выводы о технической части, связанные с возможностями разных API, какие используются ГИС технологии.
***Ключевые слова*:** геопарки; ЮНЕСКО; ГИС; API; карта; геозиты; геология; гео-занятия; геоинформационные системы.

Введение

Глобальная сеть геопарков — это международная неправительственная некоммерческая добровольная организация, которая является площадкой для взаимодействия геопарков, действующая согласно правилам, регламентируемым ЮНЕСКО. В ее основе лежит изучение и построение связи между людьми и Землей, где объекты и ландшафты международного геологического значения управляются с использованием целостной концепции защиты, образования и устойчивого развития. Георазнообразие является фундаментом всех экосистем и основой взаимодействия человека с ландшафтом. Глобальный геопарк ЮНЕСКО включает ряд геологических объектов наследия особой научной важности, редкости или красоты. Чтобы стать одним из геопарков ЮНЕСКО нужны международные рецензируемые опубликованные исследования, проводимые на геологических объектах в пределах района. Эксперты проводят глобальную сравнительную оценку, чтобы определить, представляют ли геологические объекты международную ценность.

Цель – защита и сохранение территориального геологического наследия и создание культурно-экологического устойчивого развития территории.

Состояние в мире

С тех пор весь современный мир строит геопарки, чтобы сохранить геологическое наследие, облагородить при помощи новейших восстановительных, научно обоснованных работ регионы. Геопарки созданы для просвещения людей, чтобы они имели чувство бережного отношения к окружающей среде.

ЮНЕСКО обеспечивает секретариат глобальных геопарков, способствует и стимулирует глобальную «сеть» и является соорганизатором международных конференций по геопаркам. Секретариат выполняет три основные задачи в отношении глобальных геопарков ЮНЕСКО: Строительство, улучшение управления и продвижение.

Геопарки мира

«Янган-тау»

Единственный геопарк ЮНЕСКО располагающийся на территории Российской Федерации в Республике Башкортостан.

Рассмотрим предложенную карту чуть ближе. Для ее визуализации используется *API scanex*, в котором есть возможность масштабирования, оставления меток, выделения площади, фильтрация по ключевым объектам и выбор подложки для карты, ознакомление с информацией в балунах (рис. 1).

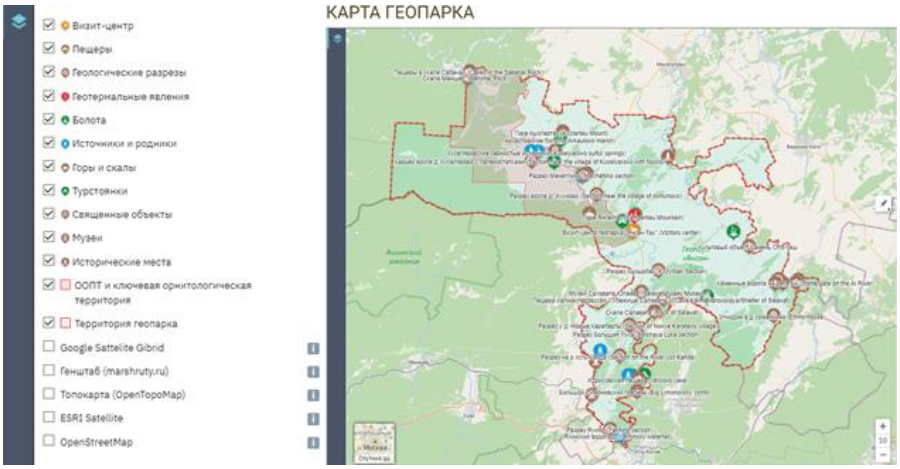


Рис. 1. Интерактивная карта Янган-тау

«Beaujolais»

Один из семи геопарков ЮНЕСКО располагающийся во Франции, самый популярный геопарк в стране

Для ее визуализации используется *Google Maps* (рис. 2), в котором есть возможность масштабирования, фильтрация по ключевым объектам, просмотр улиц, содержит дополнительную вкладку, для удобного перемещения на страницу с геозитами и балуны для просмотра информации о метке. В качестве дополнения предложена карта гео-занятий, чтобы люди знали, чем можно заняться в данном геопарке (рис. 3).

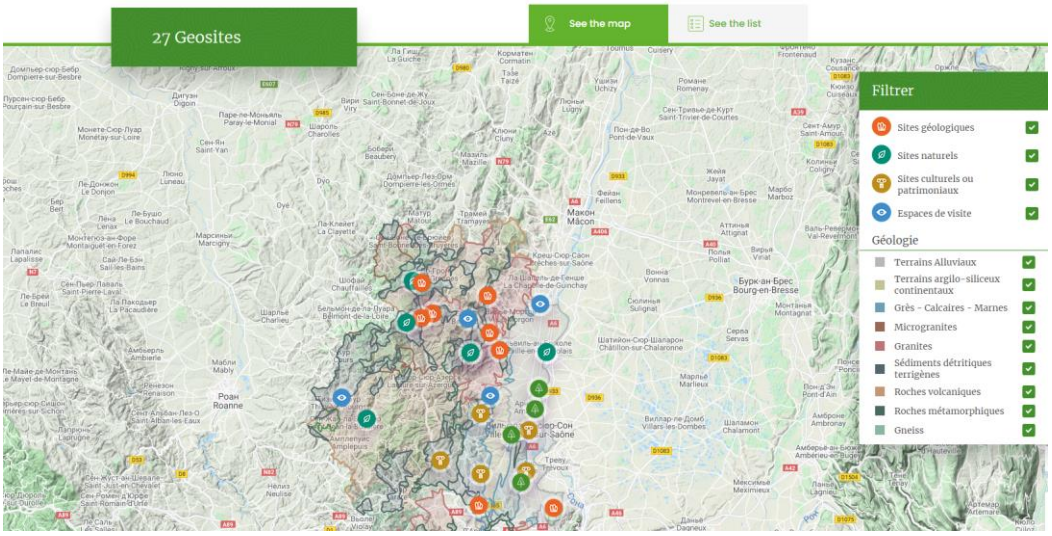


Рис. 2. Интерактивная карта *Beaujolais*

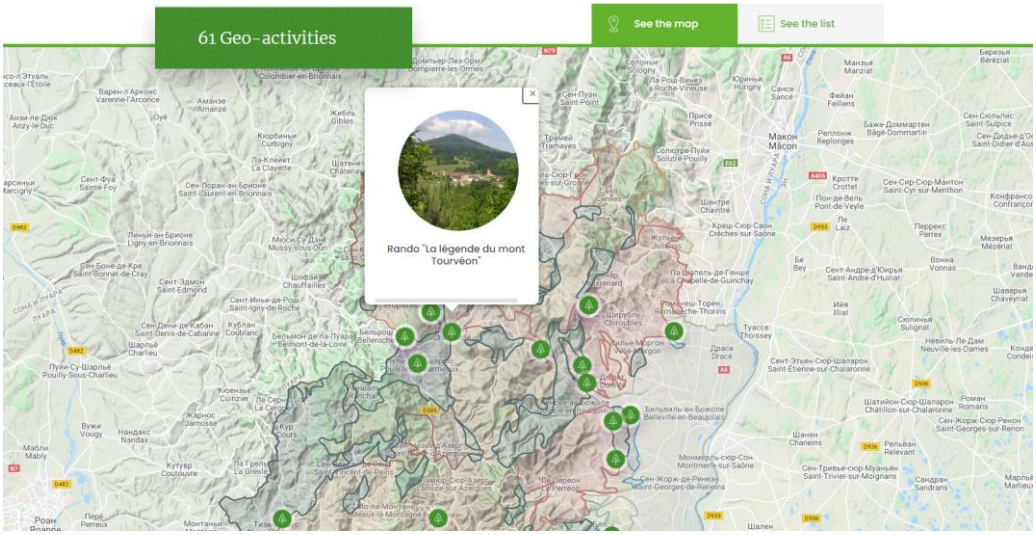


Рис. 3. Карта гео-занятий

«Psiloritis»

Один из шести геопарков ЮНЕСКО располагающийся в Греции.

Для ее визуализации используется *Staridas Geography* (рис. 4), в котором есть возможность масштабирования, фильтрация, кнопка с возвратом на начальное положение, есть система кластеров, есть возможность просмотра панорам для некоторых мест и содержит геологическую карту (рис. 5). В фильтре можно подробнее узнать о геозитах при нажатии на них.

Рис. 4. Интерактивная карта *Psiloritis*

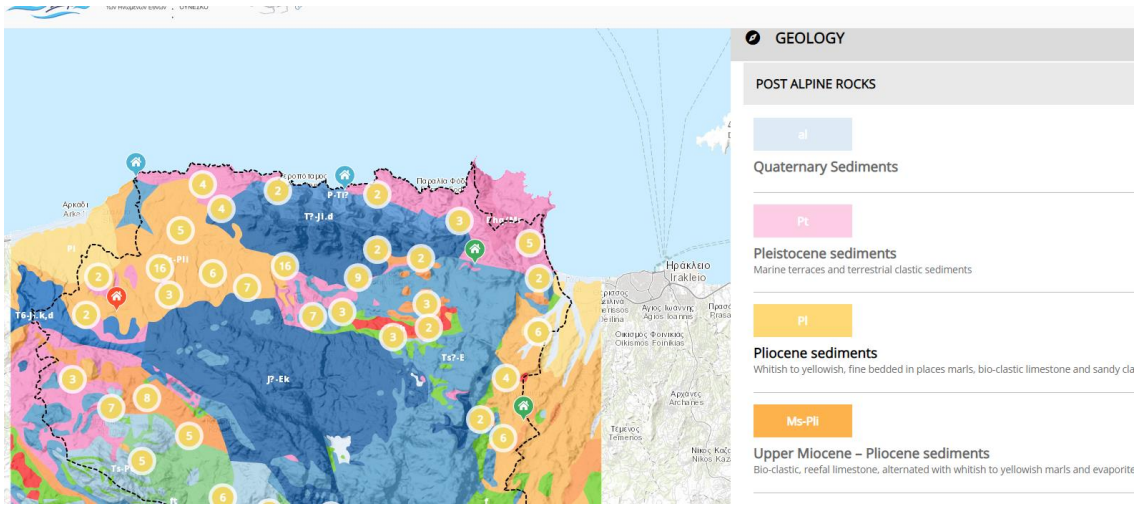


Рис. 5. Геологическая карта

Заключение

И так можно разобраться, что использование ГИС технологий неразрывно связано с геопарками, с их визуализацией, в частности. Наилучшим образом отображена карта геопарка расположенного в Греции, за счет того, что он

сможет угодить и туристам, и геологам. Следует отметить возможность знакомства с геозитами для пользователей, намеревающихся посетить парк, а также карты гео-занятий и геологическую карту.

СПИСОК ЛИТЕРАТУРЫ

1. «Frequently asked questions about UNESCO Global Geoparks – General information, definitions, governance and framing issues» // UNESCO Global Geoparks. 2021. [Электронный ресурс]. URL: https://en.unesco.org/sites/default/files/4_drupal_faqs_general_version_5_november_clean.pdf/ (Дата обращения: 09.07.2021).
2. Корф Е.Д. «Геопарк как платформа эффективного взаимодействия общества и природы» / Е. Корф // Наука и туризм: стратегии взаимодействия. 2015. № 4. с. 5-9.
3. Velazquez V. «Geotourism in the Salesópolis-Caraguatatuba Trail, São Paulo, Brazil: A Possibility to Utilize Geological Elements for Sustainable Development» / V. Velazquez // Journal of Environmental Protection. 2013. №4. pp. 1044-1053.

УДК 332.14:004.9

А. М. ХАСАНОВ
aydarhasanov99@mail.ru

Уфимский государственный авиационный технический университет

ВОЗДЕЙСТВИЕ КОСМИЧЕСКОЙ ПОГОДЫ НА МАГИСТРАЛЬНЫЕ ЛИНИИ ЭЛЕКТРОПЕРЕДАЧ СКАНДИНАВСКОГО РЕГИОНА

Аннотация. В этой работе предложен алгоритм расчета индексов геомагнитно-индуцированных токов (ГИТ) в скандинавском регионе. Данный алгоритм, основан на языке программирования Python. Предложенный алгоритм предоставляет нам полезный инструмент для обеспечения предварительной оценки риска космической погоды, связанной с деятельностью ГИТ в скандинавской энергетической сети.
Ключевые слова: ГИТ; космическая погода; временные ряды.

Введение

Магнитосферные и ионосферные электрические токи создают на поверхности Земли вариации геомагнитного и геоэлектрического поля, вызывающие так называемые геомагнитно-индуцированные (паразитные) токи (ГИТ) в длинных (многокилометровых) проводящих системах. Если в магнитоспокойное время эти вариации незначительны, то в магнитоактивные периоды ГИТ могут достигать десятки и даже сотни ампер, влияя на работу систем энергоснабжения, а также целого ряда других наземных технических систем, в которых длинные проводящие линии являются необходимым компонентом (трубопроводы, линии связи, железные дороги). Наиболее известной в этом смысле стала авария, вызванная магнитной бурей 13 марта 1989 г., в ходе которой 6 миллионов человек и большая часть промышленности канадской провинции Квебек на 9 часов остались без электричества.

Хорошо известно, что энергетические сети в высоких широтах уязвимы к воздействию космической погоды. Геомагнитно-индуцированные токи (ГИТ) протекают в линиях электропередачи в результате «геоэлектрических» полей и связанных с ними вариаций геомагнитного поля по закону Фарадея. В этой статье исследуются и классифицируются ранее задокументированные проявления активности ГИТ из регионов по всему миру по их воздействию на близлежащие

энергетические сети. Фильтр частотной области, который производит индекс, представляющий активность ГИТ, применяется к данным геомагнитного поля, записанным в местах вблизи документированной активности ГИТ, чтобы определить пороговые значения уровня риска «индекс ГИТ».

Набор данных

Данные, по которым мы будем строить полярное сияние мы будем брать с сервиса https://space.fmi.fi. Данный сервис расшифровывается как: Центр наблюдений за космосом и Землей. Этот сервис занимается исследованиями космоса и наблюдениями за Землей (ЕО), развитием космических технологий и использованием космических данных и данных ЕО для набора услуг.

Описание алгоритмов

Для начала скачиваем данные магнитометров из 13 обсерваторий (ABK, AND, IVA, KEV, KIL, KIR, MAS, MUO, NOR, PEL, SOD, SOR, TRO), которые находятся на Скандинавском полуострове. Данные магнитометров предоставлялись ежеминутно с 01.01.2015 по 31.12.2015 в виде временных рядов (в текстовых файлах). Перед работой с рядами, в них необходимо найти отклоняющиеся значения (99999.9 и т.д.), удалить эти значения и выполнить линейную интерполяцию.

Данные магнитометров из обсерваторий, расположенных вблизи наблюдаемого увеличения активности сети ГИТ, были обработаны для получения ассоциированных индексов ГИТ с использованием следующего фильтра частотной области, определенного Marshall et al.

$$Z(f) = \sqrt{\frac{f}{f_N}}\, e^{i\frac{\pi}{4}}$$

где f - частота, а f_N - частота Найквиста. Индексы ГИТ, полученные с помощью уравнения (1), представляют собой прокси для горизонтальных компонент геоэлектрического поля (предполагая горизонтальное плоское волновое поле, падающее на однородную проводящую Землю). Как правило, в течение полного дня 1 мин отбирались однокомпонентные (например, x-компонентные) данные

вариометра геомагнитного поля, которые обрабатывались с использованием уравнения (1) для получения соответствующих индексов ГИТ для каждого дня в соответствии со следующим. Пусть x(t) и y(t) представляют данные временных рядов для геомагнитного поля регистрируется в географических направлениях север- юг (НС) и Восток- Запад (РЭБ) соответственно. Если x(t) и X(f), а также y(t) и Y(f) представляют собой пары преобразований Фурье, то

$$\mathrm{GIC_x}(t) = |\mathrm{FFT}\{\mathrm{Y(f)Z(f)}\}^{-1}|$$

$$\mathrm{GIC_y}(t) = |\mathrm{FFT}\{\mathrm{X(f)Z(f)}\}^{-1}|$$

где $\mathrm{FFT}\{\}^{-1}$ представляет собой обратное преобразование Фурье величины внутри скобок, Z(f) - фильтрующая функция уравнения (1), а | | обозначает абсолютное значение комплексной величины, возвращаемой обратным преобразованием.

Далее считываем данные из станции ABK, в котором находятся временные ряды. Найдем производные по рядам X и Y.

Далее высчитываем индексы GICx и GICy, и построим графики индекса GICx и производной по ряду Y на одном полотне, а также индекса GICy и производной по ряду X на одном полотне. Потом находим корреляцию Пирсона между графиками производной по ряду X и GICy, а также Y и GICx. Корреляция получилась 0.99. Результаты на рис. 1.

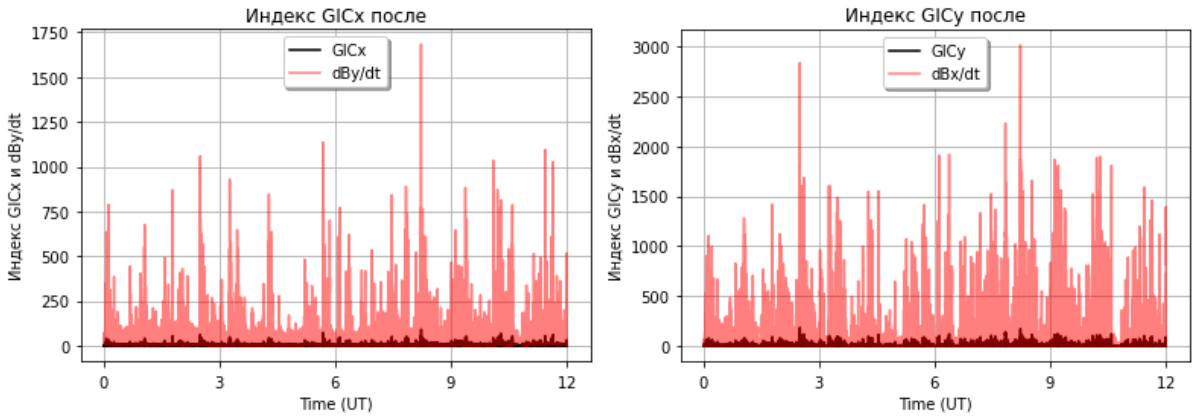


Рис. 1. Графики индексов GICx и GICy

Аналогичные действия проводим со всеми оставшимися обсерваториями.

Наконец, построим изолинии GICx и производной по Y, а также изолинии GICy и производной по X региона за время 23:15-23:19 17.03.2015 и сравним результаты. Результаты показаны на рис. 2-3.

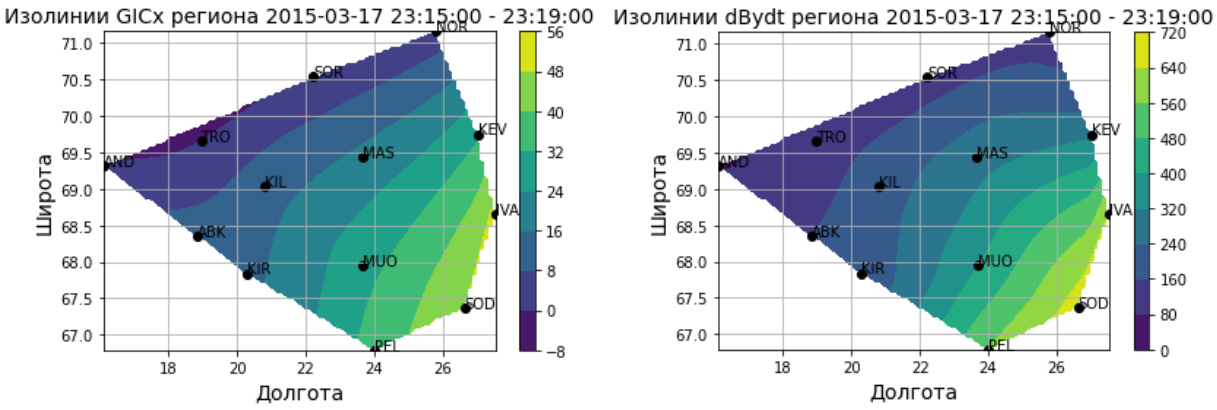


Рис. 2. График изолинии GICx и dBy/dt

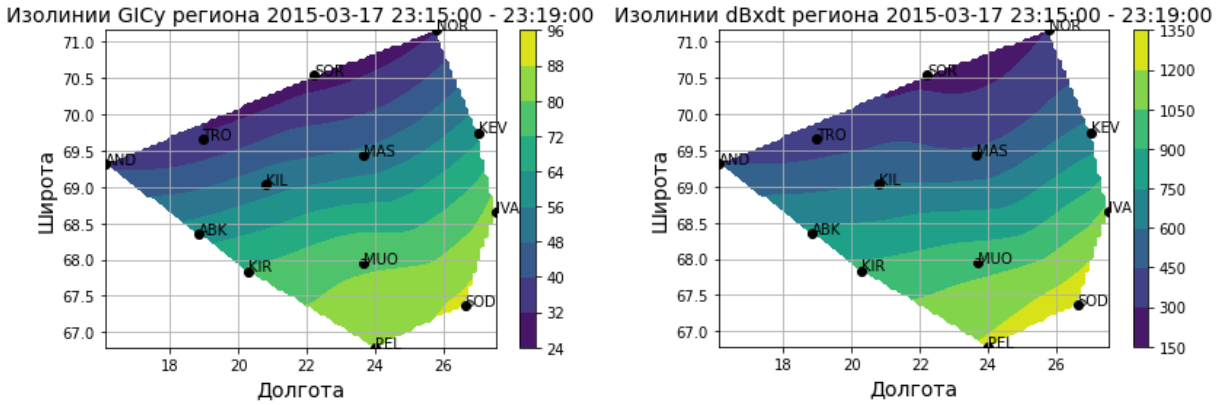


Рис. 3. График изолинии GICy и dBx/dt

Заключение

В данной статье были рассчитаны индексы GICx и GICy в скандинавском регионе, а также были приведены алгоритмы построения изолиний, показывающих распределение индексов по региону на языке программирования Python. Данные о геомагнитном поле с магнитометрических станций, расположенных рядом с задокументированными явлениями, обрабатывались с использованием «фильтра частотной области ГИТ» для получения соответствующего индекса ГИТ, обеспечивающего прямую связь между геофизическими явлениями и технологическими воздействиями. Анализ возникновения неисправностей и индекса ГИТ был использован для получения относительной вероятностной мо-

дели и связанных с ней уровней риска для электрических сетей в результате деятельности ГИТ. Оценка величин ГИТ в линиях электропередач разного класса напряжений позволит исследовать устойчивость систем электроснабжения при геомагнитных бурях различной интенсивности.

СПИСОК ЛИТЕРАТУРЫ

1. Воробьев А.В., Пилипенко В.А., Еникеев Т.А., Воробьева Г.Р., Христодуло О.И. Система динамической визуализации геомагнитных возмущений по данным наземных магнитных станций Научная визуализация. 2021. Т. 13. № 1. С. 162-176.
2. Воробьев А.В., Пилипенко В.А., Еникеев Т.А., Воробьева Г.Р. Геоинформационная система для анализа динамики экстремальных геомагнитных возмущений по данным наблюдений наземных станций Компьютерная оптика. 2020. Т. 44. № 5. С. 782-790.
3. Воробьев А.В., Воробьева Г.Р. Подход к оценке относительной информационной эффективности магнитных обсерваторий сети intermagnet Геомагнетизм и аэрономия. 2018. Т. 58. № 5. С. 648-652.
4. Воробьев А.В., Воробьева Г.Р. Веб-ориентированная 2d/3d-визуализация параметров геомагнитного поля и его вариаций Научная визуализация. 2017. Т. 9. № 2. С. 94-101.
5. Воробьев А.В., Пилипенко В.А., Сахаров Я.А., Селиванов В.Н. Статистические взаимосвязи вариаций геомагнитного поля, аврорального электроджета и геоиндуцированных токов Солнечно-земная физика. 2019. Т. 5. № 1. С. 48-58
6. Воробьев А.В., Пилипенко В.А., Решетников А.Г., Воробьева Г.Р., Белов М.Д. Веб-ориентированная визуализация геофизических параметров в области аврорального овала Научная визуализация. 2020. Т. 12. № 3. С. 108-118.
7. Воробьев А.В., Воробьева Г.Р. Визуализация геомагнитных вариаций в частотно-временной области информационного сигнала Научная визуализация. 2019. Т. 11. № 2. С. 143-155

УДК 004

Д. Д. ХОРОШИЛОВА
dariya_d_x@mail.ru
Науч. руководов. – канд. техн. наук, доц. А. Ф. АТНАБАЕВ

Уфимский государственный авиационный технический университет

ПОДСЧЕТ ВЫСОТЫ СНЕЖНОГО ПОКРОВА НА ОСНОВЕ МЕТЕОРОЛОГИЧЕСКИХ ПАРАМЕТРОВ

Аннотация. В статье рассматриваются основные характеристики снежного покрова, обосновывается необходимость расчета его высоты. Внимание уделяется актуальным методикам подсчета высоты снежного покрова, а также целесообразности использования методик, основанных на использовании основных метеорологических параметров.
Ключевые слова: снежный покров; геоинформационные системы; SnoWE; SNOW-17; климат.

Роль снежного покрова, как элемента формирования климата является одной из самых главных, особенно для территории Российской Федерации. Можно выделить несколько основных областей, в которых он оказывает явное влияние на окружающую среду.

Слой снега является сезонным барьером между атмосферой и поверхностью почвы. Отражая солнечный свет, поверхность снежного покрова охлаждается, но в то же время сохраняет достаточно высокую температуру на поверхности почвы под ней, предостерегая ее от глубокого промерзания. От высоты снежного покрова напрямую зависят его теплопроводные свойства, благодаря которым растения переживают зимовку, а многие виды мелких грызунов продолжают жизнедеятельность даже в зимний период.

Область влияния снежного покрова не ограничивается почвой, он способен поглощать азотистые соединения, адсорбировать пыль и вредные газы из воздуха, охлаждать и иссушать прилегающие воздушные слои.

В гидрологических процессах снег занимает ключевое место, так как определяет величину годового стока, уровень весеннего половодья и ледовый режим рек. Водные запасы, накапливаемые в зимний сезон в снежном покрове, являются основным источником питания большинства рек России.

Физическое строение снежного покрова разнообразно, так как имеет слоистый характер, а потому очень зависит от ряда факторов: рельефа, солнечной радиации, частоты и свойств снегопадов, ветра и прочих атмосферных процессов.

Основными параметрами снежного покрова являются:

– отражающая способность: свежевыпавший снег способен отражать около 95% солнечного излучения, а старый в период снеготаяния - до 20-40% [1];

– плотность: от 10 до 700 кг/^{3}, в зависимости от вида выпавшего снега, рельефа, сезона, продолжительности и глубины залегания слоев. Для определения данной характеристики для снежного покрова в целом, устанавливают среднюю величину между изученными слоями;

– пористость, которая является следствием плотности. Характеризует воздухопроницаемость и водопроницаемость снега;

– запас воды (SWE) и др.

Задаче моделирования снежного покрова посвящено множество исследований, методики расчетов эволюционируют благодаря технологиям. В зависимости от поставленной задачи, можно привлечь разные подходы, в одних из которых применяют полное описание процессов формирования и разрушения снежных покровов, а в других используют значительные упрощения системы, ограничиваясь лишь несколькими простыми параметрами.

В свою очередь, методики определения и расчета параметров разделяют по способу сбора и обработки данных: с применением искусственных спутников Земли и специализированной аппаратуры, а также с помощью метеорологических наблюдений.

Одним из самых экономичных способов измерения высоты снежного покрова является применение ультразвуковых приборов. Все более востребованными становятся лидарные наблюдения – бортовые и наземные. Такой вид наблюдений обеспечивает детальное представление снежного покрова [2], позволяют обеспечить ежедневную обработку данных, однако их применение чаще всего возможно лишь на государственном уровне, в крупных исследовательских центрах.

Технологии оценки снежных запасов на основе метеоданных начали активно развиваться в 2012 году трудами Е.В. Кузьминой и М.М. Чумакова [3]. На территории России расположена густая сеть синоптических метеостанций, обеспечивающих регулярное поступление стандартных метеорологических наблюдений. На базе Гидрометцентра России была создана технология «SnoWE» в рамках деятельности международного консорциума COSMO для вычисления полей запаса воды и плотности снежного покрова на основе значений температуры воздуха, влажности, скорости ветра и осадков.

Другая модель динамики снежного покрова SNOW-17 была разработана в Национальной службе погоды США и передана Гидрометцентру России в ходе двустороннего сотрудничества по проблемам океана и атмосферы. Модель позволяет рассчитать накопление снежного покрова, плотность, таяние, перемещение и отдачу воды из толщ снежного покрова. Стоит отметить, что SNOW-17 рассматривает снежный покров как один слой, несмотря на многослойность реальной физической модели.

Первым делом выделяются жидкие и твердые осадки, в зависимости от температуры воздуха. Далее рассчитывается аккумуляция снежного покрова, причем плотность свежевыпавшего снега ρ_n также зависит от температуры воздуха t_a [4]. На основе значений слоя твердых осадков P_n и плотности снега ρ_n рассчитывается высота снежного покрова [4].

Итак, задача подсчета высоты снежного покрова является очень важной и не теряет своей актуальности ввиду уникального течения каждого зимнего сезона. Разработка систем, производящих описанные вычисления, открывает перспективы накопления сезонных данных высоты снежного покрова для обширных территорий страны, которые в свою очередь могут быть применены для анализа и решения таких задач, как расчет водных запасов, теплопроводности и влагонасыщенности снежного покрова, определения снеговой нагрузки и многих других. Кроме того, в период снеготаяния возникают особенно возникает риск опасных гидрологических явления − наводнений и ледовых заторов, наносящих значительный материальный ущерб.

СПИСОК ЛИТЕРАТУРЫ

1. http://snowavalanche.ru/uchebnik/osnovnye-faktory-lavinoobrazovanija/sneg/#:~:text=Альбедо%20снежного%20покрова%20(отношение%20количества,составляет%20от%200%2C95%20до%200%2C80
2. http://method.meteorf.ru/publ/tr/tr368/tr368htm/08.htm
3. Kazakova E.V., Chumakov M.M., Rozinkina I.A. Model' dlya rascheta kharakteristik snezhnogo pokrova na osnove dannykh nablyudenii standartnoi meteorologicheskoi seti [Model for snow cover characteristics calculation based on standard net meteorological observations]. Trudy Gidromettsentra Rossii [Proceedings of Hydrometcenter of Russia], 2014, vol. 352, pp. 85-102. [in Russ.].
4. http://method.meteorf.ru/publ/tr/tr360/simon.pdf

УДК 332.14:004.9

А. Р. ШАКИРОВ
easyfreeze124@gmail.com

Уфимский государственный авиационный технический университет

ИНФОРМАЦИОННАЯ СИСТЕМА ДЛЯ ВИЗУАЛИЗАЦИИ ПОЛЯРНОГО СИЯНИЯ, НАХОЖДЕНИЕ ЦЕНТРА И СРЕДНЕЙ ЛИНИИ АВРОРАЛЬНОГО ОВАЛА

Аннотация. В данной работе предложен алгоритм отображения полярного сияния в геоинформационном продукте *ArcGis*, определения центра полярных сияний, а также средней линии аврорального овала. Этот алгоритм, основанный на языке программирования *python*. Предложенный алгоритм предоставляет нам полезный инструмент для понимания, в каких местах будет видно полярное сияние и с какой интенсивностью.
Ключевые слова: полярные сияния; ArcGIS Pro; визуализация; центр полярного сияния; средняя линия аврорального овала.

Введение

Авроральные овалы вокруг магнитных полюсов Земли в обоих полушариях образуются в результате столкновений между магнитосферными энергетическими частицами, осаждающимися в полярную область через линии магнитного поля Земли, и атомами и молекулами в верхних слоях атмосферы. Вариации полярного сияния тесно связаны с ионосферой, магнитосферой, солнечным ветром и связями между ними. Кроме того, конфигурация границ полярных сияний является хорошим индикатором связи солнечного ветра, магнитосферы и ионосферы.

Глобальная форма аврорального овала, определяемая его экваториальными и полярными границами, является непосредственным наблюдателем важных физических процессов в магнитосфере. Когда межпланетное магнитное поле (IMF) направлено на юг, повторное соединение на дневной магнитопаузе приводит к тому, что замкнутый поток становится открытым, что приводит к накоплению открытого потока в магнитосфере и увеличению площади полярной шапки. Отмечается, что понимание общей формы и вариаций границ овала полярного сияния важно для изучения взаимодействия солнечного ветра с маг-

нитосферой и связи ионосферы с внутренней магнитосферой во время авроральных суббурь.

Классификация полярных сияний, которая была разработана комитетом по решению Ассоциации геомагнетизма и аэрономии Международного союза геофизики и геодезии и была она введена с 1 января 1964 года. Полярное сияние можно классифицировать следующими характеристиками: формой, активностью, положением, характером, цветом, структурой, яркостью.

Набор данных

Данные, по которым мы будем строить полярное сияние мы будем брать с сервиса *services.swpc.noaa.gov*. Данный сервис расшифровывается как: Национальное управление океанических и атмосферных исследований. Этот сервис занимается геодезическими и метеорологическими исследованиями.

Описание алгоритмов

1. Отображение полярного сияния

Для начала нам нужно считать данные с сайты, который упомянут в разделе набора данных. После того, как у нас имеются наши данные, а именно долгота, широта и интенсивность полярного сияния, их необходимо внести в наш проект. Для этого мы создадим точечный слой, в котором будут находиться координаты нашего полярного сияния и интенсивность свечения полярного сияния, которое может быть в диапазоне от одного до ста процентов.

На данном этапе необходимо отредактировать данный точечный слой. Для начала присвоим каждой точке двумерное расположение, ведь если точки будут находиться в трехмерном расположении, то они и будут иметь свойства трехмерного объекта, то есть будут иметь тень, из-за которой при определенном угле обзора мы не будем видеть данные точки. Также укажем размер данных точек и зададим и им отображение по уникальному значению, а именно по интенсивности свечения полярного сияния.

Далее, используя инструменты интерполяции, создадим из нашего набора точек растр, который уже и будет отображать наше полярное сияние. Получившийся сплайн необходимо сгладить. После сглаживания растра, необходимо

разграничить наши значения по отображению полярного сияния. Для этого создадим линейный слой изолиний, который строится по растровой поверхности. Для создания этих изолиний необходимо также указать какой будет интервал между соседними изолиниями. Создадим изолинии, которые будет разграничивать наше сияние по определенным значениям. Результат отображения полярного сияния показан на рис. 1.

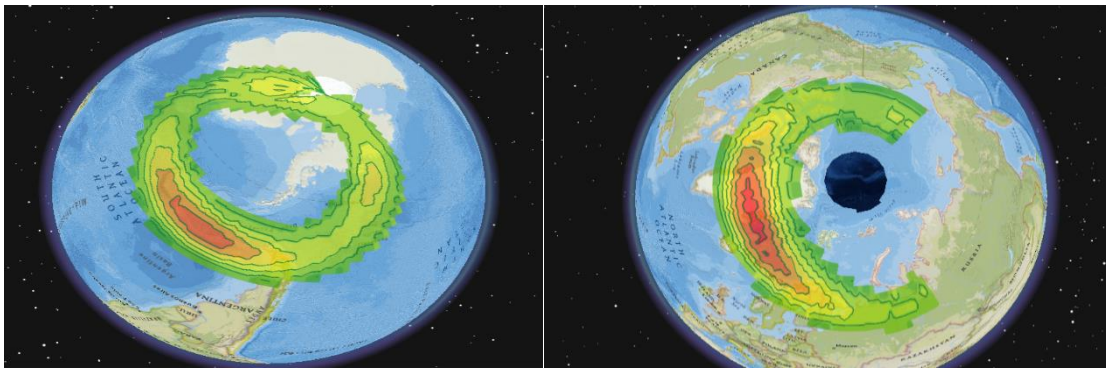


Рис. 1. Визуализация полярного сияния

2. Поиск центра полярного сияния

Для поиска центра полярного сияния используем авроральный овал, для начала создадим класс пространственных объектов, содержащий полигоны, которые представляют собой минимальные области, включающие каждый входной объект или каждую группу входных объектов. Для всех входных объектов будет создан один выходной полигон. Атрибуты входных объектов не будут поддерживаться в выходном классе объектов, используя наименьший выпуклый полигон, охватывающий входной объект, также для этого полигона все входные объекты будут рассматриваться как одна группа.

Далее создадим класс пространственных объектов, содержащий точки, созданные из представительных местоположений входных объектов. Данный класс будет иметь только одну точку, которая и будет являться нашим центром полярного сияния на определенном земном полушарии.

Если же рассматривать центры полярного сияния в течение суток, где каждая точка будет браться через каждый час, то будет заметно, что двадцать

четыре точки проходят путь, напоминающий окружность. Результат поиска центра показан на рис. 2.

Рис. 2. 24 центра за сутки

3. Поиск средней линии аврорального овала

Для поиска средней линии аврорального овала необходимо для начала найти границы нашего аврорального овала, записывая на каждую долготу по два значения широты (максимальную и минимальную). Имея границы полярного сияния, можно рассмотреть каждую долготу по отдельности и вычислить по формуле среднее значение между двумя широтами:

$$c_0 = (\varphi_{\max 0} - \varphi_{\min 0})/2 + \varphi_{\min 0}$$

$$c_1 = (\varphi_{\max 1} - \varphi_{\min 1})/2 + \varphi_{\min 1}$$

……

$$c_{359} = (\varphi_{\max 359} - \varphi_{\min 359})/2 + \varphi_{\min 359}$$

Где φ – это географическая широта, max – максимальная широта на рассматриваемой долготе, min – минимальная широта на рассматриваемой долготе, 0,1…359 номер долготы. С – центральная точна между двумя широтами.

После того, как мы получили 360 средних точек широты, мы соединим их сплошной линией, из чего получим замкнутую окружность, которая и будет являться нашей средней линией одного из аврорального овала. Результат сомкнутых точек показан на рис. 3.

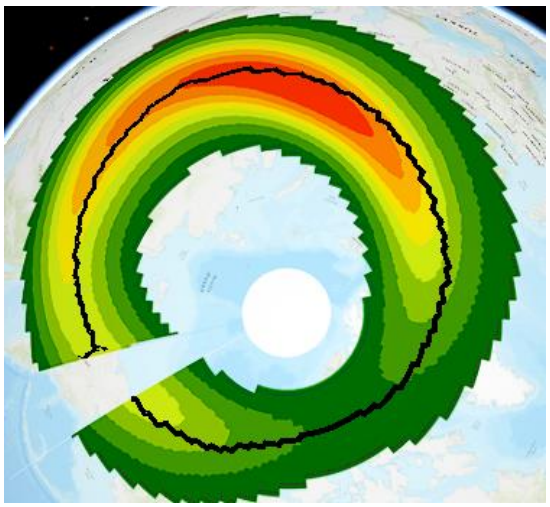


Рис. 3. Средняя линия аврорального овала

Заключение

В данной статье был рассмотрен один из способов визуализации полярного сияния в программном продукте *ArcGis*. Также были приведены алгоритмы поиска центра и средней линии аврорального овала. Так, с помощью визуализации и прогнозирования полярного сияния можно снизить техногенные риски, которые могут быть связаны со сбоями систем высокоширотных железных дорог, построение скважин в арктическом регионе, а также пригодится туристам и тем, кто хочет узнать, в какое время полярное сияние раскрывается лучше всего для просмотра.

СПИСОК ЛИТЕРАТУРЫ

1. Воробьев А.В., Пилипенко В.А., Еникеев Т.А., Воробьева Г.Р., Христодуло О.И.Система динамической визуализации геомагнитных возмущений по данным наземных магнитных станций Научная визуализация. 2021. Т. 13. № 1. С. 162-176.
2. Воробьев А.В., Пилипенко В.А., Еникеев Т.А., Воробьева Г.Р. Геоинформационная система для анализа динамики экстремальных геомагнитных возмущений по данным наблюдений наземных станций Компьютерная оптика. 2020. Т. 44. № 5. С. 782-790.
3. Воробьев А.В., Воробьева Г.Р. Подход к оценке относительной информационной эффективности магнитных обсерваторий сети intermagnet Геомагнетизм и аэрономия. 2018. Т. 58. № 5. С. 648-652.
4. Воробьев А.В., Воробьева Г.Р. Веб-ориентированная 2d/3d-визуализация параметров геомагнитного поля и его вариаций Научная визуализация. 2017. Т. 9. № 2. С. 94-101.
5. Воробьев А.В., Пилипенко В.А., Сахаров Я.А., Селиванов В.Н.Статистические взаимосвязи вариаций геомагнитного поля, аврорального электроджета и геоиндуцированных токов Солнечно-земная физика. 2019. Т. 5. № 1. С. 48-58
6. Воробьев А.В., Пилипенко В.А., Решетников А.Г., Воробьева Г.Р., Белов М.Д.Веб-ориентированная визуализация геофизических параметров в области аврорального овала Научная визуализация. 2020. Т. 12. № 3. С. 108-118.

7. Воробьев А.В., Воробьева Г.Р. Визуализация геомагнитных вариаций в частотно-временной области информационного сигнала Научная визуализация. 2019. Т. 11. № 2. С. 143-155

СЕКЦИЯ 5.7
СИСТЕМНЫЙ АНАЛИЗ, УПРАВЛЕНИЕ И ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

УДК 004

А. Д. АБЗАЛОВ
Abzalov14@mail.ru
Науч. руководв. – кан. техн. наук, доц. О. Я. БЕЖАЕВА

Уфимский государственный авиационный технический университет

ПРОЕКТИРОВАНИЕ И РАЗРАБОТКА МЕССЕНДЖЕРА ДЛЯ МОБИЛЬНОЙ ПЛАТФОРМЫ ANDROID

Аннотация. В данной статье анализируется рынок мобильных приложений и проектируется приложение-мессенджер для платформы Android.
***Ключевые слова*:** мобильная разработка; мессенджер; нереляционная база данных.

Все мобильные приложения условно можно поделить на программы для рабочих целей и на развлекательные программы. Первые позволяют бизнесменом и офисным работникам контролировать бизнес-процессы, составлять аналитическую отчетность, выполнять такие задачи, разработка дизайна фирменного стиля. Вторые включают в себя разнообразные игры, софт для просмотра фильмов и прослушивания музыки, средства для общения и т.д.

Популярнейшим средством общения посредством мобильных устройств являются мессенджеры. Мессенджер – программа, позволяющая пользователем отправлять друг другу сообщения (текст, документы, медиа) в реальном времени.

Ниже перечислены некоторые особенности, которые позволили мессенджерам набрать такую популярность:

– возможность асинхронного и синхронного обмена сообщениями. Можно отправлять сообщения, даже если собеседник не сможет прочитать их сразу. Отправленное сообщение будет «лежать в кармане» получателя, пока тот не сможет его принять. При синхронном обмене происходит общение в реальном

времени, то есть собеседники принимают сообщения и отправляют ответ без задержек.

– долговременный диалог. Сообщения от каждого пользователя объединены в диалог. Сообщения хранятся в этом диалоге и можно просмотреть всю историю общения. Этот подход отличается от тех что были раньше: старые SMS-клиенты не могли объединять сообщения от одного пользователя и отображали их в порядке поступления. В электронной почте общение пользователей привязано к определенной теме.

– список диалогов. Этот список очень просто построен: скорее всего, пользователь захочет продолжить беседу с тем, с кем общался недавно, поэтому этот диалог отображается вверху списка. В такой простоте есть большое преимущество: не приходится настраивать мессенджер, чтобы указать, кто сегодня наиболее важен. Более старые диалоги перемещаются вниз, но их тоже легко возобновить.

– экономия времени. Люди устали читать длинные посты в социальных сетях, тем более на это затрачивается самый драгоценный ресурс стремительной современной жизни – время. Им проще и быстрее прочитать короткое, информативное сообщение. Именно такую возможность предоставляют мессенджеры.

– высокий уровень надежности и защиты персональных данных. Мессенджеры по степени надежности существенно превосходят социальные сети или электронную почту.

Проектирование мобильного приложения-мессенджера

Одним из самых популярных средств визуального моделирования объектно-ориентированных информационных систем является Rational Rose компании IBM. Его работа основана на унифицированном языке моделирования UML (Unified Modeling Language). Rational Rose способен решать практически любые задачи в проектировании информационных систем: от анализа бизнес процессов до кодогенерации на определенном языке программирования. Толь-

ко Rational Rose позволяет разрабатывать как высокоуровневые, так и низкоуровневые модели, осуществляя тем самым либо абстрактное проектирование, либо логическое. Rational Rose использует синтез-методологию объектно-ориентированного анализа и проектирования, основанную на подходах трех ведущих специалистов в данной области: Буча, Рам и Джекобсона.

При помощи Rational Rose была построена диаграмма вариантов использования, отображенная на рисунке 1.

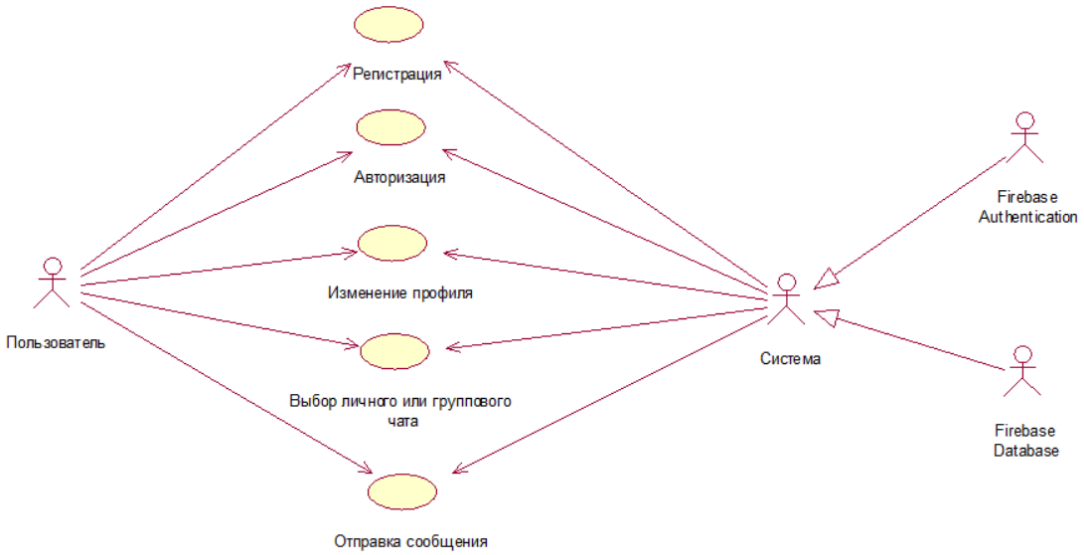


Рис. 1. Use-case диаграмма процесса работы мессенджера

Регистрация – пользователь может создать новый аккаунт.

Авторизация - пользователь может войти под уже существующим аккаунтом.

Изменить профиль –в настройках своего профиля пользователь может изменить отображаемое имя, написать статус, а также установить фотографию профиля.

Выбор личного или группового чата – личные и групповые чаты разделены для удобства восприятия.

Отправка сообщения – основная функция приложения, собеседник мгновенно увидит отправленное сообщение.

Алгоритм работы программы отображает последовательность выполнения основных операторов программы. Информационная система процесса

функционирования имеет модульную структуру. Модули имеют небольшие размеры, четко определенные функции и, кроме того, их связи между собой максимально упрощены. Разбиение программы на модули при ее написании позволяет существенно облегчить в дальнейшем работу над программой на других этапах.

Планируемая система должна обладать модульной архитектурой с одним центральным узлом, отвечающего за функционирование программной части системы. К ядру системы будут подключаться независимые друг от друга модули. В состав мессенджера должны входить следующие подсистемы:

– личные чаты;
– групповые чаты;
– настройки профиля;
– поиск друзей;
– список контактов;
– список заявок.

Backend as a service (BaaS) – модель обеспечения разработчиков разными инфраструктурными функциями, такими как облачное хранилище, интеграция с социальными сетями, пуш-уведомления, управление пользователями и т.п. BaaS значительно упрощает создание приложений, предлагая уже готовые функции и возможности разработчикам, оставляя им возможность сосредоточиться на функционале приложений.

Большинство мобильных приложении используют сервер для хранения данных и приложение, которое интегрируется с этой базой данных. Для наилучшего результата требуются как специалисты frontend для разработки клиентской части так и backend-специалисты для разработки серверной части. Роль последних стала несколько меньше после того, как появились облачные сервисы, предоставляющие возможность хранить гибкую систему данных у себя на сервере. В результате, процесс создания приложения значительно упро-

стился, и многие проекты заменили работу backend- специалистов на облачные сервисы.

Предлагается следующая логика работы приложения: приложение в реальном времени отслеживает изменения в базе данных на облачном хранилище и при появлении новых данных, отображает их на устройстве пользователя.

Приложение работает с облачной нереляционной базой данных Firebase Database. Firebase Database служит базой данных, которая изменяется в реальном времени и хранит данные в JSON.

JSON – это формат, который хранит структурированную информацию и в основном используется для передачи данных между сервером и клиентом.

Файл JSON представляет собой более простую и легкую альтернативу расширению с аналогичными функциями XML (Extensive Markup Language).

Программное приложение для ОС Android состоит из набора активностей, каждой из которых соответствует экран приложения. Активность, которая запускается первой, считается главной. Из нее можно запустить другую активность.

Каждая активность представлена в проекте классом, реализованном на языке Java, хранящемся в одноименном файле с расширением .java. Каждой активности соответствует xml файл-описание. В xml-файле описано в виде xml-кода расположение визуализируемых объектов. При запуске активности система Android автоматически распознает размер экрана мобильного устройства и приводит выводимый контент в соответствие с разметкой, описанной в xml-файле. Таким образом, одна и та же активность будет выглядеть одинаково независимо от диагонали используемого устройства.

СПИСОК ЛИТЕРАТУРЫ

1-Колесов, Ю. Б. Объектно-ориентированное моделирование сложных динамических систем [Текст] / Ю. Б. Колесов. – СПб.: СПбГПУ, 2004. – 250 с.

2- Голощапов А.Л. Google Android. Создание приложений для смартфонов и планшетных ПК. Издательство Питер 2012.

3 - Firebase Database. Firebase [Электронный ресурс] – Режим доступа: https://firebase.google.com/docs/database

УДК 004.94

С. И. БЕРГ
Sergey9514berg@gmail.com
Науч. руководов. – канд. техн. наук, доц. С. А. ЗАГАЙКО

Уфимский государственный авиационный технический университет

МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ ТРЕНИЯ И ИЗНОСА В ЦПГ ДВС С ПРИМЕНЕНИЕМ ЭВМ

Аннотация. Было проведено исследование режимов трения и условий работы пар трения поршневые кольца – цилиндр, была подобранна оптимальная математическая модель для расчета потерь и износа в ЦПГ ДВС. По выбранной математической модели была создана программа СМТИ ЦПГ ДВС. Анализ получившихся значений показал, что программу для расчета потерь и износа в ЦПГ ДВС можно использовать и она выдает данные которые соответствует экспериментальным.
***Ключевые слова*:** двигатель внутреннего сгорания; трение; износ; математическое моделирование; трение и износ в ЦПГ ДВС; моделирование с применением ЭВМ.

Введение

Повышение надежности и долговечности машин является одной из главных проблем современного машиностроения. Одним из основных узлов двигателя , имеющий огромное значение при его работе , является цилиндропоршневая группа двигателей внутреннего сгорания (ЦПГ ДВС), для обеспечения его работы важен правильный подбор материалов и обеспечение оптимальных режимов работы. Для удовлетворения этих требований необходимо использовать современные методы расчета трения и условий в цилиндре.

Целью данной работы является создание программы для автоматизированного определения потерь на трение и износ в ЦПГ ДВС по основным параметрам двигателя

Моделирование трения и износа в ЦПГ ДВС с применением ЭВМ

Математическая модель расчета величины механических потерь в поршневых кольцах создана на основании закономерностей полуэмпирического вида, выведенных Крагельским И.В. [1,2]

Последовательность выполнения расчетов и различных процедур при расчете потерь на трение в поршневых кольцах приведена на рисунке 1.

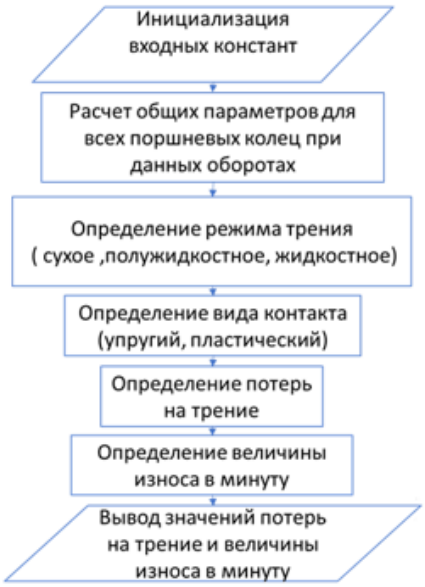


Рис. 1. Обобщенная блок-схема математической модели для расчета трения и износа в паре трения «поршневые кольца-цилиндр».

Расчет потерь на трение приводился посредством численного моделирования потерь в поршневых кольцах при условии одинакового среднего индикаторного давления на всех расчетных частотах вращения. При расчете также задавалась одинаковая геометрия компрессионных колец.

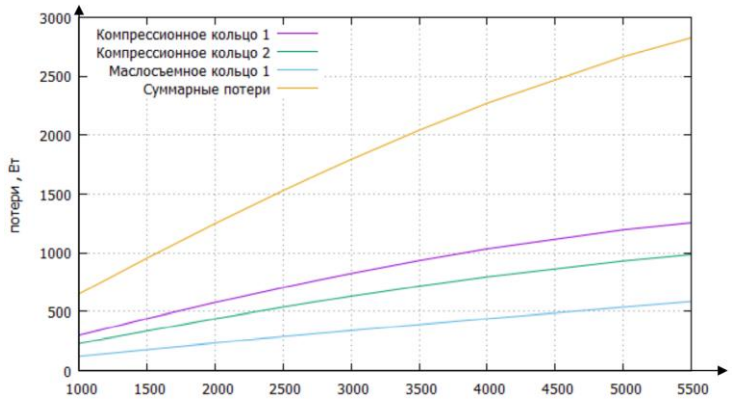


Рис. 2. Результаты расчета потерь на трение за цикл в поршневых кольцах приходящихся на 1 цилиндр

На рисунке 2 видна характерная криволинейная квадратичная зависимость среднецикловых потерь на трение в поршневых кольцах ДВС от частоты вращения коленчатого вала при одинаковой нагрузке на двигатель, что соответствует теоретическим выкладкам. Механические потери получились отличными друг от друга вследствие того, что на поршневые кольца действовали различные заколечные давления.

Для анализа получившихся данных, проведем сравнение получившихся значений с экспериментальными, полученными на режиме прокрутки в 6 точках, получившиеся значения приведены на графике рисунок 3.

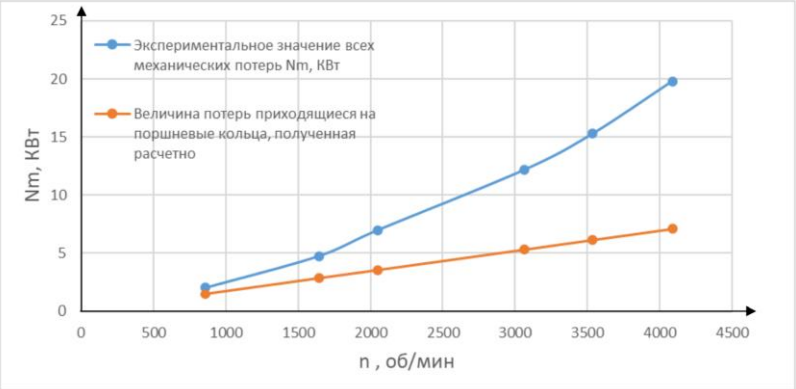


Рис. 3. Экспериментально измеренная величина потерь на трение в режиме прокрутки по двигателю УЗАМ-3320.

Таблица 1

Сравнение экспериментальных и расчетных данных по величине износа

n, об/мин	Экспериментальное значение всех механических потерь на режиме прокрутки N_m, КВт	Величина потерь приходящиеся на все поршневые кольца, полученная расчетно $N_{рас}$, кВт
857	2,027	1,488
1642	4,761	2,856
2052	7,002	3,564
3065	12,191	5,328
3535	15,281	6,156
4088	19,811	7,116

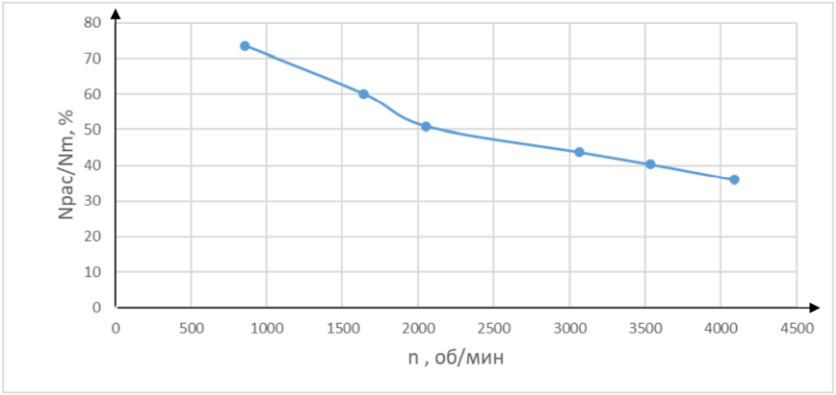


Рис. 4. Сравнение экспериментальных и расчетных значений $N_{рас}$ и N_m

Расчетные значения потерь на трение в поршневых кольцах от всех механических потерь, находятся в диапазоне от 73% при 857 об/мин до 36% при 4088

об/мин, таким образом получившиеся значения вполне соответствуют реальности.

Сравнивая экспериментальные значения и расчетные мы получаем, что расчетные значения входят в диапазон экспериментальных, таким образом данную математическую модель можно использовать для анализа величины потерь на трение.

Для определения того как влияет нагрузка на двигатель на величину потерь на трение проводится расчет при различной нагрузке и постоянных оборотах n = 4000 об/мин.

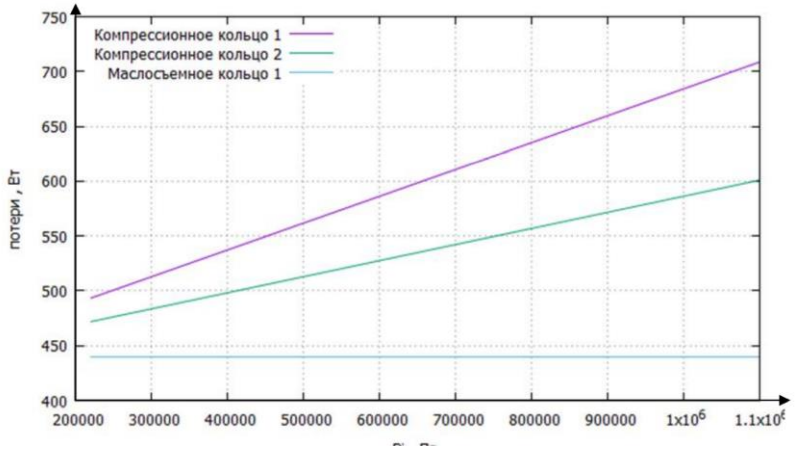


Рис. 5. Результаты расчета потерь на трение за цикл при постоянных оборотах 4000 об/мин в поршневых кольцах на 1 цилиндр

При анализе получившихся графиков рисунок 5 можно определить, что средние значение цикловых механических потерь в компрессионных кольцах линейно возрастают от нагрузки (от среднего индикаторного давления цикла Pi), поскольку давление напрямую влияет на силу прижатия колец к стенке цилиндра, что нельзя сказать о потерях в маслосъемном кольце – в нем потери практически не зависят от нагрузки, т.к. маслосъемные кольца не воспринимают давление газов и не препятствуют их проникновению в картер двигателя.

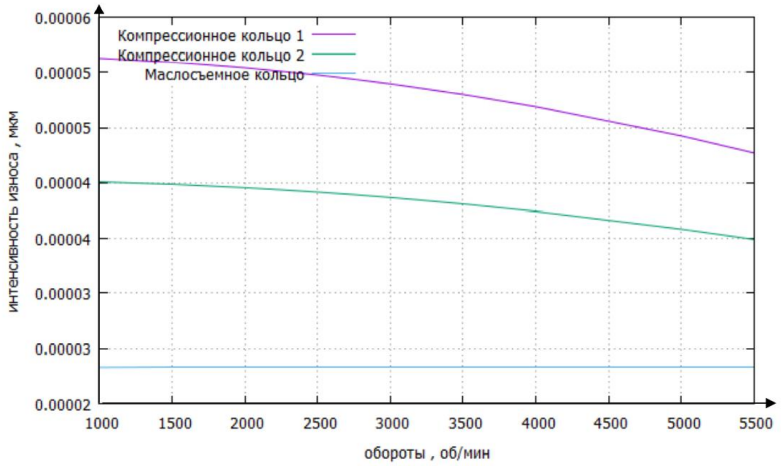


Рис. 6. Результаты расчета среднецикловой интенсивности износа в различных поршневых кольцах

На рисунке 6 видна криволинейная квадратичная зависимость среднецикловой интенсивности износа в поршневых кольцах ДВС от частоты вращения коленчатого вала при одинаковой нагрузке на двигатель, что соответствует теоретическим выкладкам [3]. Интенсивности износа получились отличными друг от друга вследствие того, что на поршневые кольца действовали различные заколечные давления.

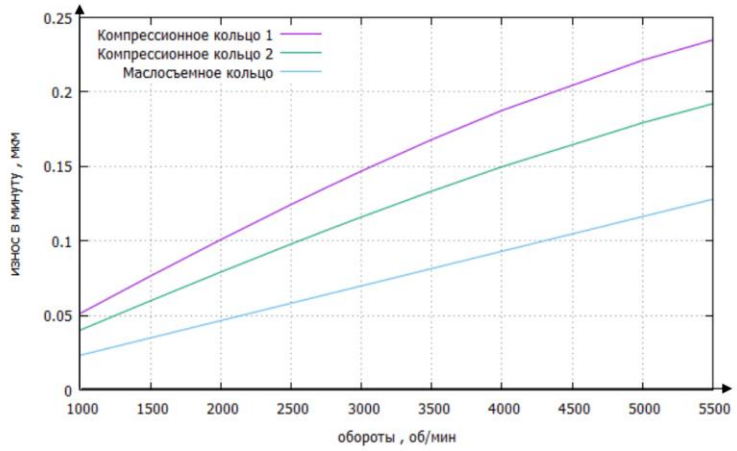


Рис. 7. Результаты расчета износа в минуту в различных поршневых кольцах

На рисунке 7 показана зависимость износа в минуту в поршневых кольцах ДВС от частоты вращения коленчатого вала при одинаковой нагрузке на двигатель. Величины износа получились отличными друг от друга вследствие того, что на поршневые кольца действовали различные заколечные давления. Соответственно криволинейность графиков объясняется тем, что среднее значение давлений приведенное на рисунке 8 является криволинейной убывающей зави-

симостью от оборотов двигателя, данный график не является ошибочным т.к. соответствует экспериментальным данным .

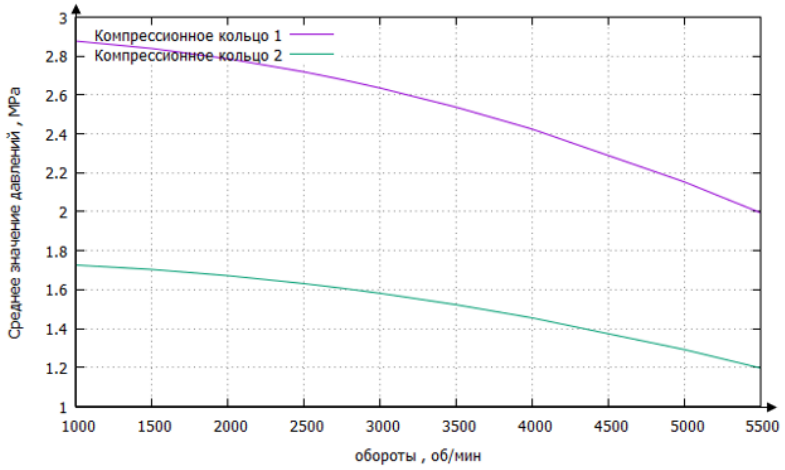


Рис. 8. Среднее значение давлений газов использованных в расчете

Для анализа получившихся данных, проведем сравнение получившихся значений с экспериментальными получаем следующие значения в соответствии с табл. 2.

Таблица 2

Сравнение экспериментальных и расчетных данных

Вид поршневых колец	Средний износ экспериментальный, мм	Износ расчетный, мм
Компрессионное верхнее	0,106 ± 0,1	0,083
Компрессионное нижнее	0,060 ± 0,1	0,057
Маслосъемное	0,070 ± 0,1	0,041

*Эксперимент проводился 288 часов при частоте коленчатого вала n = 3800 об/мин.

Сравнивая экспериментальные значения и расчетные мы получаем, что расчетные значения входят в диапазон экспериментальных, таким образом данную программу СМТИ ЦПГ ДВС можно использовать для анализа величины износа.

Для определения того как влияет нагрузка на двигатель на величину потерь на трение проводится расчет при различной нагрузке и постоянных оборотах n = 4000 об/мин.

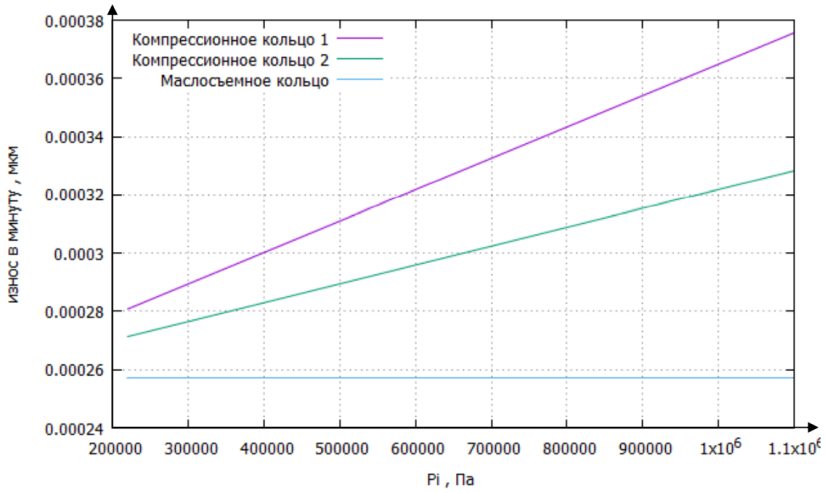


Рис. 9. Результаты расчета износа в минуту при постоянных оборотах n = 4000 об/мин в различных поршневых кольцах

При анализе графиков рисунок 9 можно определить, что средние значение циклового износа в минуту в компрессионных кольцах линейно растет и имеют прямую зависимость от нагрузки (от среднего индикаторного давления цикла P_i), поскольку давление напрямую влияет на силу прижатия колец к стенке цилиндра, что нельзя сказать о потерях в маслосъемном кольце – в нем значение средне циклового износа практически не зависит от нагрузки, т.к. маслосъемные кольца не воспринимают давление газов и не препятствуют их проникновению в картер двигателя. Получившиеся зависимости соответствуют теоретическим выкладкам.

Заключение

Было проведено исследование режимов трения и условий работы пар трения поршневые кольца – цилиндр, была подобранна оптимальная математическая модель для расчета потерь и износа в ЦПГ ДВС . По выбранной математической модели была создана программа СМТИ ЦПГ ДВС.

В ходе выполнения программы были обработаны данные , определены режимы трения и потери , а также величина износа в ЦПГ ДВС. Был проведен анализ получившихся значений и их сравнение с экспериментальными данными, анализ получившихся значений показал, что программу для расчета потерь и износа в ЦПГ ДВС можно использовать и она выдает данные которые соответствует экспериментальным.

СПИСОК ЛИТЕРАТУРЫ

1. Крагельский, И.В. Трение и износ .— М. : Машгиз, 1962 .— 383с.
2. Крагельский, И.В. Основы расчетов на трение и износ И.В. Крагельский, М.Н. Добычин, В.С. Комбалов. – М. Машиностроение, 1977. – 526 с.
3. Загайко, С. А. Расчет механических потерь в двигателях внутреннего сгорания : учебное пособие / С. А. Загайко ; Федеральное агентство по образованию ; Государственное образовательное учреждение высшего профессионального образования ; УГАТУ .— Уфа : УГАТУ, 2006 .— 123 с.

УДК 004.6

И. В. ГАВРИЛОВ
ilyavladimirovich111@gmail.com
Науч. руководитель – д-р экон. наук, канд. техн. наук, проф. И. З. МУСТАЕВ

Уфимский государственный авиационный технический университет

ОПРЕДЕЛЕНИЕ ГРАНИЦ АВТОМАТИЗАЦИИ СЛОЖНОГО ТЕХНИЧЕСКОГО ОБЪЕКТА

Аннотация. Спроектированная и работающая база данных – ключевой атрибут любого предприятия. Для составления базы необходимы специальные навыки и умения, поэтому быстро структурировать новую информацию простому сотруднику без помощи специалиста невозможно. Для упрощения структурирования информации необходимо спроектировать систему управления сложного технического объекта с упрощенным вариантом составления базы данных. Для этого нужно определиться с самим понятием «структуризация» и разобраться с их видами для дальнейшего проектирования системы.
***Ключевые слова*:** база; данных; структурирование; информационная; система.

Система управления жизненным циклом сложного технического изделия должна включать применение согласованного набора решений для поддержки совместного создания набора данных о объекте, управления этими данными, распространения их и использования в рамках всего расширенного предприятия от концепта до окончания ЖЦ продукта путем интегрирования людей, процессов, бизнес-систем и информации, то есть система должна позволять управлять множеством аспектов социофизического объекта и обеспечивать максимум его потенциала.

В данном случае суть управления информационным аспектом социофизического объекта заключается в создании системы, которая позволяла бы собирать базу данных, не прибегая к силам специалистов в области создания баз данных. Для этого необходимо:

– определить целесообразность;

– определиться со структурой.

Составление базы данных – это прежде всего структурирование информации. База данных – поименованная совокупность экземпляров групп и груп-

повых отношений. Для представления группового отношения используется формы:

а) Простая структура. Текстовое представление данных является самым простым способом. Данная структура имеет много минусов, таких как сложность использования и установок связи, ограниченность по объему и другие.

б) Графовая. Группы изображаются вершинами графа, связи между группами - дугами, направленными от группы-владельца к группе-члену с указанием имени отношения и коэффициента. По типу графов различают:

– иерархическую модель (граф без циклов – дерево), при этом каждая запись может иметь только одного «родителя». Данный тип можно увидеть в файловых системах, DNS, LDAP;

– сетевую модель (ориентированный граф общего вида), при этом каждая запись может иметь более одного родителя. Примером может служить IDMS.

в) Реляционная. Связь между группами изображается таблицей, столбцы которой представляют ключи соответствующих групп. Применяется язык запросов SQL. Благодаря внешним ключам происходит соединение таблиц между собой. Примеры данного типа – MySQL, PostgreSQL.

г) NoSQL. NoSQL баз данных, то есть «not only SQL — не только SQL».

– База данных «ключ-значение» (key-value database). Чтобы внести в базу объект необходимо предоставить сам объект и ключ к нему. Для получения объекта необходим тот самый ключ. Пример – Redis, Berkeley DB.

– Документная база данных. Хранит с помощью ключей иерархические, структурированные данные (XML, JSON, BSON). Примеры – MongoDB, CouchDB.

– Колоночная база данных. Данный тип похож на реляционный тип (хранение в строках и столбцах), но вместо таблиц – «колоночные семейства», а строки прописаны по определенной схеме. Пример – Cassandra.

– Базы данных временных рядов (time series database). Таблицы отслеживают значения, которые меняются с течением времени (системы мониторинга). Пример – InfluxDB, Prometheus.

г) Комбинированные типы.

– NewSQL – улучшенные технологии масштабирования, доступности и согласованности, чем у обычных реляционных баз данных. Пример – MemSQL, YugabyteDB.

– Многомодельные базы данных – поддержка разных моделей баз данных, таких как реляционные, колоночные, сетевые. Благодаря этому методу возможно создавать системы, в которых присутствуют необходимый на данный момент тип данных с возможностью масштабирования. Пример – ArangoDB.

Для выбора основного метода структурирования в проектируемой информационной системе необходимо протестировать все виды структур, чтобы определить, какой метод может быть использован в большинстве случаев составлении базы данных для упрощения этого процесса.

Были разработаны концептуальные формы будущей системы, включающие реляционную и древовидную структуру на примере студентов кафедры и подтаблицы «Магистранты» (Рисунок 1).

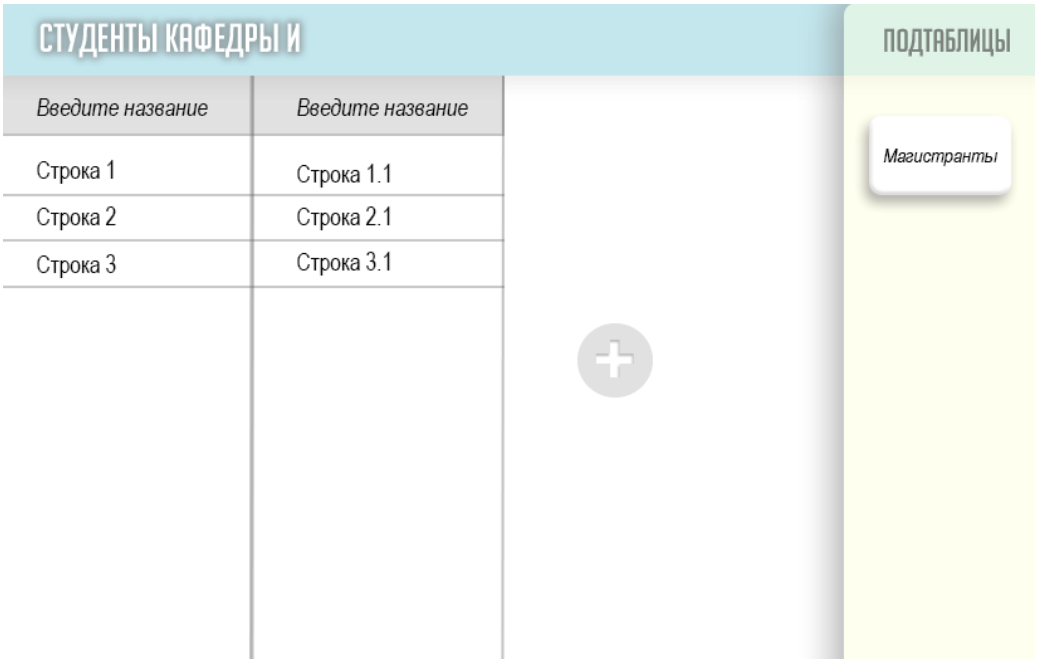


Рис. 1. Концептуальная форма приложения

На рисунке 2 изображена форма «Студенты», которые включает таблицу «Студенты кафедры И».

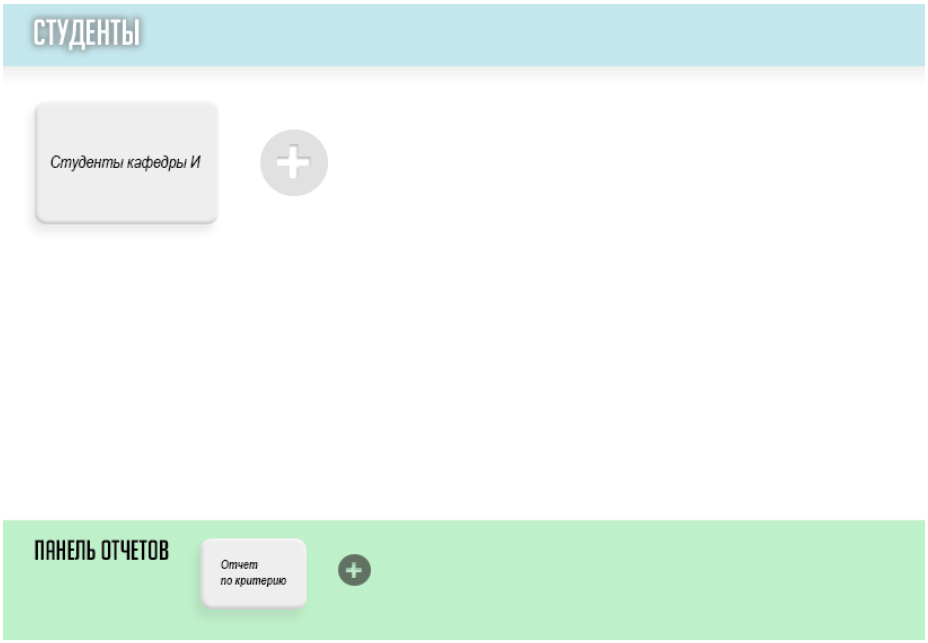


Рис. 2. Концептуальная форма приложения

Дальнейшие разработки должны показать, подойдет ли многомодельный тип данных, для прикладной системы структурирования информации, который включает реляционный и древовидный тип. Возможно, вместо древовидной системы необходимо внедрять сетевую модель, так как часто данные имеют больше одного «родителя».

В результате выполнения структурирования создается новая система управления информацией, которые упрощают действия, производимые с ней. Следовательно, мы упростим управление системой жизненного цикла сложного технического объекта, в том числе всех его аспектов в социофизической интерпретации.

СПИСОК ЛИТЕРАТУРЫ

1. Мустаев И. З., Механика живых и интеллектуальных систем // УГАТУ, 2020. С. - 200 с
2. Курносов Ю. В., Конотопов П. Ю. Аналитика: методология, технология и организация информационно-аналитической работы // РУСАКИ, 2004. С. - 512 с
3. Лосев В. Я., Симоров С.Н., Система с способ управления базами данных (СУБД) // ПЛЮСКОМ, 2019. С. – 32 с

УДК 004.94

А. М. ГАЛИЕВА
Lady.maksimus@mail.ru
Науч. руководитель – д-р техн. наук, проф. Е. А. МАКАРОВА

Уфимский государственный авиационный технический университет

ИМИТАЦИОННАЯ АГЕНТ-ОРИЕНТИРОВАННАЯ СИСТЕМА МОДЕЛИРОВАНИЯ ПРОЦЕССОВ ФУНКЦИОНИРОВАНИЯ ПРЕДПРИЯТИЙ ОБЩЕСТВЕННОГО ПИТАНИЯ В УСЛОВИЯХ РЕЦЕССИИ

***Аннотация*.** Предложены объектно-ориентированные модели для имитационной агент-ориентированной системы моделирования процессов функционирования предприятий общественного питания в кризисной ситуации в виде диаграмм прецедентов.
***Ключевые слова*:** объектно-ориентированное моделирование; предприятие общественного питания; диаграмма прецедентов.

Предприятия общественного питания (ПОП) играют важную роль в жизни любого человека и общества в целом. За прошедшие пять лет динамика качества сервиса поднимается вверх, благодаря автоматизации, исследованиям потребностей населения и внедрению новых технологий. Экономической целью рынка услуг общественного питания является в обеспечении эффективного использования потребительских ресурсов для удовлетворения потребностей общества.

Согласно ГОСТ Р 50647-2010 «Услуги общественного питания. Термины и определения» ПОП определяется как – «самостоятельная отрасль экономики, состоящая из предприятий различных форм собственности и организационно-управленческая структура, организующая питание населения, а также производство и реализацию готовой продукции и полуфабрикатов, как на предприятии общественного питания, так и вне его, с возможностью оказания широкого перечня услуг по организации досуга и других дополнительных услуг» [1].

В 2020 г. рынок общественного питания России столкнулся с рядом сложностей: локдауны и ограничения в работе, падение рубля на фоне экономической нестабильности как внутри страны, так и за ее пределами, сокращение доходов и расходов населения [2]. Пришлось произвести кардинальную перестройку –

переход на доставку продуктов питания на дом, смену режимов работы и технологий приготовления еды, поиск дополнительного финансирования для возможности перейти на новый уровень работы.

Особенности развития ПОП в 2021 году состоят в следующем.

Во-первых, новые кризисные реалии привели к тому, что значительная доля рестораторов, владельцев кафе и заведений фаст-фуда начали искать пути оптимизации расходов используя для этого программные решения.

Во-вторых, запрос на безопасность со стороны посетителей приводит к росту расходов на антисептики, маски, перчатки, в то время как требования касательно рассадки посетителей требуют сокращения количества посадочных мест и новых дизайнерских решений.

Во-третьих, говоря о развитии рынка в 2021 г., можно предположить, что часть заведений общепита продолжит закрываться, но темпы будут ниже прошлогодних. Ведь пандемия еще не закончилась, а значит рестораны и кафе продолжают страдать от ограничений и постоянных изменений в работе. Незначительно вырастут цены на продукты питания: по прогнозам Центрального Банка России годовой рост цен на продовольственные товары составит 3,7-4,2%. В итоге, подорожают блюда в самих заведениях, что скажется на спросе. Если добавить сюда и снижение платежеспособности населения, в 2020 г. реальные доходы населения снизились на 3,5%, а в 2021 г. тенденция может продолжиться, то можно предположить, что расходы населения на питание вне дома также сократятся [2].

Безусловно, в момент текущего финансового кризиса, многие рестораторы решат повременить с агент-ориентированным моделированием (АОМ), отложить ее до лучших времен. Это неправильный подход.

Правительство Российской Федерации предпринимает все возможные меры для снижения потенциального негативного эффекта пандемии на ключевые показатели экономики [3].

Основным преимуществом системы агентного моделирования возможность оперативно получать практически любую информацию, необходимую

для принятия решений, а также отслеживать динамику прибыли и рассчитывать финансовые вливания для поддержания бизнеса на плаву.

На кафедре технической кибернетики ведется разработка имитационной агент-ориентированной системы (ИАОС) моделирования процессов взаимодействия ПОП и государства в условиях рецессии.

Варианты возможного использования ИАОС процессов взаимодействия ПОП и государства в условиях рецессии отображены на диаграмме прецедентов (вариантов использования), представленной на рисунке 1.

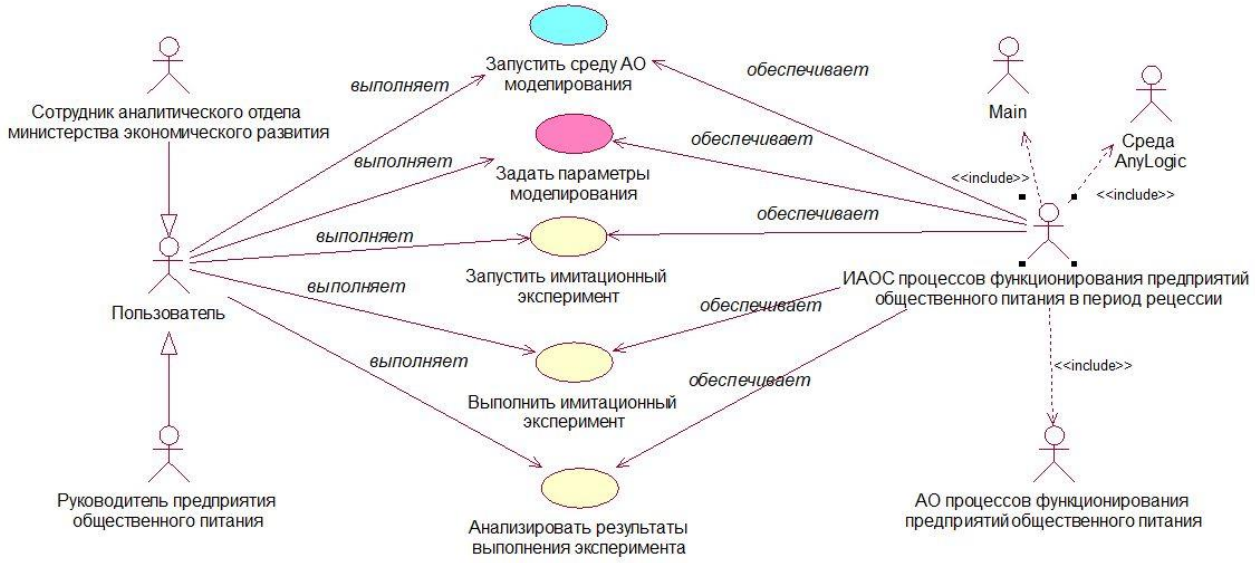


Рис. 1. Варианты использования ИАОС процессов взаимодействия ПОП и государства в условиях рецессии

Диаграмма показывает взаимодействие между вариантами использования и «актерами». На диаграмме представлены следующие объекты: Пользователь; Среда *AnyLogic* и MAIN.

Декомпозиция варианта использования «Запустить среду АО моделирования» представлена на рисунке 2. Актером является пользователь. Сначала пользователь должен открыть каталог со средой моделирования - эту опцию предоставляет *AnyLogic*. Затем пользователь может запустить исполняемый файл программы. Среда *AnyLogic* предоставляет пользователю нужные инструменты.

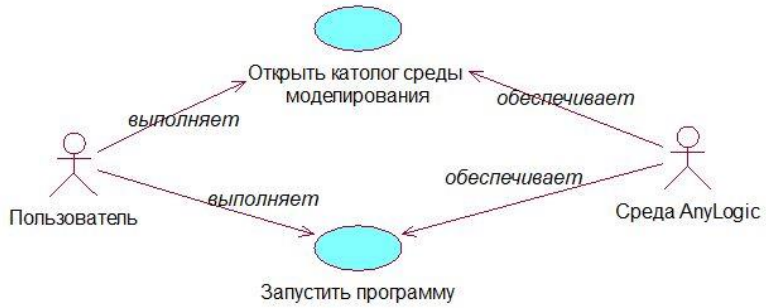


Рис. 2. Запустить среду АО моделирования

Декомпозиция варианта использования «Задать параметры моделирования» показан на рисунке 3.

Актером является пользователь. Пользователь должен сначала выбрать проект для запуска симуляции, что позволяет ему среда *AnyLogic*. Следующим шагом является задание параметров запуска имитации, таких как период выполнения, единицы модельного времени и других.

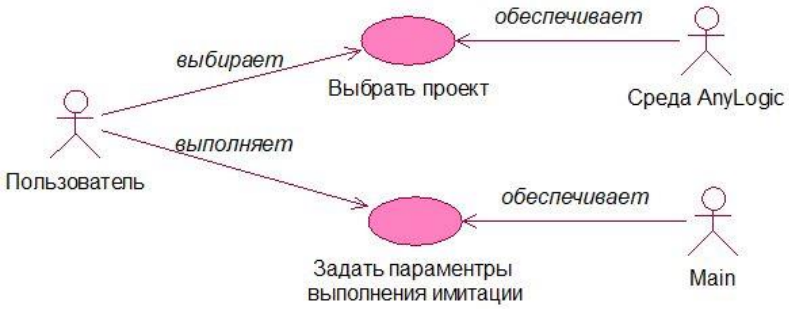


Рис. 3. Задать параметры моделирования

В созданной диаграмме вариантов использования используются следующие сценарии: «Запустить среду АОМ», «Задать параметры моделирования», «Запустить имитационный эксперимент», «Выполнить имитационный эксперимент», «Анализировать результаты выполнения эксперимента». Все актеры, принимают участие в каждом сценарии.

Таким образом, используя ИАОС процессов взаимодействия ПОП и государства в условиях рецессии, пользователь может задать параметры для неконтролируемых и контролируемых сценариев льгот от государства, провести имитационные эксперименты по различным сценариям, а также проанализировать итоги имитационных экспериментов с целью корректировки принимаемых управленческих решений.

СПИСОК ЛИТЕРАТУРЫ

1- Официальный сайт Росконгресс [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_165477
2- Официальный сайт Academyopen [Электронный ресурс]. – Режим доступа: https://academyopen.ru/journal/497
3 - Официальный сайт Росконгресс [Электронный ресурс]. – Режим доступа: https://roscongress.org/upload/medialibrary/dd0/Pamyatka-dlya-biznesa-v-usloviyakh-krizisa_25052020.pdf

УДК 681.5

К. С. ГУРОВА
gurova2067@yandex.ru
Науч. руководов. – канд. техн. наук, проф. А. М. СУЛЕЙМАНОВА

Уфимский государственный авиационный технический университет

АНАЛИЗ ПРОИЗВОДСТВЕННЫХ ДАННЫХ С ИСПОЛЬЗОВАНИЕМ НЕЙРОСЕТЕЙ

Аннотация. В данной статье речь идет об актуальности использования нейронных сетей, и о применении метода использования нейронных сетей с долгой краткосрочной памятью в сфере бюджетирования. В статье приведено описание принципа работы данной сети и процесс обучения нейронной сети. Также в данной статье говорится о результатах, которые будут достигнуты после обучения нейронных сети с долгой краткосрочной памятью.
***Ключевые слова*:** анализ; данные; информация; метод; нейрон; нейронная сеть; обучение; подход.

Введение

На сегодняшний день развитие различных сфер жизни человека связано с накоплением и обработкой полученных данных, которые содержат очень важную информацию. Для хранения такой информации требуются хранилища, способные вмещать большие объемы данных. Таким образом, сначала появилась потребность в технологии, которая позволит анализировать, хранить и обрабатывать огромное количество данных.

Целью исследования является повышение эффективности анализа большого массива данных в сфере бюджетирования.

Для достижения цели были решены следующие задачи:

1. Формирование обучающего набора данных

2. Разработка модели нейронной сети для анализа данных и их прогнозирования

3. Проведение обучения нейронной сети

4. Сравнение показателей точности анализа до и после применения метода

Материалы и методы

С помощью искусственного интеллекта решается такие задачи, как принятие решений, теория игр, обучение нейросетей и т.д [5]. В рамках данной диссер-

тации рассматривается метод обучения нейронных сетей. Учитывая объемы данных в сфере бюджетирования, возникают трудности с принятием управленческих решений. Целью данной работы является обучение нейросети для работы с данными в сфере бюджетирования.

Объектом исследования являются нейронные сети.

Предметом исследования является разработка методов использования нейронных сетей с долгой краткосрочной памятью для принятия управленческих решений в сфере бюджетирования. Новизна этого подхода заключается в том, что данный метод будет использован для анализа и прогнозирования бюджетирования Республики Башкортостан.

Нейронная сеть — это последовательность нейронов, соединенных между собой синапсами. Структура нейронной сети в программировании была заимствована из биологии[1]. Данная структура позволяет машине анализировать и даже запоминать различную информацию[4]. Также это дает возможность нейросетям воспроизводить информацию из своей памяти.

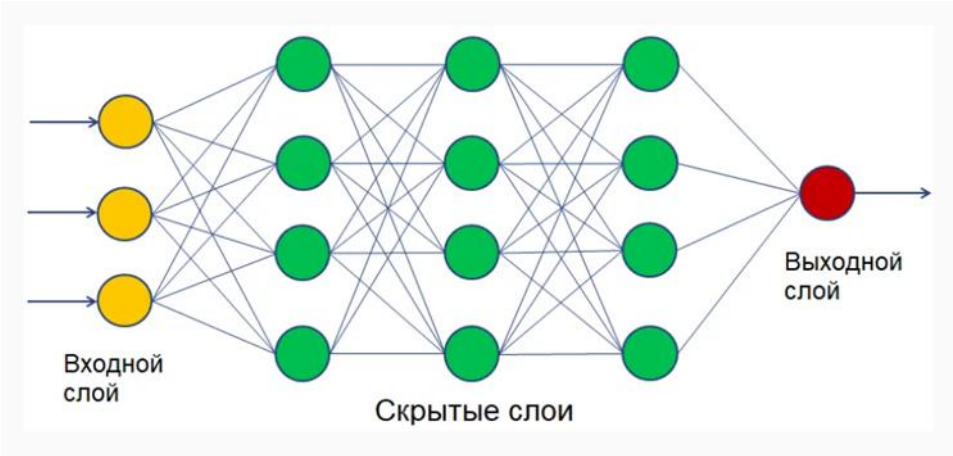


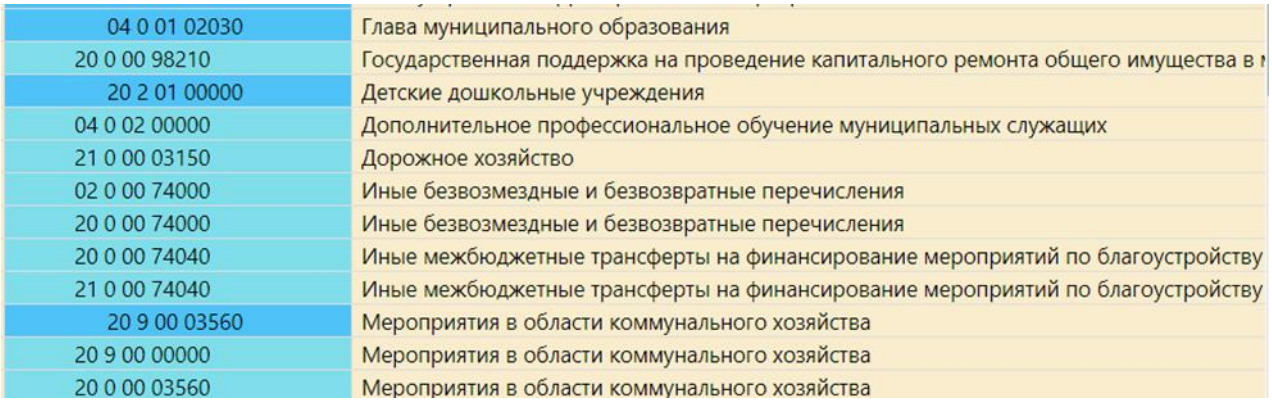
Рис. 1. Графическое представление нейронной сети

Основной принцип нейронной сети с долгой краткосрочной памятью заключается в том, что входной элемент определяет, какая входная информация будет использоваться для обновления информации и какую информацию мож-

но добавить в долгосрочную память. Выходной элемент определяет содержание выходной информации в блоке памяти[3]. Также в сети присутствует элемент «забывания». Данный элемент определяет какую информацию необходимо удалить из блока, а какую оставить[7].

В данной статье рассматривается пример обучений нейронной сети для распределения ЦСР в бюджетном планировании на основе программных продуктов предприятия НПО «Криста».

ЦСР – целевая статья расходов. Данная статья добавляется в систему под определенным кодом и имеет принадлежность к определенному бюджету, поэтому для каждого региона Республики Башкортостан данные статьи добавляются по отдельности. Пример отображения ЦСР в системе представлен на рисунке 2.



04 0 01 02030	Глава муниципального образования
20 0 00 98210	Государственная поддержка на проведение капитального ремонта общего имущества в м
20 2 01 00000	Детские дошкольные учреждения
04 0 02 00000	Дополнительное профессиональное обучение муниципальных служащих
21 0 00 03150	Дорожное хозяйство
02 0 00 74000	Иные безвозмездные и безвозвратные перечисления
20 0 00 74000	Иные безвозмездные и безвозвратные перечисления
20 0 00 74040	Иные межбюджетные трансферты на финансирование мероприятий по благоустройству
21 0 00 74040	Иные межбюджетные трансферты на финансирование мероприятий по благоустройству
20 9 00 03560	Мероприятия в области коммунального хозяйства
20 9 00 00000	Мероприятия в области коммунального хозяйства
20 0 00 03560	Мероприятия в области коммунального хозяйства

Рис. 2. Коды ЦСР

Данные статьи в систему должны добавлять финансовые органы районов, но бывает так, что пользователи изначально заводят в систему не все необходимые ЦСР. И в дальнейшем, в ходе работы у пользователей возникает множество ошибок, например, в консолидации отчетности или при составлении бюджетных обязательств, так как система пытается сослаться на ЦСР, которая изначально не была заведена.

Предлагаемая нейронная сеть будет на начальном этапе анализировать необходимую информацию и сообщать пользователям, какие ЦСР им необходимо добавить именно на их бюджет.

Для примера, в программе Deductor была построена таблица где было выбрано 5 рандомных ЦСР и 5 рандомным регионов РБ. После обучения построенной нейронной сети с помощью карт Кохонена были получены изображения, на которых видно, какая ЦСР на бюджете какого района отсутствует. Данные изображения представлены на рисунке 3.

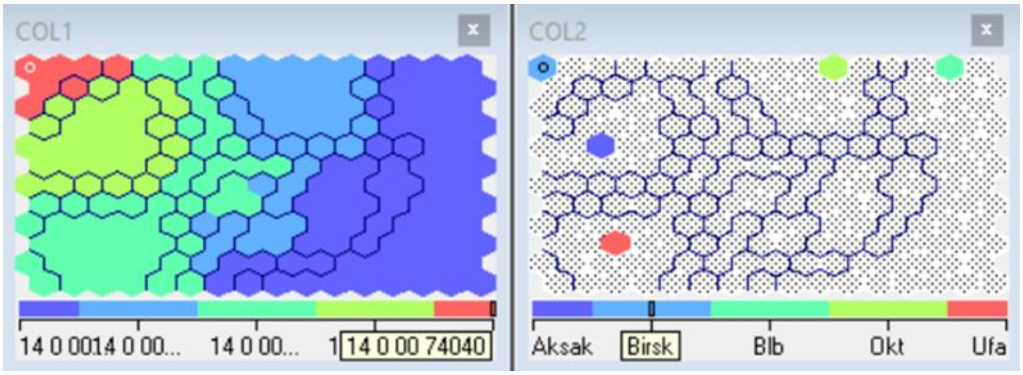


Рис. 3. Карты Кохонена

После обучения нейронная сеть будет способна обрабатывать новые данные по заданному алгоритму без участия человека.

Результаты и обсуждения

Благодаря данной нейросети сокращается время анализа данных. Устраняются ошибки, связанные с добавлением ЦСР. Данная нейросеть позволяет проводить анализ на всех уровнях иерархии от бюджета Республики Башкортостан до бюджетов муниципальных образований.

Выводы

Таким образом, в заключении можно сказать, что внедрений нейронных сетей на производство значительно облегчает процесс обработки информации, а также экономит временной и денежный ресурс. Данный метод удобен тем, что не требует глубоких знаний программирования для внедрения его на предприятии. Нейронная сеть может использоваться в любой сфере производства, помогая планировать и прогнозировать дальнейшую деятельность предприятия.

СПИСОК ЛИТЕРАТУРЫ

1. Айзерман М. А. Браверман Э. М., Розоноэр Л. И. Метод потенциальных функций в теории обучения машин: «Наука» 1970. 384с.

2. Бирюков А.Н. Нейросетевое моделирование в бюджетно-налоговой системе регионального и муниципального уровней: дис. … канд. техн. наук. Уфа 2012. 130 с.
3. Дюк В. А. Флегонтов А. В., Фомина И. К. Применение технологий интеллектуального анализа данных в естественнонаучных, технических и гуманитарных областях // Известия РГПУ им. А.И. Герцена. 2017. Том 9. №138. С. 77–84.
4. Ерофеева В.А. Обзор теории интеллектуального анализа данных на базе нейронных сетей: дис. … канд. тех. наук: 08.05.2021. Санкт-Петербург. 2018. 103 с.
5. Лабусов М. В. Нейорнные сетидолгой краткосрочной памяти и их использование для моделирования финансовых временных рядов// Инновации и инвестиции. 2020. Том 4. №3 С. 3-10.
6. Николаева Ю.В. Методы и алгоритмы интеллектуальной системы поддержки принятия решений трейдеров финансовых рынков: дис. … канд. техн. наук. 07.05.2021. Ижевск 2018. 127 с.
7. Кратович П.В. Нейросетевые модели для управления инвестициями в финансовые инструменты фондового рынка: дис. … канд. техн. наук. 08.05.2021. Тверь 2017. 165 с.
8. Тарик Р. Создаем нейронную сеть: «Вильямс» 2018. – 5-10 с.
9. Транкс Э. Глубокое обучение: «Библиотека программиста» 2019. – 4-9 с.
10. Ширяев В. И. Финансовые рынки. Нейронные сети, хаос и нелинейная динамика: «Либроком» 2009. 232 с.
11. Фаустова К. И. Нейронные сети: применение сегодня и перспективы развития// Территория науки. 2017. №4. С. 2-7.
12. Хайкин С. Нейронные сети: полный курс, 2-е издание: «Вильямс» 2008. 18с.
13. Schmidhuber J. Deep Learning in Neural Networks: «IDSIA» 2016. P. 85–87.
14. Nielsen M. Neural Networks and Deep Learning: «Scopus» 2019. P.13-16.
15. Simon O. Haykin Neural Networks and Learning Machines, 3rd Edition: «Scopus» 2018. P. 3-6

УДК 04.42

Р. Р. ДАУТОВ
dautovravil1999@mail.ru
Науч. руководитель – канд. техн. наук, доц. Н. И. ФЕДОРОВА

Уфимский государственный авиационный технический университет

ПРОБЛЕМА ПРОВЕДЕНИЯ И ОРГАНИЗАЦИИ МАСШТАБНЫХ ONLINE-МЕРОПРИЯТИЙ

***Аннотация*.** Рассматривается проблема проведения масштабных online-мероприятий, проводится анализ существующих решений и предлагается решение в виде разработки платформы для проведения online-мероприятий.
***Ключевые слова*:** online-мероприятие; проведение; организация; интеграция; цифровое пространство.

Проблема проведения мероприятий существует давно. Организаторы должны не только подготовить место проведения события, необходимое оснащение, питание и культурную программу, но также учесть особенности гостей из разных стран и предвидеть возможность возникновения различных внештатных ситуаций и потенциальные пути их решения. Для посетителей мероприятия необходимо заранее учесть дату и варианты проезда к нему. Еще одной трудностью в проведение мероприятия являются связанные с пандемией ограничения, отменяются и переносятся offline-события: конференции, ярмарки, выставки, туры.

Главным способом минимизации потерь стал переход в online. Торговые выставки и конференции являются крупным бизнесом во всем мире и стали жизненно важными для всех секторов экономики. Такие мероприятия предлагают ценные возможности для налаживания контактов для предприятий, чей опыт в основном сосредоточен на привлечении внимания к стендам, гостевым беседам и демонстрациям своей продукции. Виртуальные мероприятия очень похожи на личные, за исключением того, что они проводятся через Интернет, а не в одном физическом месте. Тем не менее, люди приходят в назначенное время, слушают выступающих, смотрят артистов, общаются друг с другом. Для небольших виртуальных мероприятий принять решение о хостинге будет до-

вольно просто. Ско-рее всего, выбор падет на Zoom или Cisco Webex. Однако с более крупными вир-

туальными событиями все усложняется. Более того, стоимость крупных виртуальных площадок для проведения мероприятий значительно возрастает. Особенно сейчас, когда рынок процветает. Платформа виртуальных мероприятий - это инструмент, который позволит вам воссоздать атмосферу личной конференции или торговой выставки через Интернет.

Сейчас для того что бы участвовать в каком либо мероприятии, участнику необходимо лично подавать документы на участие, что не всегда удобно. Существующая мнемосхема процесса проведения online-мероприятия представлена на рисунке 1.

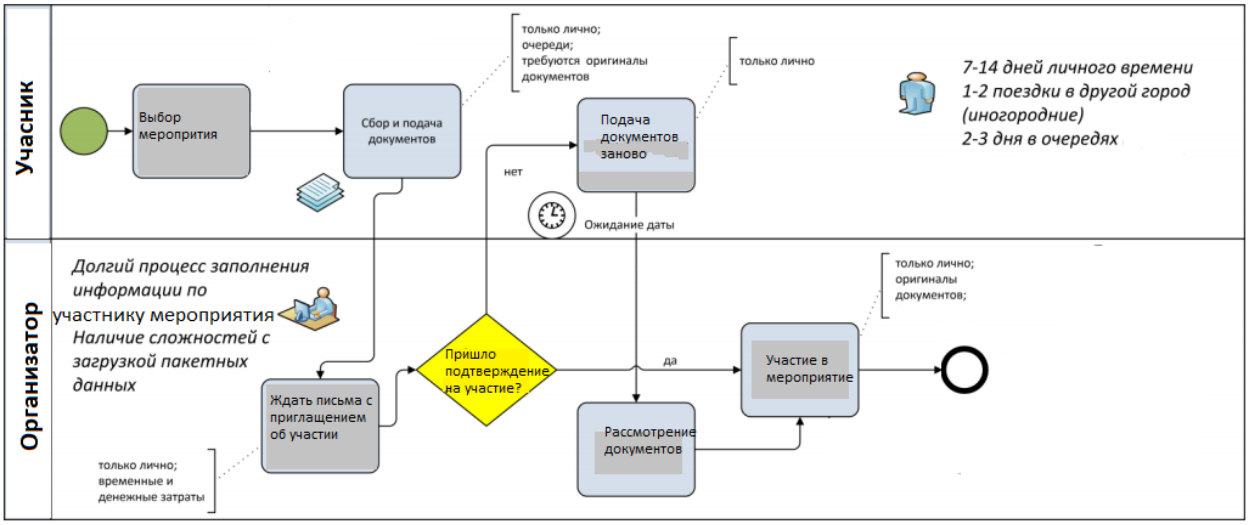


Рис. 1. Мнемосхема существующего процесса проведения мероприятия

Участник, который хочет поучаствовать в мероприятии, должен подать заявку на участие, ее могут не одобрить с первого раза, тогда придется повторно подавать документы. Для того чтобы участнику попасть на конференцию приходиться ехать в другой город или даже страну, на что тратятся деньги и время. География и способы прибытия на мероприятие представлена на рисунке 2.

Рис. 2. География участников мероприятия

Создание web-сервиса для проведения online-мероприятий даст возможность участнику легко принимать в них, а организатору удобство для организации мероприятий.

Мнемосхема предлагаемого процесса проведения online-мероприятия представлена на рисунке 3.

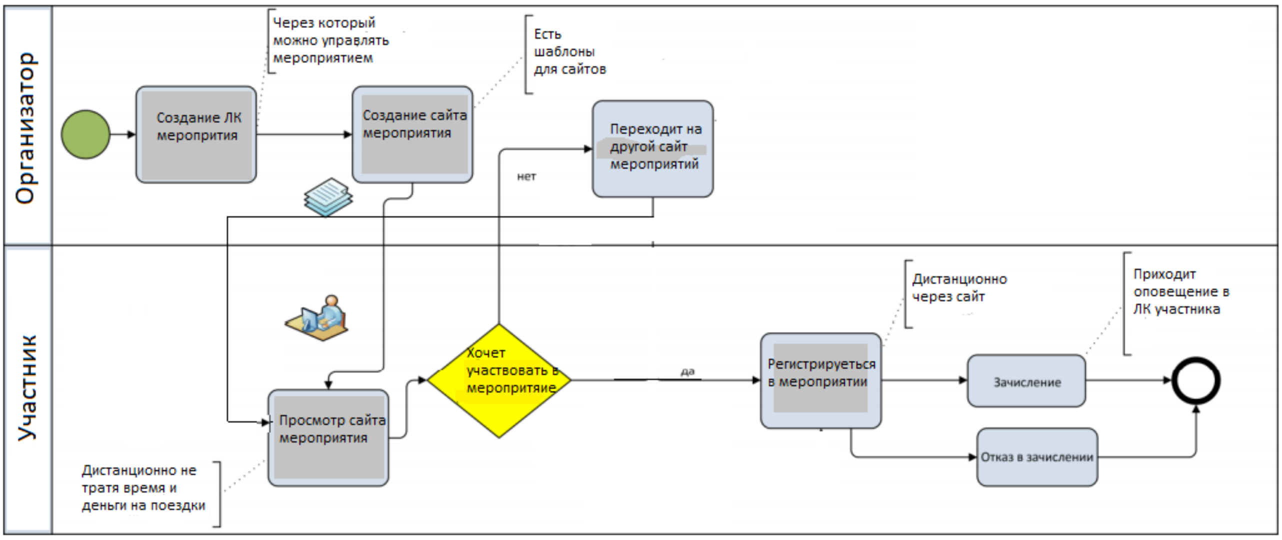


Рис. 3. Мнемосхема предлагаемого процесса проведения online-мероприятия

Организатор заходит на сайт «Платформы для онлайн конференций», где Организатор заходит на сайт «Платформы для онлайн-конференций», где он мо-жет зарегистрироваться, получить доступ к личному кабинету организатора, по-

смотреть текущие, прошедшие, предстоящие мероприятия, а также добавить новое мероприятие. Также организатор создает сайт мероприятия через который участник, который хочет присутствовать на мероприятие, регистрируется или заходит в личный кабинет участника. В личном кабинете участника можно увидеть программу, трансляцию и записи трансляции мероприятия.

Основными преимуществом являются:

1. Независимость от локации. Не нужно собирать участников только в своем городе, теперь аудитория – это вся страна, весь мир!

2. Стоимость проведения. Арендовать помещение, заботиться о питании и проживании спикеров, готовить стенды, печатную продукцию, нанимать звукооператора и осветителя сцены – это лишь крохотная часть на затраты при проведении оффлайн-мероприятий.

3. Легкость привлечения участников. Для того чтобы прийти на мероприятие офлайн, человеку нужно приехать в определенное место к определенному времени и провести там целый день. Для того чтобы прийти на мероприятие в онлайн, человеку нужно просто перейти по ссылке и он уже на мероприятии.

Требования к разрабатываемой ИС:

Платформа должна представлять собой информационную структуру, доступную в сети Интернет. Платформа должна состоять из взаимосвязанных разделов (подсистем и функциональных модулей) с четко разделенными функциями.

– Сайт (Платформа) должен корректно отображаться во всех поддерживаемых десктопных браузерах и мобильных устройствах. Для реализации целей Платформы должны быть внедрены следующие инструменты:

– Конструктор сайтов на основе 9 шаблонов под различные тематики мероприятий;

– Механизм рассылки приглашений через сервер отправки сообщений/стороннее программное обеспечение (в зависимости от количества рассылаемых писем);

– Механизм регистрации участников - на основе внутренней системы;

– Механизм видеоконференции - путем подключения видеохостинга yotube/zoom илидругих путем добавления ссылки на конкретное мероприятие в ЛК участника;

– Механизм сбора статистики - Яндекс метрика/Google аналитика.

Пользовательский интерфейс сайта, разработанный Исполнителем, должен обеспечивать наглядное, интуитивно понятное представление структуры размещѐнной на нѐм информации, быстрый и логичный переход к разделам и страницам. Навигационные элементы должны обеспечивать однозначное понимание пользователем их смысла: ссылки на страницы должны быть снабжены заголовками, условные обозначения соответствовать общепринятым.

Система должна обеспечивать навигацию по всем доступным пользователю ресурсам и отображать соответствующую информацию. Для навигации должна использоваться система контент-меню. Меню должно представлять собой текстовый блок (список гиперссылок) в верхней части страницы.

Для разделов, содержащих подразделы, должно быть предусмотрено выпадающее подменю. При выборе пользователем какого-либо из пунктов меню должна загружаться соответствующая ему информационная страница, а в блоке меню открываться список подразделов выбранного раздела.

Предлагаемое решение, представляющее собой разработку платформы для проведения и организации online-мероприятий, решает проблему их интеграции в цифровое пространство и является экономически более выгодным, чем проведения их offline.

СПИСОК ЛИТЕРАТУРЫ

1. Айриев Г.Б. Деловые онлайн-мероприятия глазами модераторов. Плюсы, минусы и перспективы [Электронный ресурс]. URL: https://event.ru/interviews/delovyie-onlayn-meropriyatiya-glazami-moderatorov-plyusyi-minusyi-i-perspektivyi/ (дата обращения: 01.09.2021).
2. Онлайн-конференции: плюсы, минусы, подводные камни [Электронный ресурс]. URL: https:// https://habr.com/ru/company/jugru/blog/506488/ (дата обращения: 03.09.2021)
3. Румянцев Д.В.,Франкель Н. Event-маркетинг. все об организации и продвижении событий // Питер. – 2017.

УДК 81'322.2

Р. И. КАРИМОВ
karirob@mail.ru
Науч. руководит. – доц., проф. Р. В. НАСЫРОВ

Уфимский государственный авиационный технический университет

NLP – ОБРАБОТКА ЕСТЕСТВЕННОГО ЯЗЫКА. ЛИНГВИСТИЧЕСКИЙ МЕТОД ОБРАБОТКИ ТЕКСТА

Аннотация. В данной работе представлен лингвистический метод обработки текста, который состоит из четырех этапов: графематический анализ, морфологически анализ, синтаксический анализ и семантический анализ.
Ключевые слова: NLP; обработки естественного языка; лингвистический метод.

NLP – обработка естественного языка является актуальным на сегодняшний день. NLP используется в разных сфера жизни. Основными направлениями является: распознавание речи, понимание естественного языка и генерация естественного языка. Основными методами обработки текстов естественного языка является: статический и лингвистический. Суть статического подхода в подсчете количество вхождений слов в документ. Недостатком данного подхода является то, что метод подсчитывает количество слов без учета связанности текста, эту проблему помогает решить лингвистический подход.[1]

Существует четыре этапа лингвистический анализ:

– Графематический анализ;

– морфологический анализ;

– синтаксический анализ;

– семантический анализ.

Рассмотри каждый из этих анализов подробней.

Графематический анализ выполняет начальный этап обработки текста, в результате анализа выделяет элементы структуры текста.

Выделение структурных элементов (абзацев) производится при помощи анализа большего текста следующим способом:

1. подсчет количества символов, которые определяют новый абзац:

– последовательность перевода строки и символа табуляции;

– последовательность перевода строки и двух или более символов пробелов;

– перевод строки, который не удовлетворяет предыдущим условиям.

2. подсчет отношения количества каждой последовательности в текстовом буфере к его размеру.

Задачи графематического анализа:

– выделение слов, разделителей и т.д.;

– разбиение текста на графы;

– выделение абзацев, заголовок, примечаний;

– определение в тексте границ предложений;

– распознавание сокращений, устойчивых оборотов и т.д.

Для определения границ предложений используется словарь сокращений, который содержит в информацию: текст сокращения, информацию о регистре букв в тексте, словосочетания, морфологические характеристики.[2]

Морфологический анализ представляет получение леммы или основы заданного токена или морфологических параметров.

Главной задачей является определить морфологический характер слова и словоформы, сильно завит от выбранного естественного языка.

Теперь разберем каждый из этих терминов.

Токен – это слово, которое отделено от других пребелом или другим знаком препинания. Пример: самолет, под, перелет, дом.

Лемма – это начальная форма слова, то есть без окончания. Изменение начальной формы слова при помощи добавления окончания называется «флексия». Пример: дом (начальная формы) добавляем флексию (а) и получаем новый токен (дома).

Грамматическими параметрами являются: часть речи, род, число, падеж, притяжательность и т. д. Пример: дом (сущ., муж. род, ед. ч., им. п.)

Словоформа – это группа, состоящая из токена, ее леммы и грамматических параметров. Пример: дома, дома (сущ., муж. род, ед. ч., им. п.), дома связан с начальной формы дом и имеет следующие параметры: (сущ., муж. род, множ. ч, им. п.)

Лексама – это множество слов, которые образованы от общей начальной формы. Примеры: начальная форма (лемма) дом, в этому случае лексемами будут дома, домах.

Синтаксический анализ представляет собой определение синтаксических зависимости слов в приложении.

Имеет две задачи: проверить, что предложение сформирована корректно и создать структуру(граф), наглядно показывающую синтаксические отношения между словами. Синтаксический анализатор использует словарь определенных слов (лексикон) и набор синтаксических правил (грамматика). Простой лексикон содержит только синтаксическую категорию каждого слова, простая грамматика описывает правила, которые указывают как синтаксические категории, могут быть объединены для формирования фраз разных типов. Не все системы NLP требуют полного разбора предложений.[3]

Пример: Колобок покатился в густой лес

Таблица 1

Лексикон

Слово	Категория
колобок	существительное
покатился	глагол
в	предлог
густой	прилагательное
лес	существительное

В таблице 1 показан лексикон.

Таблица 2

Грамматика

Предложение	существительное глагол ГруппаСущ
ГруппаСущ	предлог ГруппаПрилагСущ
ГруппаПрилагСущ	прилагательное существительное

В таблице 2 представлена грамматика.

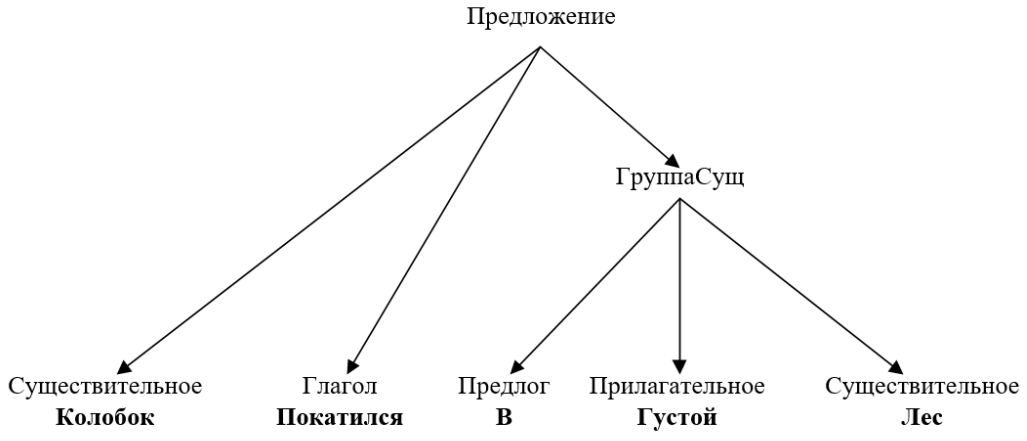


Рис. 1. Синтаксический анализ предложения

На рисунке 1 представлен синтаксический анализ предложения

Семантический анализ – определение смыслового понимания текста

Конечной целью системы обработки естественного языка является «понимание» текста. Данный этап зависит от результатов предыдущих этапов системы и лексической информации.

Модели семантического анализа текста

Тезаурус – словарь, в котором представлены семантические отношения между лексическими значениями. С помощью тезаурусу можно понять смысл слов не только с определения, но и сопоставляя с другими понятиями и группами. В большинстве случае в тезаурус записываются синонимы, антонимы, гиперонимы, паронимы и т. д. [4]

Семантическая сеть представляет из себя граф, в которой имеются концепты предметов, событий, состояний и с представлено отношение между концепций.

Фреймовые модели – это структура, которая описывает понятия или ситуации, состоящая из характеристик ситуации и их значения. Данная модель является элементом семантической сети.

Онтологическая модель – это подробное описание предметной области, которое можно использовать для формулировки утверждений общего характера. Данная модель помогает создавать понятия, которые в будущем будут пригодны для машинной обработки.[4]

СПИСОК ЛИТЕРАТУРЫ

1.Обзор методов автоматической обработки текстов на естественном языке/ Белов С.Д., Зрелова Д.П., Зрелов П.В., Кореньков В.В.// Системный анализ в науке и образовании -2020. -№3. -С. 8-22.
2. Ерина И.С., Попов А.А. Анализ метода обработки естественного языка // MODERN SCIENCE -2020. -№7-1. -С 393-402.
3.Автоматическая обработка текстов на естественном языке и анализ данных: Учебное пособие / [Большакова Е.И и д.р.] - — М.: Изд-во НИУ ВШЭ, 2017. — 269 с.
4. Черницова Л.В. Методы и модели семантического анализа текста// Методы и модели семантического анализа текста-2017. -№11 -С 171 – 173

УДК 004.42

Е. Ю. МОХОВА
mohovakatyasv@mail.ru
Науч. руководит. – канд. техн. наук, доц. Н. И. ФЕДОРОВА

Уфимский государственный авиационный технический университет

ПРОБЛЕМА ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ ПРОЦЕССА ДОСТАВКИ ТОПЛИВА ДЛЯ ТРАНСПОРТА

Аннотация. Рассматривается проблема повышения эффективности процесса доставки топлива для транспорта, проводится анализ доставки топлива для транспорта, описываются достоинства разработки мобильного приложения доставки топлива.
***Ключевые слова*:** мобильное приложение; доставка; АЗС; топливо; цифровое пространство.

В наш стремительный век, когда современному человеку необходимо быт «одновременно в нескольких местах», люди стараются приобрести личное автотранспортное средство для того, что бы сделать свою жизнь удобнее и мобильнее. Сейчас наличие в каждой семье уже не одного, а нескольких автомобилей стало нормой.

На начало 2020 года количество автотранспорта всех типов в России оценивалось экспертами в размере 59 млн. единиц, что на 15 млн. больше начала 2010 года. Все это ведет к увеличению спроса на топливо, увеличению количества автомобильных заправочных станций.

В настоящее время распространены автозаправочные станции стационарного типа, которые располагаться не всегда в удобном месте для водителя, находиться не походу движения автотранспорта, далеко от дом или работ, неудобный подъезд к АЗС, пробка по ходу движения автотранспорта, на них могут быть большие очереди, которые возникают из-за приема нефтепродуктов или внеплановых работ. Иногда расположены рядом, ноне той компании, которую предпочитает водитель в силу цены на топливо или наличия различных акций. Так же при личном посещении автозаправочной станции существует опасность заразиться новой коронавирусной инфекцией. На рисунке 1 представлена мнемосхема процесса заказа и получения топлива на стационарной АЗС.

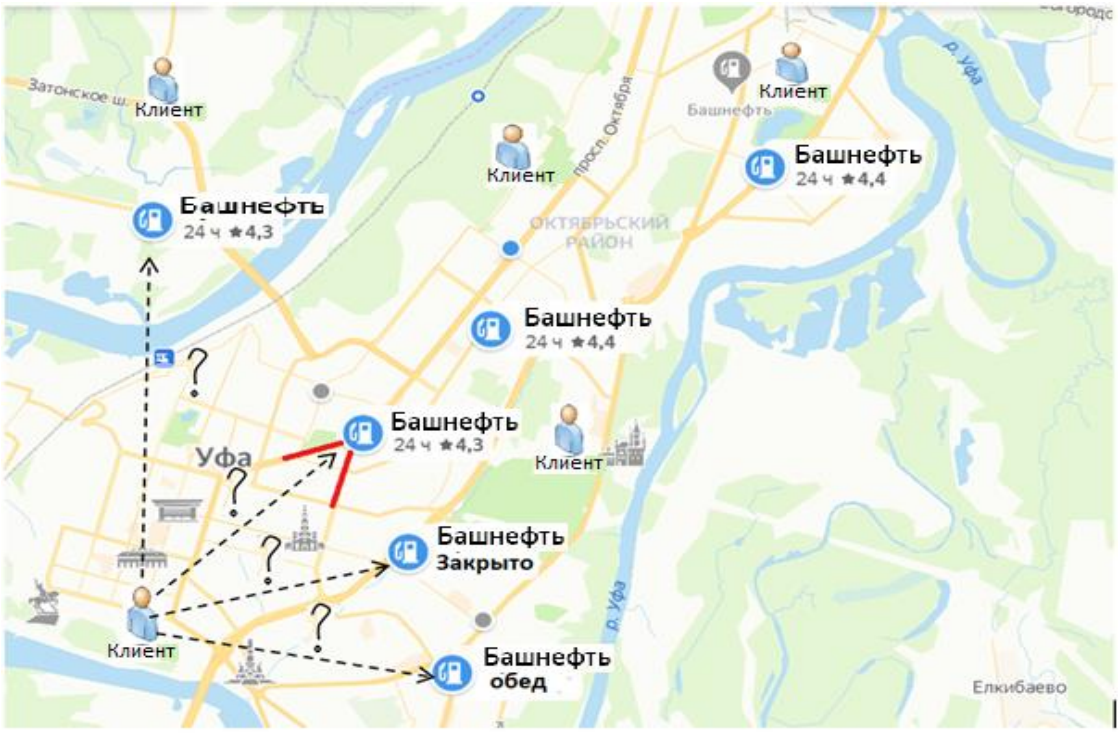


Рис. 1. Мнемосхема существующего процесса заказа топлива

Клиент, покупающий топливо, должен заехать на заправку, подъехать к нужной колонке, вставить пистолет в бензобак автомобиля, зафиксировать его, подойти к кассе, заказать у кассира необходимое количество топлива, оплатить указанную сумму. Вернуться к автомобилю, дождаться пока закончит заправляться машина, вынуть пистолет из бензобака автомобиля, убрать обратно на бензоколонку, сесть в автомобиль и продолжить движение в нужную сторону. Из-за этого, человек теряет драгоценное время, опаздывая на важное совещание, работу, учебу. Приблизительное время заправки автомобиля на стационарной автомобильной заправочной станций в среднем занимает около 18 минут.

В настоящее время можно воспользоваться существующими сервисами, где клиент может заказать топливо заранее через различные приложения, но получить топливо он может только лично, приехав на автомобильную заправочную станцию и залив топливо.

На рисунке 2 представлено среднее время, затрачиваемое на заправку автомобиля на стационарной автомобильной заправочной станции.

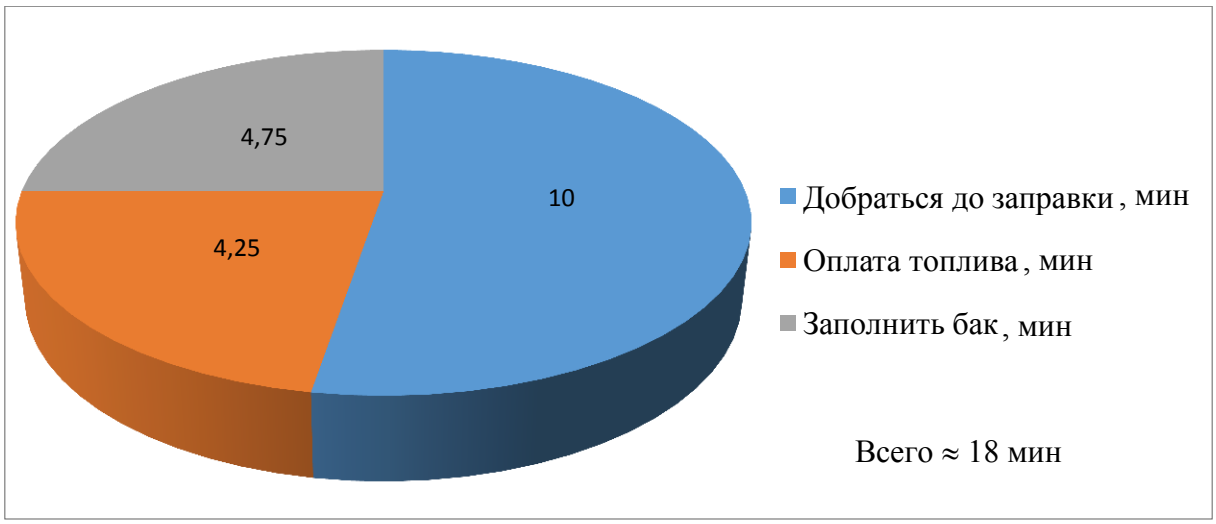


Рис. 2. Среднее время, затрачиваемое на заправку автомобиля на автоматической заправочной станции

Предлагается разработать мобильное приложение, через которое покупатель (клиент) будет заказывать доставку топлива, куда ему будет удобно. Пока покупатель занят своими делами, приезжает курьер, заправляет автомобиль покупателя и уезжает. Покупателю даже не нужно присутствовать при заправке, необходимо будет открыть только лючок у бензобака. Станет проще планировать свой день, не тратя время, что бы заехать на заправку и ждать в очереди. После введения информационной системы, процесс заказа и получения топлива будет выглядеть следующим образом (рисунок 3).

Клиент, обращаясь к мобильному приложение создает заказ. Оператор следит за поступающими заказами через свой сайт и вручную передает заказ курьеру, который будет доставлять топливо заказчику, курьер видит поступившие ему заказы через свое мобильное приложение «Мобильная АЗС курьер». Покупатель топлива может не присутствовать при заправке своего автомобиля, в таком случае нужно будет оплатить заказ через мобильное приложение «Мобильная АЗС» и оставить лючок бензобака открытым. Курьер, ориентируясь на марку и место расположения автомобиля, произведет заправку нужным топливом и уедет.

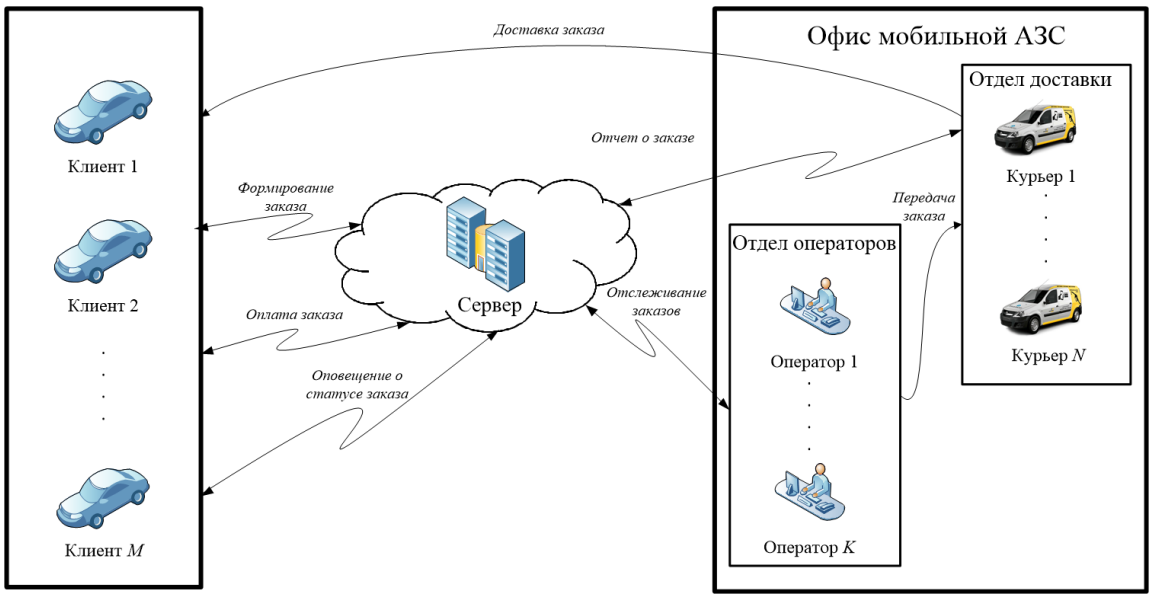


Рис. 3. Мнемосхема предлагаемого процесса доставки топлива

Таким образом, можно спланировать свой день до мелочей, не тратя время на заправку и очереди, не бояться заразиться новой коронавирусной инфекцией. Кроме того, современные люди предпочитают делать закупки через Интернет, потому что это можно совершать в комфортных домашних условиях

Основными преимуществом данного приложения является:

1. Отсутствие привязки к территориальному расположению. Точность доставки будет определяться не конкретным местом (расположением заправочной станции), и точными координатами места стоянки автомобиля, которому необходимо заправиться;

2. Экономия времени при заправке автомобиля, т.е. отсутствие очереди, пробок;

3. Заправка автомобиля без его владельца.

4. Возможность заправки крупногабаритного, маломобильного транспорта (комбайны, катера, асфальтоукладчики).

В наше время все активнее пользуются планшетами, мобильными телефонами, в связи с этим большое внимание уделяется разработкам различных мобильных приложений. Мобильные приложения захватывают практически все сферы быта. Компаниям различные мобильные приложения позволяют повысить эффективность своего бизнеса, разрабатывать новые каналы для общения

с клиентами. Разработка мобильных приложений позволяет компаниям более широко общаться с клиентами без привлечения большего количества сотрудников, так как при использовании мобильных приложений большую часть интересующих клиента вопросов он может решить самостоятельно

Разработка предлагаемого мобильного приложения позволит осуществлять заказ и доставку топлива для транспорта в удобное место для клиента, сократит время, затрачиваемое на этот процесс, поможет в разработке новых каналов общения с клиентами. Заправка автомобиля станет более удобной и комфортной, чем была раньше.

СПИСОК ЛИТЕРАТУРЫ

1. Российский автопарк [Электронный ресурс]. URL: https://starlube.ru/news/novosti-rynka/ – (дата обращения 18.09.2021г.)
2. Автоматизация предприятий, что это такое. [Электронный ресурс] – Режим доступа URL: http://www.itmservice.ru/info/avtomatizaciya-predpriyatiya/ – (дата обращения 18.09.2021г.)
3. Трофимов О.В., Ефимычев Ю.И., Ефимычев А.Ю., Шипилов А.Г. Модернизация предприятий промышленности: концепция, стратегии и механизм реализации // Креативная экономика. – 2011. Т. 5, №11.

УДК 004.021

Д. А. ПОЛОНСКИЙ, А. О. ФЕДОСОВА
kHRYSTALq@gmail.com, fedos_anastasiya@bk.ru
Науч. руководов. – канд. техн. наук, доц. Р. В. НАСЫРОВ

Уфимский государственный авиационный технический университет

ПРЕДОБРАБОТКА ТЕКСТА ДЛЯ РЕШЕНИЯ NLP (NATURAL LANGUAGE PROCESSING)

Аннотация. Рассматриваются методы предварительной обработки текста для дальнейшей работы с алгоритмами машинного обучения.
Ключевые слова: предобработка; NLP; natural language processing; токенизация; стоп-слова; лемматизация; стемминг.

Предобработка текста переводит текст на естественном языке в формат удобный для дальнейшей работы. Предобработка состоит из различных этапов, которые могут отличаться в зависимости от задачи и реализации.

Как правило, первым шагом обработки текста является нормализация. Эта операция, в результате которой тексты приводятся к нужному регистру, удаляются знаки пунктуации (обычно реализуется как удаление из текста символов из заранее заданного набора), удаляются числа (или приводятся к другому формату), удаляются пробельные символы. Нормализация необходима для унификации методов обработки текста [1].

Следующим шагом является токенизация, которая заключается в разбиении длинных строк на более короткие. Обычно используется токенизация по словам.

В случае разбиений на предложения нужно просто найти точку, вопросительный или восклицательный знак. Но в русском языке существует сокращения, в которых есть точка, например, *к.т.н.* – кандидат технических наук или *т.е.* – то есть. Вследствие этого могут возникать ошибки, но Python-библиотека NLTK позволяет избежать этой проблемы.

Рассмотрим пример:

```
>>> from nltk.tokenize import sent_tokenize
```

>>> text = "Мой научный руководитель – доцент и к.т.н., т.е. он имеет множество публикаций. А также грантов и научных проектов."
>>> sent_tokenize(text, language="russian")
[' Мой научный руководитель – доцент и к.т.н., т.е. он имеет множество публикаций.', ' А также грантов и научных проектов.']

Функция *sent_tokenize* разбила исходное предложения на два, несмотря на присутствие слов к.т.н. и т.е.

Помимо разбиения на предложения в NLTK можно в качестве токенов использовать слова:

>>> from nltk.tokenize import sent_tokenize, word_tokenize
>>> text = "Мой куратор тоже к.т.н. По образованию он инженер-проектировщик."
>>> word_tokenize(text, language="russian")
['Мой ', 'куратор ', 'тоже', 'к.т.н.', '.', 'По', 'образованию', 'он' 'инженер-проектировщик', '.']

Здесь к.т.н. и инженер-проектировщик были определены как отдельные слова.

После токенизации важным шагом является удаление стоп-слов. Стоп-слова – это слова, которые не несут смысловой нагрузки. В русском языке, например: союзы, предлоги [1].

Библиотека NLTK также имеет список стоп-слов, всего в него входит 151 слово. Некоторые из них: и, в, во, не, что, он, на, я, с, со, как, а, то, все, чтоб, без, будто, впрочем, хорошо, перед, иногда, лучше, чуть, том, нельзя, такой, им, более, всегда, конечно, всю, между.

Поскольку это список, то к нему можно добавить дополнительные слова или, наоборот, удалить из него те, которые будут информативными для вашего случая. Например, для последующего исключения слов из токенизированного текста можно написать следующее:

```
for token in tokens:
    if token not in stop_words:
        filtered_tokens.append(token)
```

Следующим шагом является стемминг. Количество корректных словоформ, значения которых схожи, но написания отличаются суффиксами, приставками, окончаниями и прочим, очень велико, что усложняет создание слова-

рей и дальнейшую обработку [2]. Стемминг позволяет привести слово к его основной форме. Суть подхода в нахождении основы слова, для этого с конца и начала слова последовательно отрезаются его части. Правила отсекания для стеммера создаются заранее, и чаще всего представляют из себя регулярные выражения. В Python-библиотеке NLTK для этого есть *SnowballStemmer*, который поддерживает русский язык:

```
>>> from nltk.stem import SnowballStemmer
...
>>> snowball = SnowballStemmer(language="russian")
>>> snowball.stem("Хороший")
хорош
>>> snowball.stem("Хорошая")
хорош
```

Проблемы возникают со словами, которые значительно изменяются в других формах:

```
>>> snowball.stem("Хочу")
хоч
>>> snowball.stem("Хотеть")
хотет
```

В этом случае, следует использовать лемматизацию, так как "хочу" и "хотеть" – грамматические формы одного и того же слова.

Лемматизация является альтернативой стемминга [2]. Основная идея в приведении слова к словарной форме — лемме.

Например, для русского языка:

для существительных — именительный падеж, единственное число;

для прилагательных — именительный падеж, единственное число, мужской род;

для глаголов, причастий, деепричастий — глагол в инфинитиве несовершенного вида.

Отличие в том, что стеммер действует без знания контекста и, соответственно, не понимает разницу между словами, которые имеют разный смысл в зависимости от части речи. Однако у стеммеров есть и свои преимущества: их проще внедрить, они работают быстрее.

Например, *хочу, хотят, хотели* имеют начальную форму *хотеть*. В этом случае можем воспользоваться pymorphy2 – инструмент для морфологического анализа русского и украинского языков.

```
>>> import pymorphy2
>>> morph = pymorphy2.MorphAnalyzer()
>>> morph.parse("хочу")
[Parse(word='хочу', tag=OpencorporaTag('VERB,impf,tran sing,1per,pres,indc'), normal_form='хотеть', score=1.0, methods_stack=((<DictionaryAnalyzer>, 'хочу', 2999, 1),))]
```

Метод parse возвращает список объектов Parse, которые обозначают виды грамматических форм анализируемого слова. Такой объект обладает следующими атрибутами:

– *tag* обозначает набор граммем. В данном случае слово хочу – это глагол (VERB) несовершенного вида (impf), переходный (tran), единственного числа (sing), 1 лица (1per), настоящего времени (pres), изъявительного наклонения (indc);

– *normal_form* – нормального форма слова;

– *score* – оценка вероятности того, что данный разбор правильный;

– *methods_stack* – тип словаря распарсенного слова с его индексом.

По умолчанию объекты Parse сортированы в порядке убывания значения score. Поэтому из списка лучше всего брать 1-й элемент:

```
>>> morph.parse("хотеть")[0].normal_form
хотеть
>>> morph.parse("хочу")[0].normal_form
хотеть
>>> morph.parse("хотят")[0].normal_form
хотеть
```

Следовательно, мы получили одно слово из разных его форм.

Векторизация. Большинство математических моделей работают в векторных пространствах больших размерностей, поэтому необходимо отобразить текст в векторном пространстве. Основным подходом является мешок слов: для документа формируется вектор размерности словаря, для каждого слова выделяется своя размерность, для документа записывается признак насколько часто

слово встречается в нем, получаем вектор. Наиболее распространенным методом для вычисления признака является TF-IDF (TF — частота слова, term frequency, IDF — обратная частота документа, inverse document frequency). TF вычисляется, как счетчиком вхождения слова. IDF обычно вычисляют как логарифм от числа документов в корпусе, разделенный на количество документов, где это слово представлено. Таким образом, если какое-то слово встретилось во всех документах корпуса, то такое слово не будет никуда добавлено.

СПИСОК ЛИТЕРАТУРЫ

1. Васильев, Ю.А. Обработка естественного языка. Python и spaCy на практике [Текст] / Ю.А. Васильев. – Санкт-Петербург: Питер, 2021. – 256 с.
2. Хобсон, Л. Обработка естественного языка в действии [Текст] / Л. Хобсон, Х. Ханнес, Х. Коул. – Санкт-Петербург: Питер, 2020 – 576 с.

УДК 004

Н. С. САЯПИН
koljas98@mail.ru
Науч. руководов. – док. техн. наук, проф. О. Я. БЕЖАЕВА

Уфимский государственный авиационный технический университет

СРАВНИТЕЛЬНЫЙ АНАЛИЗ СРЕД РАЗРАБОТКИ ИГРОВЫХ ПРИЛОЖЕНИЙ

Аннотация. в данной статье предложен сравнительный анализ игровых движков Unity3D, Unreal Engine 4, CryEngine, Godot, рассмотрены их особенности, преимущества и недостатки.

На сегодняшний день рынок развлечений является одним из самых популярных. Благодаря своей доступности наиболее популярными являются компьютерные игры, которые занимают досуг и выполняют обучающую роль. В отличие от других видов развлечений, благодаря интернету компьютерные игры доступны любому пользователю с доступом во всемирную паутину. Массовая разработка игр стала реальной из-за того, что появились новые игровые движки, которые сильно упрощают процесс разработки.

Игровой движок — это базовое программное обеспечение, благодаря которому разрабатывается игра. В него входит несколько подсистем такие как: звуковая, графическая, физическая, такие системы называются модульными.

Unity

Unity – кроссплатформенная среда разработки двумерных и трехмерных компьютерных игр, разработанная американской компанией Unity Technologies. Поддерживает практически все операционные системы: Windows, Android, IOS, Linux, PlayStation, Xbox и многие другие. Есть возможность создавать приложения для запуска их в браузерах, с помощью технологии WebGL.

Редактор Unity имеет простой и понятный Drag&Drop интерфейс, который интуитивно понятен и его легко настроить. Платформа поддерживает язык программирования C# дополненный своими библиотеками. Расчеты физической составляющей производил PlhysX от NVIDIA.

Однако простота работы системы имеет за собой ряд недостатков: не очень богатый базовый функционал, среда предоставляет не самую лучшую графику.

Вес проект Unity состоит из сцен (уровней) — игровых миров, каждый со своим набором настроек, объектов и сценариев их поведения.

Бесплатная версия программы имеет некоторые ограничения, но это не сильно мешает разработке. Бесплатная версия действует при ежегодном доходе приложения менее 100 000$.

Unreal Engine 4

Unreal Engine 4 – среда разработки, поддерживаемая компанией Epic Games. Позволяет разрабатывать игровые приложения для большинства операционных систем.

В отличии от ближайшего конкурента (Unity) среда позволяет создавать проекты более высокого качества. Движок предоставляет мощный редактор, содержащий несколько более узкоспециализированных редакторов, освоение которых очень помогает в разработке. Все элементы представлены в виде объектов со своими характеристиками и класса, который определяет доступные характеристики. Для описания моделей поведения объектов используется язык C++, а так же можно использовать визуальные скрипты Blueprint.

Unreal Engine поддерживает связь клиента с сервером с помощью простого инструмента создания выделенного сервера для 64 одновременных пользователей, однако это ограничение можно обойти с использованием плагинов.

Большое количество видео-уроков в сети сильно повышает конкурентоспособность данной среды.

Так же у среды есть и свои минусы:

– программа и все разработанные на ней игры занимаю много места;

– из-за большого количества возможностей увеличивается сложность разработки;

– интерфейс достаточно сложен для освоения

Платформа бесплатна, но пользователи обязаны перечислять 5% от мирового дохода, когда он превысит 3 000 долларов.

CryEngine

CryEngine — инструмент, разработанный студией Crytek и нацеленный на разработку игр под платформы: Windows, PlayStation, Xbox.

В отличии от предыдущих сред разработки, предназначен для более сложных проектов, ориентирован на производство многопользовательских онлайн игр с продвинутой графикой. Платформа является полностью коммерческой, но есть бесплатная версия для некоммерческого использования. Объекты управляются скриптами, основанными на языке Lua.

Движок достаточно сложен в освоении и требует от разработчика большого опыта работы с ним.

Godot

Godot является игровым движком с открытым исходным кодом. В среде большое внимание уделяется наличию отличных инструментов и визуально-ориентированному рабочему процессу. Разработку можно производить на ПК, мобильные и web- платформы. Это кроссплатформенный двумерный и трехмерный игровой движок.

По опросу разработчиков выявлено, что они отмечают, он идеально подойдет для новичков, простота разработки прельщает. Так же в среде есть возможность подключения огромного количества плагинов, что делает разработку игр в данной среде заметно проще, так же дает возможность разрабатывать более масштабные проекты.

Godot имеет небольшой вес программы и созданных игр, что является существенным плюсом для разработчиков и конечных пользователей.

В данном движке используется язык разработанный специально для данной среды GDScript, который сильно похож на Python, так же можно использовать C#.

Основным недостатком данной среды разработки является его простота, что не позволяет разрабатывать масштабные проекты без достаточной модификации.

Таким образом, сравнительный анализ вышеупомянутых сред разработки игровых приложений показал, что на текущий день существуют как движки, которые предоставляют мощные инструменты, которые позволяют создавать масштабные игры, но и среды с небольшим, простым функционалом, подходящим для начинающих разработчиков.

Отмечу, что на данный момент нет среды разработки, которая бы подходила по требованиям всем проектам и разработчикам. Именно поэтому необходимо выбирать не самую лучшую среду, а самую подходящую для конкретного проекта, ведь проект должен быть реализован вовремя, с каждым днем простоя он становится все менее актуален.

СПИСОК ЛИТЕРАТУРЫ

1. Дмитриев В.С., Зоткина А.А. Сравнительный анализ мультиплатформенных движков для разработки игр // Современные технологии: актуальные вопросы, достижения и инновации сборник статей XXXIII Международной научно-практической конференции
2. Романов Д.С. Разработка мультиплеерной игры на платформе Unity 3D // Научный журнал. 2018. №6 (29).
URL: https://cyberleninka.ru/article/n/razrabotka-multipleernoy-igry-na-platforme-unity-3d
3. Unity и C#. Геймдев от идеи до реализации Гибсон Б. 2019

УДК 005.6

А. В. ТИМОФЕЕВ
timofeev461@yandex.ru
Науч. руководов. – канд. техн. наук, проф. Н. И. ФЁДОРОВА

Уфимский государственный авиационный технический университет

МЕТОДИКА SERVQUAL ДЛЯ ИЗМЕРЕНИЯ КАЧЕСТВА БАНКОВСКИХ УСЛУГ

Аннотация. В текущих рыночных условиях, когда разница предоставляемых услуг становится менее заметными, для сохранения лидирующих позиций и повышения конкурентоспособности банковским компаниям следует уделять больше внимания качеству продукции и поставляемых услуг. Для повышения качества работы необходима информация о качестве работы со службами и отделениями банка, а также проведение опросов и исследований, анализ комментариев и предложений, что особенно актуально для российских региональных банков. Целью данной статьи является изучение методики *SERVQUAL* и возможность ее применения для измерения качества банковских услуг.
Ключевые слова: управление качеством; качество, servqual, сервквал, банковские услуги, оценка.

1. Состояние и важность проблемы

В связи с увеличением числа банков в стране (связано со вступлением России в ВТО) возникает острая необходимость в повышении качества работы банков в связи с усилением конкуренции в условиях более открытой экономики. По мере увеличения числа банков клиенты становятся все более требовательными к кредитным компаниям, поскольку им предоставляется широкий спектр услуг, а цена больше не является определяющим фактором. Теперь качество оказываемых услуг выходит на передний план.

В настоящее время на банковском рынке важно уделять максимальное внимание клиенту и предлагать именно тот спектр услуг, который ему больше всего подходит.

Но сегодня не все кредитные компании в России осознали этот факт, и поэтому существует необходимость в разработке методов и инструментов, способствующих полному пониманию банками клиентов и повышению их удовлетворенности и лояльности [1].

Практика показывает, что конкурентоспособность коммерческого банка может быть обеспечена в том случае, если банк постоянно совершенствует

продукты, обновляя и расширяя спектр услуг, с использование имеющихся финан-
совых ресурсов и внутренних ресурсов для развития, применение современных информационных технологий.

Но даже в случае их успешной реализации банк не достигнет ожидаемых результатов, не сосредоточившись на максимальном удовлетворений требований и ожиданий клиента. Управление знаниями о потребителях становится приоритетом для любого банка, независимо от размера и масштабов его деятельности, обеспечивая его реальную конкурентоспособность, поскольку быстрое увеличение числа кредитных компаний приводит к смещению акцента на обеспечение качества услуг [2].

Определение требований клиента является основополагающим принципом современного менеджмента, являясь основой почти всех успешных бизнес-стратегий. Чтобы привлечь новых клиентов и удержать текущих, банки разрабатывают программы, направленные на повышение привлекательности банковских продуктов. Программы включают такие методы, как удовлетворение потребностей в услугах конкретных групп клиентов, разработка новых банковских продуктов и рекламных мероприятий (в том числе и разработка приложений, отдаленных от банковских услуг), поддержание имидж надежного банка и т.д. Но в настоящее время, банки предоставляют аналогичный набор услуг и большее влияние на клиентов оказывает непосредственно качество этих услуг.

В настоящее время в теории и практике управления качеством существуют инструменты для получения подробной информации от клиента о его предпочтениях и требованиях, а затем использования ее в управлении услугами. Наиболее распространенные методы изучения качества услуг и процессов обслуживания в региональном масштабе заключаются в проведение коммерческими банками опросов, методы тайного покупателя и обработка жалоб. Однако, несмотря на их преимущества, в том числе простоту, низкую стоимость, простоту проведения и обработки результатов, эти методы не всегда позволяют достичь запланированных целей. В частности, эти методы не позволяют региональным кредитным компаниям более полно и эффективно оценивать удовлетворенность клиентов качеством предоставляемых банком услуг. Поэтому бан-

кам необходимо получать от клиента больше информации, используя дополнительные методы и инструменты управления качеством.

Исходя из этого, возникает необходимость в расширении инструментария оценки качества обслуживания клиентов банков. Необходимо узнать, есть ли возможность применения других методов и инструментов управления качеством в этой области, приведет ли это к положительному эффекту и будут ли сделаны новые выводы.

2. Описание методики SEVQUAL в сфере оценки качества банковских услуг

Задача *SERVQUAL* – измерить степень разрыва между Ожиданиями покупателей и Восприятием покупателей (то есть фактическим положением дел). Полученная информация (в форме индексов) используется как один из индикаторов успешности функционирования предприятия, наряду с финансовыми, экономическими и другими показателями

Согласно маркетинговому исследованию востребованности банковских услуг [2] потребители оценивают функциональные и технические аспекты качества банковской услуги по пяти основным критериям:

1) Материальность (оснащенность банка: оргтехника, интерьеры помещений, внешний вид персонала, информационные материалы).

2) Надежность (выполнение обещанной банком услуги точно, основательно и в срок).

3) Отзывчивость (искреннее желание помочь потребителю и быстрое обслуживание в банке).

4) Убежденность (компетентность, ответственность, уверенность и вежливость обслуживающего персонала банка).

5) Сочувствие (выражение заботы и индивидуальный подход к потребителю банковской услуги)

Для измерения пяти критериев качества банковской услуги может быть успешно использована адаптированная методика «*SERVQUAL*».

Принцип данной методики в сфере определения качества банковских услуг разделен на две части. Сначала потребитель с помощью пятибалльной или семи-

балльной шкалы (где 0 это полностью не согласен, а 5/7 – полностью согласен) оценивает каждый из пяти критериев качества банковских услуг. Каждый из этих характеристик имеет подпункты, полная совокупность разделения данных критериев составляет 22 подкритерия. Пользователь должен оценить каждый из этих подпунктов два раза, сначала он ставит ожидаемую оценку от услуги, которая будет предоставлена, а затем с помощью аналогичной шкалы, клиент выставляет фактические оценки от предоставленной услуги. Следующим шагом, данные оценки с помощью метода средних значений группируются в пять коэффициентов качества и высчитываются по формуле $Qi = Pi - Ei$, где Pi – уровень (оценка) воспринятой услуги по i-му фактору (i =1…22), Ei – уровень (оценка) ожидаемой услуги по i-му фактору (i =1…22). На основании полученных 22 значений качества можно получить общий индекс качества услуг (*SQI*), который рассчитывается как суммарное среднее значение всех 22 коэффициентов качества. После того как сбор информации об ожиданиях и восприятии обслуживания покупателями завершен, она анализируется, и полученные выводы используются для установления стандартов и разработки системы предоставления высококачественного сервиса [4].

Подход качества *SERVQUAL* позволяет получить сведения о существующих ожиданиях клиента относительно процесса взаимодействия с компанией, предоставляющей услуги. С помощью данного метода, появляется возможность определить главные для потребителя характеристики оценки качества обслуживания. Опрос с использованием методики *SERVQUAL* позволяет определить, как потребитель оценивает услугу в разрезе основных параметров качества, и выявить их неудовлетворенные потребности. Полученная оценка, которая была выявлена с помощью сравнения предварительного ожидания и итогового восприятия более точна и корректна, чем принятое измерение удовлетворенности клиента от предоставленной услуги.

СПИСОК ЛИТЕРАТУРЫ

1. Беляева, Л.А. Уровень и качество жизни. Проблемы измерения и интерпретации // Социс. – 2009. - №1. – С.33-42.
2. Андреев И. Критерии конкурентоспособности однородных банковских услуг / Маркетинг. -1998. № 1. С. 22-41.
3. Гуреева Е.П., Миронов Н.А., Булганина С.В., Лебедева Т.Е., Маркетинговое исследование востребованности банковских услуг // Московский экономический журнал. 2020, № 6.
4. Копанева, И. Н. Как измерить удовлетворенность потребителя // Методы менеджмента качества. 2003. № 6. С. 21-26.

УДК 004.93

Р. З. ХАМЗИН
khamzin.ruslan.z@mail.ru
Науч. руководитель – канд. техн. наук, доц. Р. В. НАСЫРОВ

Уфимский государственный авиационный технический университет

ПРОБЛЕМА ИНТЕГРАЦИИ УСТАРЕВШИХ LEGACY-УСТРОЙСТВ В ЦИФРОВОЕ ПРОСТРАНСТВО

Аннотация. рассматривается проблема интеграции устаревших устройств в цифровое пространство, проводится анализ существующих решений и предлагается решение в виде разработки приложения для распознавания изображений с показаний legacy-устройств.
***Ключевые слова*:** legacy-устройство; распознавание; изображение; интеграция; оборудование; цифровое пространство.

Введение

Во многих российских компаниях, промышленных предприятиях, заводах, цехах до сих пор продолжается использование значительного количества устаревшей техники, унаследованных систем (legacy-устройств), имеющих низкую вычислительную мощность и не обладающих интерфейсами информационного обмена. Аналогичная проблема в частном домашнем секторе, у многих рядовых пользователей установлены устаревшие приборы учета, имеется в использовании старая техника, не имеющая каналов информационного обмена. Как следствие, данные с таких датчиков, устройств, приборов и систем собираются пользователями вручную на бумажные носители.

В 2017 году 45% промпредприятий располагали машинами и оборудованием в возрасте от 10 до 30 и более лет, сообщает Центр конъюнктурных исследований (ЦКИ) ИСИЭЗ НИУ ВШЭ по результатам мониторинга «Инвестиционная активность российских промышленных предприятий в 2017 г.»

Вопреки установкам на импортозамещение, значительная часть организаций закупала зарубежное оборудование: 43% – новое, 30% – бывшее в употреблении. Лидировали угледобытчики, металлурги, производители табачных изделий, кокса и нефтепродуктов, лекарственных средств, транспорта, компьютеров и электронных изделий.

Для автоматизации и оптимизации бизнес-процессов производственных предприятий, решения проблемы с устаревшей техникой в частном домашнем секторе есть два способа интеграции современного оборудования с унаследованным.

Известным способом решения проблемы является замена устаревшего оборудования на современное. Замена устаревшего оборудования означает миллионы капитальных затрат и годы планирования, не говоря уже о значительных инвестициях в управление цепочкой поставок, улучшение процессов, системы безопасности, обучение операторов. Установка нового оборудования может создать необходимость в привлечении нового персонала, более квалифицированного и, соответственно, более требовательного в плане оплаты труда. Оборудование приобретается с учетом того, что оно прослужит десятилетия и может амортизироваться в течение срока его полезного использования. Также, при таком решении, возникает проблема с утилизацией заменяемого устаревшего оборудования, что подразумевает значительные материальные затраты.

Предлагаемый способ решения проблемы подразумевает интеграцию существующих персональных устройств пользователей с достаточной вычислительной мощностью и каналами информационного обмена (ПК с веб-камерами, смартфоны и т.д.) для организации информационного канала с унаследованными устройствами.

Информационный канал с унаследованными устройствами формируется путем снятия изображений либо видеопотока показаний датчиков и приборов с камеры современного персонального устройства с дальнейшим распознаванием полученной визуальной информации. Далее полученные данные предполагается выводить в онлайн и облачные платформы.

Для реализации такого решения требуется разработка соответствующего программного обеспечения для современных персональных устройств, обеспечивающего точный сбор и передачу информации.

Текущее состояние вопроса

Обзор публикаций, в которых изложены результаты в этой области. [*Библиографическая ссылка на статью: Дзеник А.Д. Проблема технически устаревшего оборудования и способы его решения // Современная техника и технологии. 2017. № 1 [Электронный ресурс]. URL: https://technology.snauka.ru/2017/01/11696 (дата обращения: 12.07.2021).*]

В статье поднимается проблема технически устаревшего оборудования на предприятиях. Отмечается, что предприятия использующие устаревшее оборудование несут значительные потери и проигрывают по показателям качества тем, что используют новое оборудование. Описываются проблемы, возникающие в случае замены устаревшего оборудования новым.

В статье приводится лишь общий вывод о том, что эффективным и рациональным решением является модернизация устаревшего оборудования, а не замена его новым.

Модернизация старого оборудования

Меженный Евгений Викторович

Руководитель отдела АСУ электротехнического завода ASD-electric

https://www.elec.ru/publications/tsifrovye-tekhnologii-svjaz-izmerenija/805/

Отмечается, что наилучшим способом является установка современного оборудования взамен устаревшего, но поскольку это дорогостоящий способ и в этом случае процесс остановится для монтажных работ, то предлагается решение в виде замены устаревшего оборудования в несколько стадий. Это постепенное внедрение нового оборудования в виде ПЛК и дополнительных датчиков, которые будут собирать необходимую информацию.

Способ, описываемый в публикации подразумевает значительные материальные затраты, этот способ также не является оптимальным, так как технологии постоянно развиваются и скорость этого развития становится только больше, соответственно техническая актуальность нового оборудования скоротечна и вложенные средства себя не окупают.

Проблема legacy-устройств присутствует и в частном домашнем секторе. К примеру, замена классических энергомеров и приборов учета на современные умные счетчики стоит значительных материальных затрат. Так, замена счетчика электричества на «умный» обойдется потребителю в 12-15 тыс. рублей, базовый комплект для замены счетчика воды от 45 тыс. рублей до 47 тыс. рублей, «умный» счетчик газа обойдется от 10 тыс. рублей. Таким образом, если полноценно внедрять «умную» систему приборов учета, это обойдется потребителю в сумму от 112 тыс. рублей.

Предположим, что клиентская база состоит из 100 000 квартир, оборудованных счетчиками старой конструкции, тогда переоборудование всей базы обойдется порядка 10 млрд рублей.

В тоже время, разработка предлагаемого приложения обойдется в сумме в пределах 1 млн рублей.

Мнемосхемы и требования

Сейчас для того чтобы пользователю взаимодействовать с legacy – устройством и контролировать его параметры, нужно вести на бумажном носителе записи в виде журнала показаний, хранить бумажный носитель и, в случае необходимости, обращаться к нему, что не всегда удобно, практично и надежно.

Мнемосхема существующего процесса использования legacy-устройства приведена на рисунке 1.

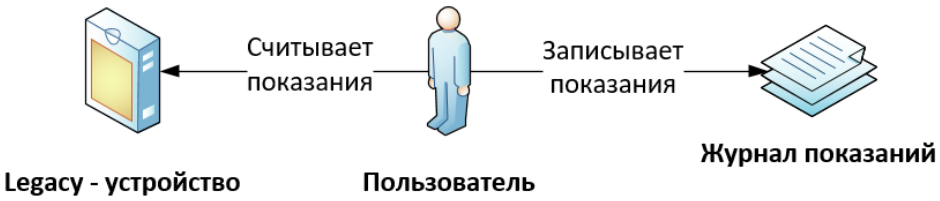


Рис. 1. Мнемосхема существующего процесса

Создание приложения по распознаванию изображений даст возможность пользователю снимать и загружать изображения с показаниями legacy-

устройств со своего персонального устройства, распознавать их и хранить результаты распознавания в электронном виде.

Мнемосхема предлагаемой интеграции персонального устройства пользователя в процесс использовании legacy-устройства приведена на рисунке 2.

Рис. 2. Мнемосхема предлагаемого процесса

Предлагаемое приложение обеспечит быструю загрузку показаний с legacy-устройств в информационную систему, их хранение в электронном виде и своевременный доступ к хранимым данным.

Требования к разрабатываемой ИС:

1) Данные должны храниться на неком выделенном сервере, обеспечивающем анонимизацию пользователей (152 ФЗ).

2) Клиент должен существовать стационарно

3) Должен быть реализован мобильный клиент

4) Необходимо подобрать технологию разработки, обеспечивающую реализацию системы и для мобильного и для стационарного клиента.

5) Требуется разработать некий типовой интерфейс, чтобы и настольное и мобильное приложение были оформлены однотипно.

Заключение

Предлагаемое решение, представляющее собой разработку приложения для распознавания показаний с legacy-устройств, решает проблему их интеграции в цифровое пространство и является экономически более выгодным, чем замена парка legacy-устройств на современные.

СПИСОК ЛИТЕРАТУРЫ

1. Дзеник А.Д. Проблема технически устаревшего оборудования и способы его решения // Современная техника и технологии. 2017. № 1 [Электронный ресурс]. URL: https://technology.snauka.ru/2017/01/11696 (дата обращения: 12.07.2021).
2. Почти половина российской промышленности работает на устаревшем оборудовании [Электронный ресурс]. URL: https://issek.hse.ru/news/216195559.html (дата обращения: 09.07.2021)
3. Трофимов О.В., Ефимычев Ю.И., Ефимычев А.Ю., Шипилов А.Г. Модернизация предприятий промышленности: концепция, стратегии и механизм реализации // Креативная экономика. – 2011. Т. 5, №11.

УДК 00.004.021

А. С. ШУРЫГИН
Andrew02ufa@rambler.ru
Науч. руководов. – д-р техн. наук, проф. Е. А. МАКАРОВА

Уфимский государственный авиационный технический университет

РАЗРАБОТКА АЛГОРИТМОВ ДЛЯ ИМИТАЦИОННОГО МОДЕЛИРОВАНИЯ ПРОЦЕССА ФОРМИРОВАНИЯ НАЛОГОВЫХ ОТЧИСЛЕНИЙ ПРЕДПРИЯТИЯМИ ПРОМЫШЛЕННОГО КОМПЛЕКСА

Аннотация. В данной работе описываются основы алгоритма формирования налогов для предприятий промышленного комплекса, а также взаимодействия предприятий с Федеральной налоговой службой.
***Ключевые слова*:** формирование налоговых отчислений; предприятия промышленного комплекса.

Разрабатываемый алгоритм для имитационного моделирования процесса формирования налоговых отчислений предприятиями промышленного комплекса создается в среде AnyLogic. На данном этапе моделируется лишь 3 вида налоговых отчислений, которые оплачиваются с разной периодичностью.

На рисунке 1 показан алгоритм формирования налоговых отчислений для предприятий промышленного комплекса с учетом периодичности их уплаты. Алгоритм начинается с запуска имитации в среде AnyLogic. Сразу после этого переменной t присваивается значение 0 для того, чтобы в последствии производить подсчет прошедших календарных месяцев. Таким образом, после того, как проходит один календарный месяц, значение переменной t увеличивается на единицу, то есть становится равным t+1. После этого предприятием осуществляется расчет и отчисление налогов в Федеральную налоговую службу (ФНС). Затем выполняется проверка истинности, получена ли информация о результатах проверки корректности оплаты налогов. Это делается по причине того, что уплаченная сумма налогов не всегда корректна.

В том случае, если информация о корректности оплаты получена, а также оплата налогов была осуществлена корректно, то программа выполняет проверку,

продолжает ли работу имитация. Если имитация попрежнуму работает, то значение переменной t увеличивается и начинается отсчет нового месяца. В случае, если оплата налогов оказалась некорректной, предприятие получает от ФНС информацию о своей задолженности, а также о начисленном штрафе в виде пени.

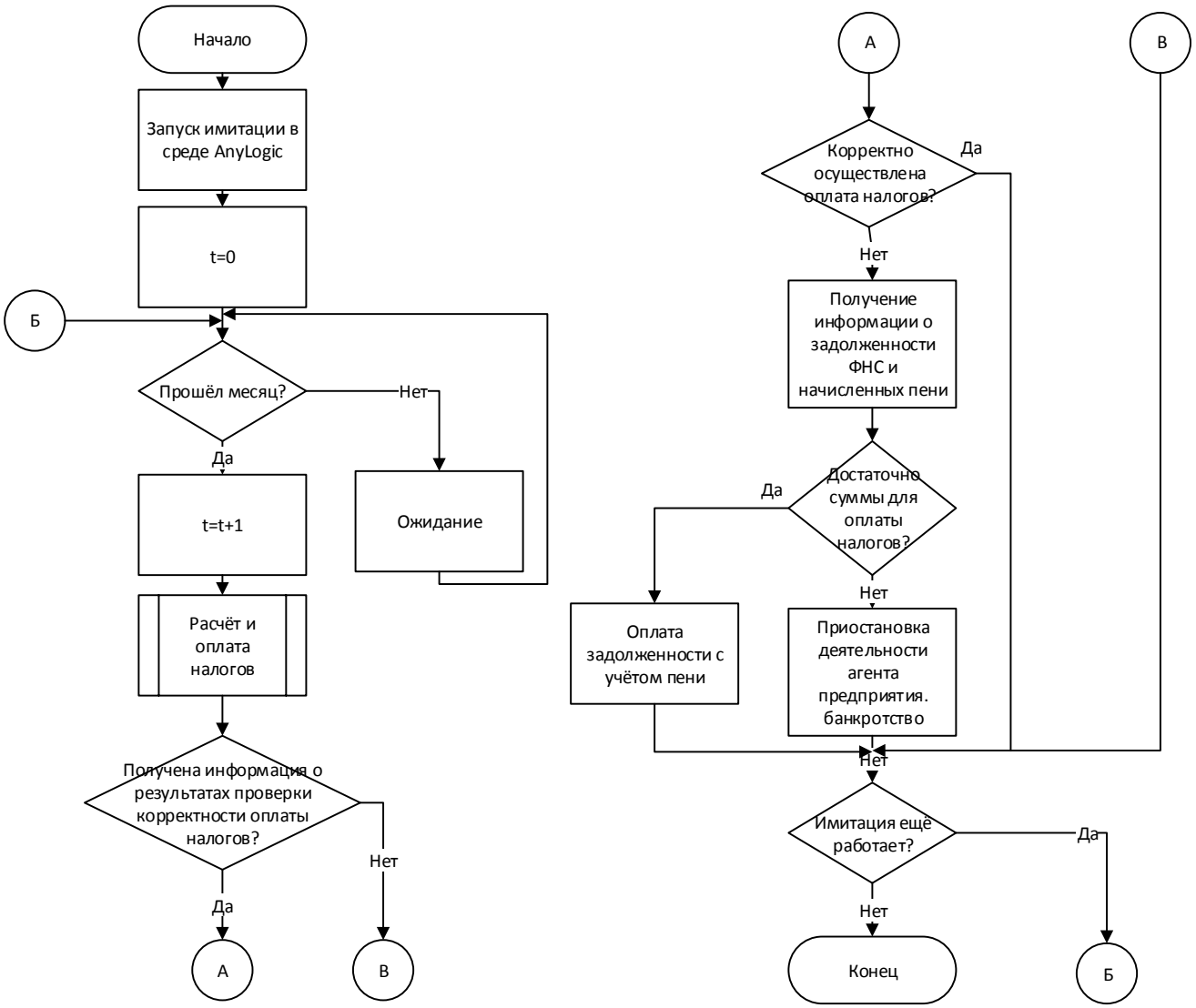


Рис. 1. Схема алгоритма формирования налогов для предприятий промышленного комплекса с учетом их периодичности

Если у предприятия недостаточно средств для погашения своего долга, то его деятельность приостанавливается и предприятие считается банкротом. Если же средств для погашения долга достаточно, то предприятие осуществляет оплату задолженности, после чего выполняется проверка, работает ли имитация. Если имитация работает, то происходит отсчет нового месяца и цикл функционирования предприятия начинается заново.

На рисунке 2 показана декомпозиция подпроцесса «Расчет и оплата налогов». На этой схеме становится видно, что разные налоги уплачиваются с разной периодичностью. Здесь также используется переменная t с целью проверки, прошло ли нужное количество месяцев. Раз в год предприятия платят налог на прибыль. Оплата НДС и налога на заработную плату происходит ежемесячно.

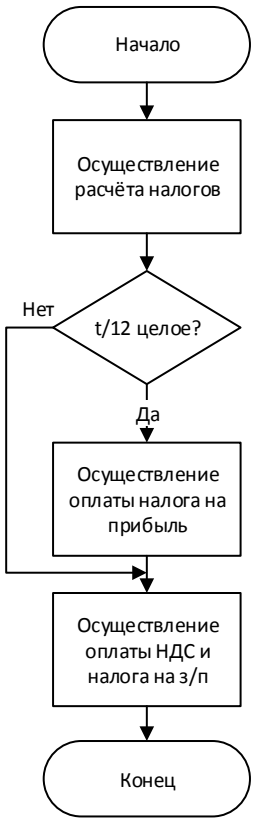


Рис. 2. Декомпозиция подпроцесса «Расчет и оплата налогов» алгоритма формирования налогов для кластера предприятий

В алгоритме на рисунке 3 отражена суть деятельности ФНС в процессе налогообложения предприятий промышленного комплекса. В этом алгоритме также происходит учет прошедшего времени при помощи переменной t, изме-

ряемого в выбранной единице моделирования, равной одному месяцу. После того, как с момента начала имитации в среде AnyLogic прошел один моделируемый месяц, ФНС получает первые налоговые выплаты от предприятий по всем моделируемым видам налогов. Затем со стороны ФНС выполняется проверка корректности осуществления оплаты налогов. В случае, если оплата была произведена некорректно, происходит расчет и начисление пени на сумму задолженности, после чего ФНС информирует предприятие о его долгах и начинает выполнять проверку ликвидации задолженности.

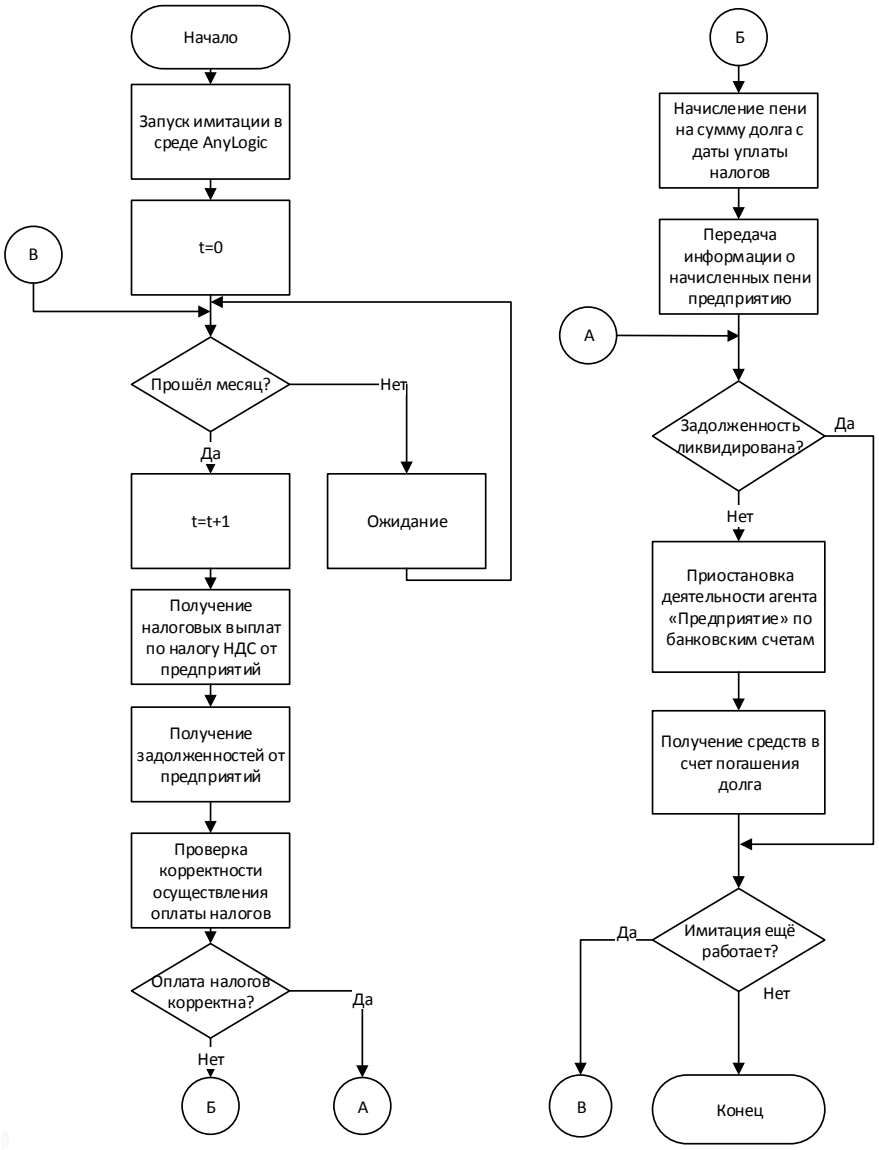


Рис. 3. Схема алгоритма взаимодействия Федеральной налоговой службы с предприятиями реального сектора

В том случае, если оплата налогов все же была выполнена корректно, осуществляется проверка ликвидации задолженности. Это необходимо по той причине, что у предприятия могли оставаться долги с прошлого календарного месяца. В случае, если задолженность предприятием не ликвидируется, ФНС приостанавливает деятельность предприятия по банковским счетам и получает и с них средства в счет погашения долга. После чего выполняется проверка, работает ли имитации и начинается новый месяц с повторном циклом всех действий.

Таким образом, были разработаны схемы алгоритмов функционирования и взаимодействия предприятий промышленного комплекса с ФНС, которые демонстрируют процесс налогообложения в усеченном варианте, с учетом особенностей формирования налогов для предприятий и позволяет увидеть суть деятельности ФНС.

СПИСОК ЛИТЕРАТУРЫ

1. Аристов С.А. Имитационное моделирование экономических систем: Учеб. Пособие / С.А. Аристов. – Екатеринбург: Изд-во Урал.гос.экон.ун-та. 2004. – 121 с.
2. Бусленко, Н.П. Моделирование сложных систем / Н.П. Бусленко. – М.: Изд-во «Наука», 1968. – 357 с.
3. Лычкина, Н.Н. Современные тенденции в имитационном моделировании/Н.Н. Лычкина. – Вестник университета, серия “Информационные системы управления”. – М.: ГУУ, 2000. –№ 2.
4. Окольнишников В.В. Разработка средств распределенного имитационного моделирования для многопроцессорных вычислительных систем // Москва: РГБ, 2007 (Фонд Российской Государственной Библиотеки).
5. Палюх, Б.В. Программные средства имитационного моделирования размерной структуры технологических процессов / Б.В. Палюх, Г.Б. Бурдо, Г.И. Рогозин // Программные продукты и системы. – 2010.-№1(89).– С.82 - 85.

УДК 004

М. М. ЮСУПОВ
yusu-marat@yandex.ru
Науч. руководв. – проф. Е. А. МАКАРОВА

Уфимский государственный авиационный технический университет

ПРОГНОЗИРОВАНИЕ ОТКАЗОВ ОБОРУДОВАНИЯ НЕФТЯНОЙ СКВАЖИНЫ НА ОСНОВЕ АЛГОРИТМА СЛУЧАЙНОГО ЛЕСА

Аннотация. В данной статье рассматривается процесс прогнозирования отказов глубинно-насосного оборудования в нефтяной отрасли. Представлен результат прогнозирования отказов глубинно-насосного оборудования нефтяной скважины и описаны результаты проведения экспериментальных исследований с использованием разработанных моделей на реальных данных.
Ключевые слова: *случайный лес; прогнозирование; нефтяная скважина.*

Прогнозирование наработки на отказ позволяет определить будущие затраты на подземный ремонт скважин и ремонт глубинно-насосного оборудования, потери добычи нефти от непланового простоя скважин и потребность предприятия в новом оборудовании, то есть эффективно и целенаправленно распределить имеющиеся ресурсы предприятия с целью выполнения производственной программы, предоставляет возможность построения плана капитальных ремонтов скважин. Особенно актуальна проблема прогнозирования наработки на отказ для установок электроцентробежных насосов, что связано с высокой стоимостью оборудования.

Таким образом, прогнозирование наработки на отказ установок погружного электроцентробежного насоса, являются актуальной задачей, так как позволяет наиболее точно планировать расходы предприятия на приобретение нового оборудования, ремонт эксплуатируемого оборудования и подземный ремонт скважин.Для решения задачи прогнозирования отказов оборудования нефтяной скважины предлагается применить алгоритм случайного леса. Предложена прогнозирования отказов оборудования нефтяной скважины, которая включает следующие этапы.

На первом этапе выполняется выделение признаков, необходимых для проведения анализа. Объекты (нефтяные скважины) описаны с помощью некоторого

набора характеристик, которые называются признаками. Вектор X всех признаков объекта (скважины) называется признаковым описанием этого объекта. Целевой переменной при прогнозировании отказов оборудования нефтяной скважины является количество отказов.

На втором этапе выполняется предобработка данных.

Первым шагом этого этапа является обработка пропущенных значений. Пропущенные значения заменяются на медиану значений для каждого признака соответственно по всей выборке, так как медиана более статистически устойчива к выбросам.

Вторым шагом предобработки данных является кодирование категориальных признаков. Кодирование категориальных признаков осуществляется по следующему правилу: во-первых, если количество возможных значений признаков небольшое (меньше 10), можно кодировать способом Dummy; во-вторых, когда возможных значений признака много (>10), категориальный признак заменяется средним количеством вхождений признака во всей выборке; и, в-третьих, если есть справочник, то можно заменить на число, характеризующее главное свойство признака [1].

Третьим шагом предобработки данных является избавление от выбросов.

Выбросы — это экстремальные значения, которые существенно отличаются от других наблюдений данных, они могут указывать на изменчивость измерения, экспериментальные ошибки или новизну. В цикле по всем скважинам происходит фильтрация выбросов с помощью метода интерквартильного размаха.

На третьем этапе применяется алгоритм случайного леса для прогнозирования отказов глубинно-насосного оборудования в нефтяной скважине. В работе применяется реализация алгоритма случайного леса из библиотеки sklearn. Класс случайного леса называется RandomForestRegressor [3].

Для реализации метода случайного леса необходимы следующие параметры. Во-первых, длина признакового подописания max_features принята равной: max_features=10. Во-вторых, введено ограничение на число объектов min_samples_leaf в листьях: min_samples_leaf = 5. В-третьих, критерий расщепления “mse”.

График зависимости изменения среднеквадратической ошибки (mse) от количества решающих деревьев показан на рисунке 1.

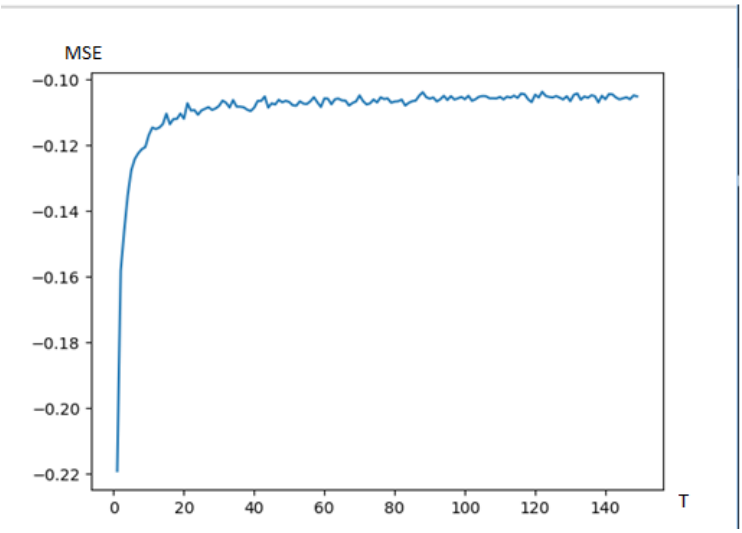


Рис. 1. График зависимости изменения среднеквадратической ошибки (mse) от скорости обучения (learning_rate)

Таким образом, метод случайного леса показывает качество прогнозирования (mse) равное 0.104 при количестве решающих деревьев 122.

Произведен расчет прогнозного значения количества отказов глубинно-насосного оборудования нефтяной скважины для дочернего предприятия компании ПАО «НК «Роснефть» АО «РН-Няганьнефтегаз». Прогнозируемое значение количества отказов глубинно-насосного оборудования нефтяной скважины рассчитано для 2022 скважин (рис. 2).

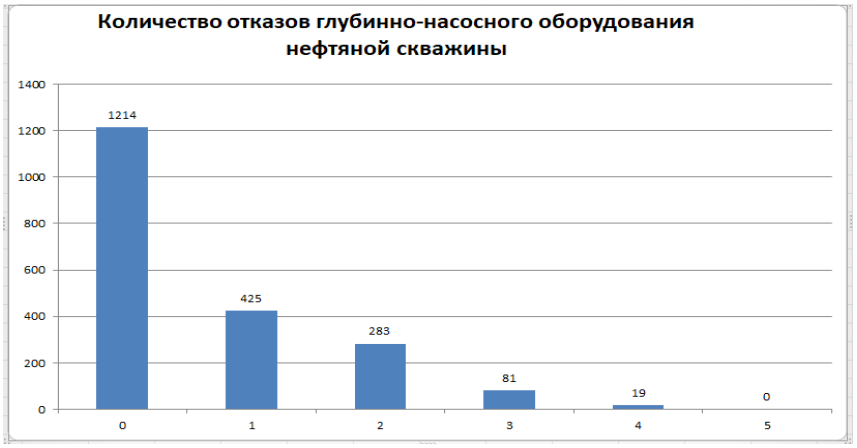


Рис. 2. Результаты прогнозирования количество отказов глубинно-насосного оборудования нефтяной скважины

Далее (рис. 3) представлены признаки, влияющие на отказ ГНО, с их степенями влияния на целевую переменную, (количество отказов).

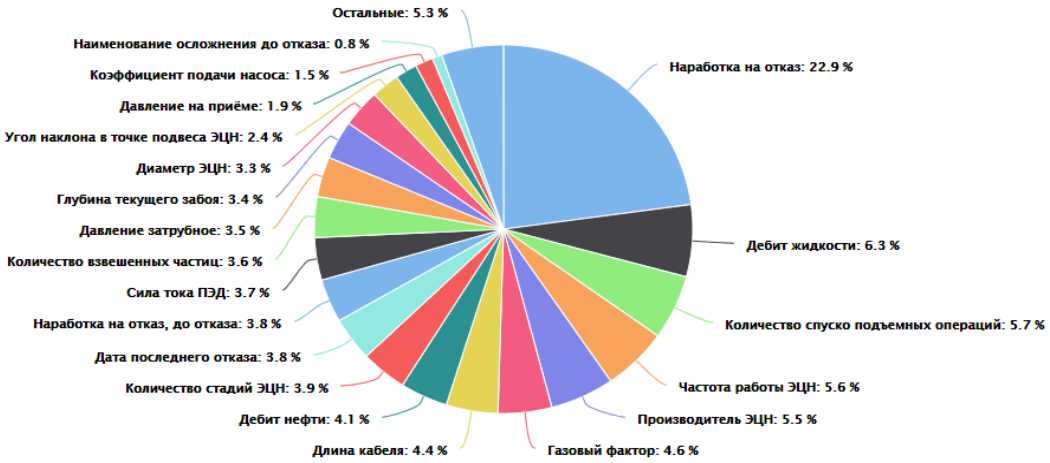


Рис. 3. Признаки, влияющие на отказ ГНО

Таким образом, прогнозирование наработки на отказ установок погружного электроцентробежного насоса, являются актуальной задачей, так как позволяет наиболее точно планировать расходы предприятия на приобретение нового оборудования. Произведен расчет прогнозного значения количества отказов глубинно-насосного оборудования нефтяной скважины. Наиболее важными признаками для целевой переменной являются: наработка на отказ (22.9%), дебит жидкости (6.3%), количество спуско-подъемных операций (5.7%), частота работы ЭЦН (5.6%), производитель ЭЦН (5.5%).

СПИСОК ЛИТЕРАТУРЫ

1. Официальный сайт документации пакета Pandas для Data Science. URL: https://pandas.pydata.org/pandas-docs/stable/reference/api/ (дата обращения: 15.12.2020).;
2. Официальный сайт документации по языку программирования python. URL: https://docs.python.org/3/tutorial/index.html (дата обращения: 15.12.2020).;
3. Официальный сайт документации пакета Scikit-learn для Data Science. URL: https://scikitlearn.org/stable/modules/generated/sklearn.ensemble.GradientBoostingRegressor.html (дата обращения: 15.12.2020).;
4. Шумейко А.А., Сотник С.Л., Интеллектуальный анализ данных (Введение в Data Mining): Учебное пособие, Днепропетровск, Издатель Белая Е.А. – 2012. – С. 19.;
5. Комаров В.С., Прогнозирование наработки на отказ УЭЦН // Журнал «Вестник кибернетики», 2011. – С. 133.;

УДК 681.5

И. А. ЯКОВЛЕВ, А. В. ЕЛИЗАРОВА
ilya-yakovlev-1999@bk.ru, elizarovaanastasia@gmail.com
Науч. руководв. – канд. техн. наук, доц. Г. А. САИТОВА

Уфимский государственный авиационный технический университет

ОЦЕНКА СОСТОЯНИЯ ЗАРЯДА АККУМУЛЯТОРА НА БАЗЕ НЕЛИНЕЙНОЙ АВТОРЕГРЕССИОННОЙ НЕЙРОННОЙ СЕТИ

Аннотация. В процессе эксплуатации автономной системы, работающей от электроэнергии, необходимо отслеживать состояние батареи в реальном времени, чтобы учитывать оставшееся время работы системы в заданном режиме. В статье рассматриваются задачи разработки алгоритма прогнозирования состояния заряда аккумулятора, описание условий использования и функциональное представление, разработанного алгоритма, который в последующем будет применен в работе реальной автономной системы.
Ключевые слова: методы прогнозирования; автономная система; интеллектуальные системы; нейронная сеть; аккумуляторная батарея.

Введение

Состояние заряда аккумулятора зависит от многих параметров. Их кривые разряда и заряда представляют нелинейный процесс, зависящий как от собственных химических процессов аккумулятора, так и от параметров его эксплуатации. Собственными эффектами аккумулятора, вносящих нелинейность, являются эффекты саморазряда, деградации, гистерезиса и др. Параметрами эксплуатации, от которых зависит кривая разряда, являются ток разряда, температура аккумулятора, количество циклов разряда, условия заряда и др.

Анализ существующих интеллектуальных методов прогнозирования состояния заряда аккумуляторов

Преимущество интеллектуальных методов в том, что они имеют свойство автоматической настройки на протяжении всей эволюции системы. Для прогнозирования состояния заряда аккумулятора применяются следующие методы [1]:

– нейронная сеть на основе алгоритма обратного распространения;

– нейронная сеть, основанная на радиально-базисных функциях;

– нейронная сеть, основанная на алгоритме опорных векторов;

– нейронные сети, основанные на нечеткой логике;

– фильтр Калмана. Как правило для прогнозирования применяется расширенный фильтр Калмана или фильтр Калмана «без запаха».

Проектирование нелинейной авторегрессионной нейронной сети с внешним входом

Перед началом формирования обучающей выборки необходимо обеспечить ее репрезентативность и непротиворечивость данных. Для корректного определения текущего состояния заряда аккумулятора необходимо, чтобы на вход подавались как минимум следующие данные: ток заряда/разряда аккумулятора (I, А), напряжение на клеммах аккумулятора в каждый момент времени (U, В), время заряда/разряда (τ, с), температура аккумулятора (T, ºС), количество циклов заряда/разряда (n, шт.) [2].

При проектировании искусственной нейронной сети необходимо учитывать особенности архитектуры и математической модели, а также имеющихся для обучения данных. Аккумуляторная батарея – динамическая система, и для обучения имеются данные, полученные в ходе испытаний.

Исходя из того, что необходимо построить зависимость между входными параметрами для получения более точного результата прогнозирования степени заряженности аккумулятора, была выбрана архитектура и математическая модель рекуррентной нелинейной авторегрессионной нейронной сети с внешним входом.

Количество нейронов в скрытом слое определяется экспериментальным путем. Нет четких правил, по которым можно было бы однозначно определить оптимальное количество нейронов. Таким образом выбор количества нейронов представляет собой задачу оптимизации, для решения которой можно применить уже известные методы этой области.

Архитектура построенной нейронной сети включает 10 нейронов, 4 единицы входной задержки, 4 единицы задержки по обратной связи, тип нелинейной авторегрессионной сети – с разомкнутой обратной связью. В качестве функции активации для скрытого слоя используется гиперболический тангенс,

область значений которой находится в интервале (1, -1). Окончательная архитектура сети представлена на Рис. 1.

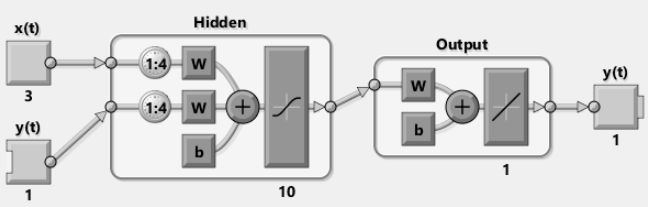


Рис. 1. Архитектура нелинейной авторегрессионной нейронной сети с внешним входом

Нейронная сеть обучалась с применением алгоритма байесовской регуляризации. Для обучающей выборки использовались данные разряда с трех аккумуляторных ячеек. Выборка была поделена в следующем соотношении: 70% данных использовалось для обучения, 15% данных на валидацию и 15% данных для тестирования. На вход подавались значения времени (τ, с), тока нагрузки (I, А) и температура аккумулятора (T, ºС). В качестве целевых данных использовано напряжение на клеммах аккумулятора (U, В).

Результаты обучения соответствуют среднеквадратической ошибке порядка 10e-4 и коэффициенту регрессии равному 0.99999.

Эффективность такой системы можно наблюдать на прогнозировании напряжения трех кривых разряда аккумуляторной ячейки, данные с которой не участвовали в обучении нейронной сети (Рис. 2).

Соответствие целевых значений выходным показывает наиболее плотное распределение данных именно в номинальной зоне процесса разряда аккумулятора (Рис. 3).

Гистограмма распределения ошибок по значениям показывает, что основная часть спрогнозированных значений имеет наименьшую ошибку близкую к нулю (Рис. 4).

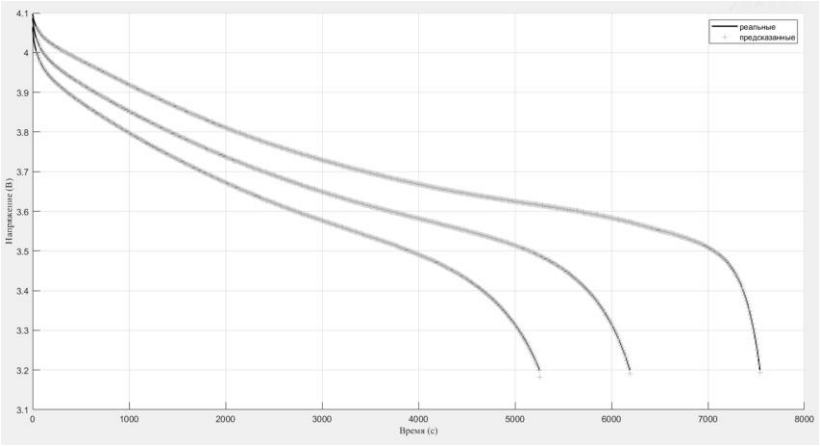


Рис. 2. Результат прогнозирования состояния заряда аккумулятора на трех процессах разряда

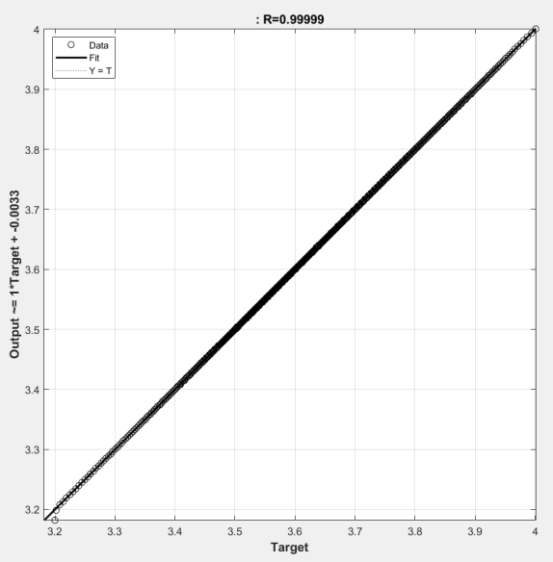


Рис. 3. Линейная регрессия целевых значений по отношению к выходным

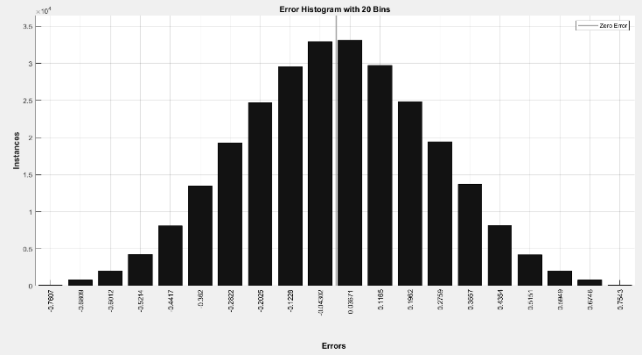


Рис. 4. Гистограмма распределения ошибок по 20 выборкам

Автокорреляция ошибок на временных рядах показывает высокую степень уверенности в прогнозируемых данных (Рис. 5).

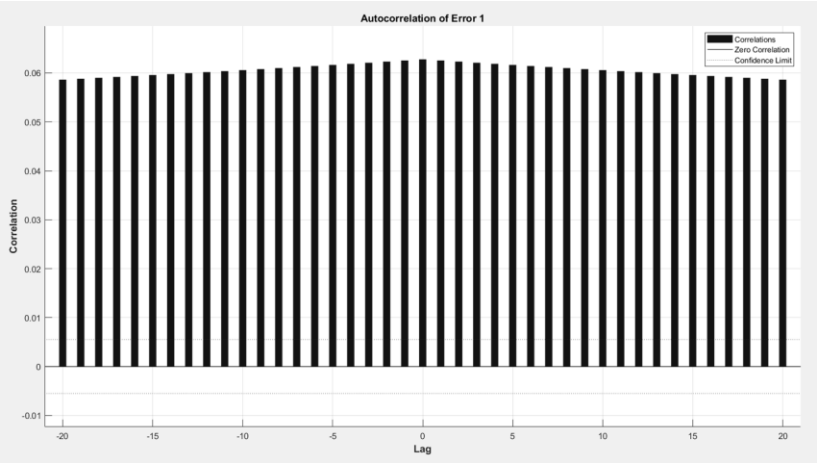


Рис. 5. Автокорреляция ошибок на временных рядах

Таким образом можно сказать, что разработанная система способна достаточно точно спрогнозировать состояние заряда аккумулятора по входным данным. Наиболее точным образом нейронная сеть прогнозирует номинальную зону кривой разряда.

Проведены тесты на реальных характеристиках разряда аккумулятора. По результатам можно наблюдать, что при данных параметрах нейронной сети, качество прогнозирования состояния заряда аккумулятора является достоверным. Наиболее точным образом нейронная сеть прогнозирует номинальную зону разряда аккумулятора, и чуть хуже экспоненциальные. Такой недостаток можно исправить путем ввода дополнительных параметров состояния аккумулятора, оказывающие наибольшее воздействие конкретно на экспоненциальные зоны.

СПИСОК ЛИТЕРАТУРЫ

CHANG W. Y. The state of charge estimating methods for battery: A review //International Scholarly Research Notices. – 2013. – Т. 2013. – 8 с.

TANG X. et al. Li-ion battery parameter estimation for state of charge //American Control Conference (ACC), 2011. – IEEE, 2011. – С. 941-946.

СЕКЦИЯ 5.8
УПРАВЛЕНИЕ ИННОВАЦИЯМИ В СИСТЕМЕ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ

УДК 338.48

А. Р. АБДУЛХАКОВА, Д. Р. ТИМЕРГАЛИНА
darina.timergalina@mail.ru
Науч. руководит. – канд. экон. наук, доц. Ю. Т. МАНСУРОВА

Уфимский государственный авиационный технический университет

ПРОБЛЕМА И ПЕРСПЕКТИВА РАЗВИТИЯ ИННОВАЦИОННОЙ ДЕЯТЕЛЬНОСТИ В РОССИЙСКОМ ТУРИЗМЕ

Аннотация. В статье проведен анализ основных направлений развития туризма в России, определены проблемные аспекты туристической деятельности, которые требуют поиска инновационных решений.
Ключевые слова: туризм; инновации в российском туризме; проблемы туризма.

Туризм в последние годы набирает все большую привлекательность, люди готовы вкладывать свои финансы в эмоции и невероятные впечатления, которые останутся с ними на протяжении всей жизни.

Как одна из развивающихся с высокой скоростью индустрий, туризм приобретает характерные ему черты, которые являются как положительными, так и отрицательными. Любая деятельность, приносящая прибыль всегда нуждается в постоянном и качественном развитии.В случае с туризмом, люди уже давно поняли его привлекательность и прибыльность, поэтому на фоне его популярности, разрабатываются различные инновации и улучшения, которые привлекают все больше новых лиц.

Актуальность данной темы состоит в высоком спросе на туристические поездки, которые совершаются либо через туроператоров, либо людьми самостоятельно. Цель работы заключается в анализе влияния инновации на общий рынок туристических услуг.

В туризме инновационная деятельность развивается по трем направлениям:

− внедрение нововведений (организационные инновации);

− маркетинговые инновации, позволяющие охватывать потребности целевых потребителей или привлекать новую аудиторию;

− периодические нововведения (продуктовые инновации).

Инновационный туристический бизнес может оказать многостороннее воздействие на региональную экономику. Прежде всего, он открывает возможности для развития инфраструктуры, дорожной сети и современных средств связи, стимулирует производство экологически чистых продуктов питания, увеличивает доходы местного населения.

Для более детального рассмотрения проблемы внедрения инноваций в туризме,обратимся к российскому рынку туризма, в котором существует следующий ряд проблем: дороговизна, небольшой выбор объектов туристской инфраструктуры, необходимость более активного проведения государственной политики в сфере туризма, отсутствие широкой имиджевой рекламной кампании туристических возможностей страны.

В связи со сложившимися обстоятельствамив России появился новый национальный проект в начале 2021 года, как сообщила глава Росстуризма. Данная идея рассматривает три основных направления работы: развитие туристической инфраструктуры; повышение доступности; повышение информированности граждан о возможности внутреннего туризма.

Для каждого направления разрабатывается федеральный закон и назначается ответственное лицо внутри регионов за реализацию идеи, а также предусмотрено субсидирование регионов на создание советующей инфраструктуры туризма.

В соответствии с Федеральным законом от 8 декабря 2019 г. № 385-ФЗ «О федеральном бюджете на 2021 год и на плановый период 2022 и 2023 годов» Ростуризму предусмотрены бюджетные ассигнования федерального бюджета на реализацию следующих мер государственной поддержки развития туристской отрасли Российской Федерации.

Снижение спроса российского населения на туристические услуги в 2014–2016 годах привело к уменьшению количества реализованных турпакетов: наименьшее годовое число проданных туров было отмечено в 2016 году (3,4 млн), 57,3% из которых пришлось на поездки граждан России в зарубежные страны. Начиная с 2017 года наблюдалось восстановление спроса на туристические «пакетные» туры, в особенности по территории России. В 2019 году по сравнению с 2016 годом количество реализованных туристических пакетов по России возросло на 2,0 млн (до 5,3 млн, +59,4%).

Далее обратимся более детальному рассмотрению инновационной деятельности в России по секциям, представленные в таблице 1.

Таблица 1

Инновационная деятельность в туризме России

Секция	Инновация
Инновация процесса	Система Белые Ночи позволяет бронировать отели России по специальным ценам в режиме реального времени
Инновация в управлении	В систему выставляется количество свободных номеров в каждой категории на даты
Инновация бизнес-модели	Формирование отелей по единым федеральным стандартам и брендам
Маркетинговая инновация	Программа «Аэрофлот-бонус»
Инновация в логистике	«Хабы» (hubsystems) аэропортов - принципиально новая концепция перемещения через единый связующий авиатранс- портный узел
Ресурсные инновации	Различные виды агротуризма, деревенского туризма.

Российская Федерация обладает большим туристским ресурсным потенциалом, грамотное и рациональное использование которого на основе применения инновационных технологий способно значительно повысить привлекательность страны среди иностранных граждан за счет формирования новых, интересных, разнообразных туристских видов отдыха.

СПИСОК ЛИТЕРАТУРЫ

1. Информационные системы оперативного управления туристской фирмой: Учебное пособие. - М: РИБ «Турист», 2006.
2. Новиков В.С. Инновации в туризме: учеб. Пособие для студ. высш. учеб. заведений/ В.С. Новиков. - М.: Издательский центр «Академия», 2007. - 208 с.
3. turfirma-online.inf.ua - сайт компании, представляющей инновационную программу «Турфирма-Онлайн Professional».

УДК 33.338

А. Н. АДУШЕВ
nictofeel@yandex.ru
Науч. руководитель – канд. экон. наук, доц. Ю. Т. МАНСУРОВА

Уфимский государственный авиационный технический университет

ИННОВАЦИИ В ЭКОНОМИКЕ В ПЕРИОД КОРОНОВИРУСА

Аннотация. В данной статье рассматриваются инновации которые помогли мировой экономике справиться с проблемами, которые принесла пандемия короновируса. Первой инновацией стало полномасштабное использование УРР (удаленный режим работы). Второй инновацией послужила значительная цифровизация процесса коммуникации между сотрудниками. Третьей инновацией послужило всеобщее объединение компаний с облачными сервисами для сбыта своей продукции.
Ключевые слова: инновации; пандемия; короновирус; УРР; цифровизация; облачные сервисы.

2020 год был трудным для всех. Каждый месяц происходило событие повергавшее мир в шок. Главным ударом для человечества в этом году стала пандемия короновируса. Многие привычные нам вещи, такие как проезд в общественном транспорте, походы в кафе и рестораны стали опасны.

Так что же такое пандемия? Согласно критериям ВОЗ, пандемия – распространение нового заболевания в мировых масштабах. К примеру, пандемия гриппа происходит, когда появляется новый вирус гриппа и распространяется по всему миру и большинство людей не обладают иммунитетом.

В 2020 году пандемия парализовала и нанесла серьезный урон всем экономикам мира. Многие компании понесли тяжелые убытки, и были вынуждены адаптироваться, а кто не смог или не успел принять новую структуру рынка, покинули его.

В этом докладе мы рассмотрим роль инноваций в решении проблем, которые повлияли на экономические процессы в период пандемии.

Первой проблемой стала организация процесса производства продукта. Из-за объявленных ограничений сотрудники компаний не могли эффективно работать по причине отсутствие возможности близкой коммуникации друг с

другом и своими руководителями. Вследствие этого было принято решение перехода на УРР или «удаленный режим работы».

УРР - это способ организации труда, при котором работник выполняет важнейшие функции, связанные со своей работой, с помощью информационно-коммуникационных технологий (ИКТ), при этом находясь дома. В условиях пандемии COVID-19 термин "удаленный режим работы" означает исключительно удаленную работу на дому как альтернативный способ организации труда.

УРР дает множество преимуществ, среди которых сокращение затрат времени на транспорт, большая степень автономии и свободы при организации труда, увеличение возможностей для сочетания трудовой и личной жизни, рост мотивации и сокращение текучести кадров, а также повышение производительности и рациональности труда.

Это благотворно повлияло на процесс производства товаров. Процесс производства получил новое дыхание за счет того, что сотрудники работали в домашней обстановке что, делало их более свободными что в свою очередь увеличивало их производительность в то время как работодатель сильно сокращал свои издержки на организацию рабочего процесс т.е. не нужно было арендовывать офис и платить за него.

По данным РБК 20 марта 2020 года 3% россиян заявили о полном переходе компаний на удаленную работу из-за эпидемии коронавируса, то 15 апреля того же года таких ответов было уже 14%. Еще 15% респондентов ответили, что в их компаниях на удаленную работу переведены только некоторые отделы. 5% опрошенных заявили, что руководство рекомендовало им перейти на работу из дома, но окончательное решение остается за сотрудниками. Как мы видим виднеется четкая тенденция того как российские компании постепенно меняли свое отношение к УРР.

В данный момент УРР пользуется популярностью и многим сотрудникам компаний он в целом пришелся по душе.

Второй проблемой стало отсутствие интегрированной информационно технологической среды, которая могла помочь в организации процесса производства, в структурах компании.

Для создания возможности организации процесса производства полная интеграция информационно технологических подразделений во все структурные элементы компании стала необходимостью. Ведь теперь многие сотрудники оказались заперты в своих квартирах, и корпоративно-информационная среда стала единственной их возможностью организовать работу со своими коллегами. Это позволяет развивать и перестраивать корпоративную информационно технологическую среду, эффективно применять облачные сервисы, программное обеспечение по автоматизации производственных процессов, тестированию, внедрению и эксплуатации новых цифровых инструментов.

По статистике, приведенной аналитиками из Cnews основными задачами, которые предстали перед информационно технологическими подразделениями стали организация техподдержки удаленных рабочих мест 29%, внедрение VDI 29%, а также обеспечение безопасности удаленного доступа 29%.

Третьей проблемой оказался почти полный паралич цепочек поставок от производителя к потребителю. Из-за введенных ограничений поставки продуктов с предприятий до точек сбыта оказалась под угрозой из-за возможности распространения вируса.

Также участники рынка были вынуждены решать проблему почти полного паралича процесса распределения, и сбыта покупателями своих товаров. Ведь они не могли показывать свои товары напрямую потребителям, так как все магазины-посредники суть которых заключалась в том, что потенциальные покупатели собирались в одном месте и рассматривали возможные варианты товаров оказались недоступны.

Наиболее яркий пример это рынок онлайн-магазинов. Ведь если раньше компаниям не требовались веб-сервисы для удовлетворения нужд покупателей так как для этого они использовали магазины и супермаркеты, то в период пан-

демии, когда посещение последних стало невозможным теперь они стали им необходимы. Ведь по данным Ассоциации компаний розничной торговли к началу апреля трафик покупателей в супермаркетах уменьшился на 40-60%.

В этом случае предприятиям пришлось объединяться с крупными IT-компаниями, которые могли бы дать предприятиям платформы для сбыта своего продукта. Такие объединения обусловлены, в первую очередь, тем, что создание собственных веб-сервисов либо их масштабирование является рискованным мероприятием с точки зрения маркетинга и финансов, а владельцы крупных облачных платформ имеют необходимый канал продвижения. По мнению специалистов отрасли, в посткоронавирусном мире усилится роль партнерских услуг, включая модели «программное обеспечение как услуга» (SaaS) и «платформа как услуга» (PaaS), где компании могут получать готовый для использования функционал через веб-интерфейс или даже через API (Application Programming Interface – программный интерфейс приложения). Таким образом, конкурентная позиция в мире после короновируса будет во многом определяться позицией в экосистемах с взаимным доступом их участников к API друг другу.

По исследованию агентства AdvantShop в апреле 2020 года число новых открытых интернет-магазинов стало почти в 2 раза больше (на 99,02%), чем за период январь-март, и в полтора раза больше, чем в апреле прошлого года. Это связано с тем, что бизнесу приходится адаптироваться к новой жизни и лучшее решение — это выход в онлайн.

Из трех рассмотренных инновационных методов организации экономических процессов мы можем сделать выводы о том, что российская экономика хоть и с трудом, но смогла адаптироваться к изменениям, которые принесла пандемия. Обозначилась положительная динамика перехода россиян к УРР, компании получили новые способы представления и сбыта своего продукта покупателям, а сформировавшаяся информационно технологическая среда обеспечит четкую согласованность и развитие всех структур компаний.

СПИСОК ЛИТЕРАТУРЫ

1.Исследование: как крупный российский бизнес будет развивать технологии удаленной работы//https://www.cnews.ru/articles/2021-01-26_cnews_analytics_itogi_udalenki_2020_i_budushchie
2.Как завершится кризис из-за коронавируса. Главные прогнозы// https://www.rbc.ru/economics/17/11/2020/5fabc9289a79476ec20f16cc
3.Куликов О. А. Пандемия коронавируса как фактор интенсификации развития и внедрения цифровых технологий // Изв. Сарат. ун-та. Нов. сер. Сер. Экономика. Управление. Право. 2020. Т. 20, вып. 4. С. 400–404. DOI: https://doi. org/10.18500/1994-2540-2020-20-4-400-404

УДК 371

А. А. АХМЕТГАРЕЕВА, А. И. АЮПОВА
dance4444@mail.ru, alsu_ayupova_2000@mail.ru
Науч. руководит. – канд. экон. наук, доц. А. В. СТАРЦЕВА

Уфимский государственный авиационный технический университет

ОНЛАЙН-ОБУЧЕНИЕ КАК СОВРЕМЕННАЯ ТЕХНОЛОГИЯ ОРГАНИЗАЦИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА

Аннотация. В представленной статье рассматриваются современные реалии организации образовательных процессов в условиях пандемии Covid-19. Обозревается влияние дистанционного формата обучения на конфиденциальную безопасность данных обучающихся, а также выделяются положительные и отрицательные стороны организации дистанционного получения новых навыков, умений, знаний.
Ключевые слова: пандемия; современные технологии; дистанционное обучение; конфиденциальность.

Пандемия Covid-19, разразившаяся в начале 2020 года, заставила изменить ход привычного ритма жизни во всем мире. В целях сдерживания распространения инфекции,учебные заведения по всему миру перешли в дистанционный формат обучения. Так, например, в Великобритании директоров учебных заведений обязали провести разъяснительные беседыс родителями обучающихся, а также принимать большинство важных организационных решений. В Грузии под контролем министерства образования были созданы виртуальные классы для обучения, контроля и консультаций учителей, администрации школ и учащихся. В Италии, Аргентине, Израиле, Португалии, Бельгии и Австралии подготовили специализированные онлайн-страницы, вебинары, образовательные платформы, обеспечили методическую и техническую поддержку, провели мониторинг образовательного процесса. В России принято решение о том, что каждый регион самостоятельно решает вопросы ограничения работы школ и ВУЗов в зависимости от эпидемиологической ситуации, решения по данным вопросам согласуются с Федеральным Правительством.

В таблице 1 представлен процент распространения дистанционного обучения в общем образовательном процессе по различным странам [3].

Таблица 1

Дистанционное образование в различных странах

Страна	Процент распространения дистанционного обучения в общем образовательном процессе
Англия	56 %
Германия	61 %
Франция	59 %
США	58 %
Канада	65 %
Япония	25 %

Разумеется, качество получаемых обучающимися знаний резко ухудшилось. Однако, предприятия, учебные заведения и целые отрасли экономикив связи с оперативной разработкой инновационных способов выхода из данной ситуации, оказалось,могут работать не менее эффективно, при условии, что сотрудники и обучающиеся будут находиться «по ту сторону» экрана.

Цифровое обучениена данный момент является спасителем для современного образования, поскольку объединяет миллионы учащихся, студентов и преподавателей, содействуя непрерывному, высокоэффективному процессу обучения.

Разработанная система онлайн-обучения по всему миру, как ожидается, останется весьма влиятельной сферой в будущем, так как дистанционные образовательные технологии с использованием Интернета применяются как для освоения отдельных курсов повышения квалификации пользователей, так и для получения разных видов образования, причем, если сначала дистанционное обучение развивалось в рамках высшего образования, то теперь оно все больше распространяется на все уровни образования [1].

При рассмотрении сервиса для дистанционного обучения, онлайн-встреч и конференций удобным и простым в использовании является американская компания коммуникационных технологий «Zoom». За время пандемии компания достигла рыночной капитализации более чем 100 миллиардов долларов (табл.2). Фактически, платформа настолько популярна, что в «Zoom» есть це-

лые руководства, посвященные тому, чтобы помочь людям использовать десятки функций внутри приложения [5].

Таблица 2

Капитализация «ZoomVideoCommunications» за период пандемии

Квартал, финансовый год	Годовые протоколы вебинаров
2 квартал 2020 г.	2000000000
3 квартал 2020 г.	3 миллиарда
4 квартал 2020 г.	3 миллиарда
1 квартал 2021 г.	42 миллиарда
2 квартал 2021 г.	42 миллиарда
3 квартал 2021 г., квартал	45 миллиардов +

В сфере онлайн-образования по объему выручки одним из крупных игроков является «Skillbox», лидер сегмента дополнительного профессионального онлайн-образования (рис.1).На базе данной платформывозможно получить профессии будущего и удачно трудоустроиться.

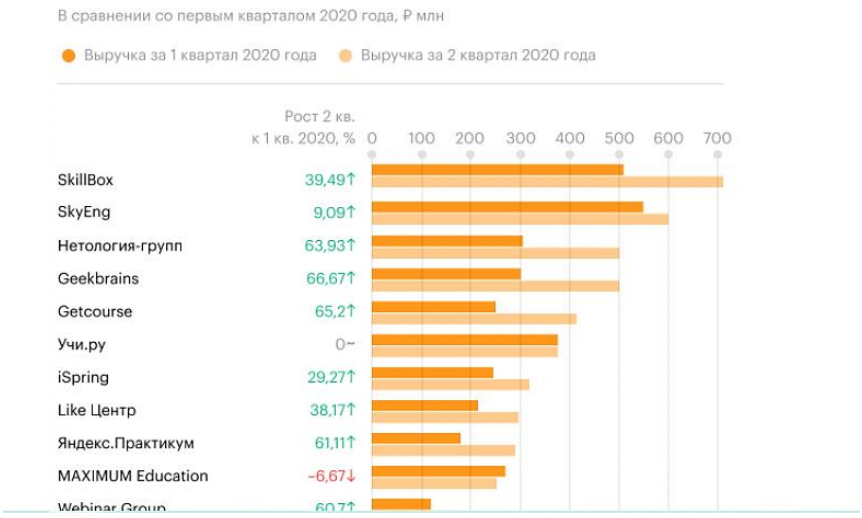


Рис. 1. Рейтинг крупнейших EdTech -платформ за 2 квартал 2020года

Широкое распространение дистанционных видов образования объясняется весомыми преимуществами удаленного обучения, которые заключаются в:

– возможности организации уроков в труднодоступных районах, для инвалидов и часто болеющих детей, возможность обучения в иностранных ВУЗах;

– возможности занятий во время эпидемий или при сложных погодных условиях;

– возможности самостоятельного обучения, приобретения второй специальности, дополнительных знаний;

– снижении затрат на обучение;

– самодисциплине и ответственности обучающегося;

– отсутствии строгой привязки к месту и времени проведения занятий;

– всеобщей доступности обучения (любому возрасту, уровню образования, профессиональной подготовки, в любом месте планеты, где есть коммуникативная связь) [2].

Такие технологии облегчают выполнение различных образовательных задач, например, позволяют учителям выдавать ученикам домашние задания, позволяют точно отслеживать и оценивать успеваемость отдельных учащихся. Кроме того, учителя могут планировать и контролировать выполнение заданий и экзаменов.

Несмотря на преимущества, следует также отметить, что с ростом числа внедряемых технологий дистанционного обучения, произошел серьезный рост числа утечек данных.

Согласно данным МВД, за январь-июнь 2020 года, рост киберпреступности в России составил 91,7% по сравнению с аналогичным периодом прошлого года [4].

Основная цель киберпреступников – кража денег или ценной информации, которую можно продать, продажа фейковых цифровых пропусков, рассылка сообщений о штрафах за нарушение карантина, поддельные сайты служб по доставке грузов, еды и другого, мошеннические рассылки от имени сервиса видеоконференций «Zoom». Множество университетов и вовсе заявили об отказе от платформы «Zoom» и переходе на «Google Meet», а также сторонние приложения. Появилось понятие «Zoombombing», характеризующее действия, связанные с нарушением онлайн-пространств, включая взлом виртуальных классов, размещение порнографических или вызывающих ненависть изображений, выкрикивание ненормативной лексики и прочее.

Таким образом, возникают проблемы с онлайн-приложениями, посредством которых университеты проводят дистанционные лекции или семинары.

Наблюдается явный переход конфиденциальности в разряд стандартных обязательных требований при обсуждении вопросов цифровизации и достижения бизнес-целей. В соответствии с этим, знания и навыки в области обеспечения защиты персональных данных занимают центральное положение в системе внедрения современных технологий.

Исходя из вышеизложенного, нами разработаны и предложены мероприятия по повышению уровня безопасности конфиденциальной информации в современных реалиях.

В первую очередь, учебные организации должны напомнить своим сотрудникам и обучающимся о политике и методах защиты информации и надлежащим образом поддерживать их, чтобы они также стали передовой линией в борьбе с кибератаками.

Организация учебы на дому должна сопровождатьсянеобходимостью в предельной осторожности при переходе по различным ссылкам.

Особо важно выделить такие меры предосторожности, какбезопасная система Wi-Fi, полностью обновленное антивирусное программное обеспечение, осторожность при работе в общем пространстве, установка соответствующих инструментов шифрования и периодическое резервное копирование данных.

Преступники будут продолжать использовать пандемию в корыстных целях, поэтому в то время как внимание большинства людей сосредоточено на сдерживании вируса и прекращении его распространения, сохранении здоровья, важно также не забывать об эффективной защите данных.

Резюмируя вышеописанное, можно судить о том, что в период пандемии стала очевидной необходимость развивать цифровые ресурсы, формируя смешанную модель обучения с использованием дистанционного формата.

СПИСОК ЛИТЕРАТУРЫ

1. Ольшанникова Н.А. Новые формы высшего образования с использованием современных онлайн-технологий / Н. А. Ольшанникова // Профессиональное образование в современном мире. – 2020. – № 2. – С. 3688-3694. – ISSN 2224-1841. –Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/journal/issue/312929 (дата обращения: 08.09.2021)
2. Яковлева Л.С. Роль самодетерминации личности в онлайн-образовании / Л. С. Яковлева, В. И. Кудашов // Профессиональное образование в современном мире. – 2019. – № 4. – С. 3215-3223. – ISSN 2224-1841. –Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/journal/issue/311802 (дата обращения: 08.09.2021)
3. Рейтинг лидеров рынка онлайн-образования России. [Электронный ресурс]. URL: https://trends.rbc.ru/trends/education/5fa1cc249a794739b65c7b5c (дата обращения: 07.09.2021)
4.Статистика и аналитика. [Электронный ресурс]. URL:https://мвд.рф/Deljatelnost/statistics (дата обращения: 07.09.2021)
5.Статистика пользователей Zoom. [Электронный ресурс]. URL: https://www.affde.com/ru/zoom-users.html (дата обращения: 07.09.2021).

УДК 332.05

Э. Р. БАШАРОВ, Н. Р. ГУСМАНОВ, Д. Р. ЛАТЫПОВА
nuralig@mail.ru
Науч. руководв. – канд. экон. наук, доц. А. В. СТАРЦЕВА

Уфимский государственный авиационный технический университет

ИННОВАЦИОННЫЕ СИСТЕМЫ В АГРОПРОМЫШЛЕННОМ КОМПЛЕКСЕ: ОПЫТ ВНЕДРЕНИЯ В РОССИИ И БАШКИРИИ

Аннотация. Инновационная деятельность АПК как в стране, так и в регионе может выражаться в разных системных формах. В данной работе рассматриваютсяколичественные и качественные изменения технической базы производства и механизмов управления организацией в сельском хозяйстве. Данные новшества направлены на производство системно новой, улучшенной продукции, внедрение и использование инновационных видов оборудования, новые формы организации производства, сбыта и новые методы управления. Каждая из данных инноваций поможет улучшить не только техническую и производственную составляющую, но и экономические и финансовые показатели.
Ключевые слова: сельское хозяйство; фермерство; инновации; инновационная деятельность; экосистема; сельхозпродукция; сельхозпроизводители; сельхозтехника; цифровизация АПК; IT-инновации.

На сегодняшний день развитие любой отрасли основывается на применении высокотехнологичной, инновационной продукции, ведь только таким способом возможно поддерживать высокий уровень конкурентоспособности на рынке, а также обладать достаточным потенциалом развития. Данный феномен не только подтверждается экспертами в различных областях, но и проходит проверку временем.

Цель данного исследования состоит в выявлении современных особенностей инновационной деятельности в агропромышленном секторе экономики, определении перспективных систем ведения сельского хозяйства в России и Башкирии.

После вступления России во Всемирную торговую организацию(ВТО) в 2012 году стало ясно, что конкуренция с западными производителями, которые имеют большой опыт работы в условиях рынка и несравнимо большую государственную поддержку, ставит перед национальными сельскохозяйственными организациями ряд задач по организации эффективной деятельности. Следующим неоднозначным этапом для сельскохозяйственных производителей стало

введение санкций. С одной стороны, положительно сказалось возмещение санкционной политики от России в виде закрытия части рынка для заграничных сельскохозяйственных производителей, благодаря чему местные аграрии и производители получили возможность развиваться. С другой стороны сами санкции ограничивают возможность выхода национальных производителей за рубеж, но этот фактор не столь значим из-за особенностей местного сельского хозяйства.

В настоящее время можно говорить о достаточно неплохих тенденциях для сельхозпроизводителей, например, на фоне пандемии в 2020 году многие европейские страны решили увеличить продуктовые резервы, благодаря чему в России рекордно увеличился экспорт сельскохозяйственной продукции. Все эти факторы при грамотном управлении, внедрении инновационных технологий и государственной поддержке дают российскому АПК возможность выйти на очень хорошие показатели. Об этом же говорит и «Доктрина продовольственной безопасности Российской Федерации», утвержденная Президентом РФ в 2020 году, рост показателей по культурам, внедрение инновационных технологий и систем – все это должно уже в ближайшем будущем значительно увеличить состояние АПК.

Так что же такое инновации и процесс их внедрения? «Инновационный процесс»–это определенный цикл, в котором осваиваются научные знания, разработки, технологии в хозяйственной и иной деятельности, предполагаются определенные формы инновационной деятельности, имеется своя специфика. Конкретно в сельском хозяйстве сущность инновации зависит от отрасли деятельности: животноводство, растениеводство, рыбоводство, иные отделы или же межсистемные сферы. Для более подробного рассмотрения далее будут приведены примеры инноваций из различных отраслей сельского хозяйства.

В простонародье считается, что все новое – это хорошо забытое старое. Так, осенью 2021 года, главой РАН было предложено увеличить долю производства промышленных сортов конопли в России. Конопля является субститу-

том таких ресурсов как хлопок, нефть, древесина, кроме того, данное растение полезно для экологии: «На гектар посадок она депонирует лучше, чем хороший лиственный лес», – заявил Сергеев А.М. Особый интерес может быть вызван для Башкирии наряду с улучшением экологической обстановки в республике, культивирование данного растения также поможет вернуть в строй заброшенные пахотные земли, коих насчитывается 500 тысяч гектар. Инновационностьюданного предложения является современная сортовая база, а также новые методы применения полученного сырья как для нужд промышленности в производстве современных материалов, медицины, так и при разработке новых лекарств.

Сегодня профессионалы в области сельского хозяйства стараются максимально использовать технологии точного земледелия. Развитие цифровых технологий и средств связи помогает аграриям снижать издержки, повышая при этом продуктивность полей и конечную рентабельность бизнеса. В этой связи существует спрос на мобильные приложения, которые облегчают работу аграриев, позволяют внедрить новые технологии. Большего прогресса в этом добились иностранные разработчики, которые представляют свои приложения на общемировой уровень. Российские аграрии могут воспользоваться большинством этих приложений на английском либо ином другом языке. Среди большого разнообразия приложений стоит выделить наиболее перспективные и заслуживающие наибольшего внимания. К таким стоит отнести приложение ID Weeds, разработанное Университетом штата Миссури, и позволяющее идентифицировать тип сорняков в поле. Приложение содержит более чем 430 разновидностей сорняков, встречающихся в сельском хозяйстве. А программа YaraCheckIT содержит фото-библиотеку, по которой можно быстро установить случаи, когда растение испытывает дефицит тех или иных веществ и дает советы, как это можно исправить. Наверное, самое перспективное направление связано с крупными базами данных. Например, приложение Wunderground обеспечивает мониторинг погоды с 270 тыс. станций, а TankMixCalculator хранит в

себе всю информацию, касающуюся того, сколько удобрений было внесено в почву.

Башкирские аграрии, в этом году включительно, уже применили данные технологии на своей практике. На данный момент многие компании занимаются разработкой и внедрением сервисов для управления сельскохозяйственным производством, которые в свою очередь позволяют автоматизировать все процессы путем цифрового планирования, использования агрономических модулей, описывающих поля, их историю и особенности, а также блоков учета и контроля работы техники. Более того следует отметить, что такие сервисы с помощью спутниковых снимков полей позволяют вносить данные агронаблюдений, что значительно облегчает жизнь аграриям. Обобщая, можно сказать, что данные разработки представляют собой единую экосистему, соединяющую разных специалистов и разные отделы друг с другом с целью обмена опытом, информацией. Кроме того, сейчас аграрии активно используют продукты искусственного интеллекта, которые оцифровывают культуры в ретроспективе 5 лет, т.е. возможно спрогнозировать урожайность участков полей и без труда планировать и контролировать производственные процессы (рисунок 1).

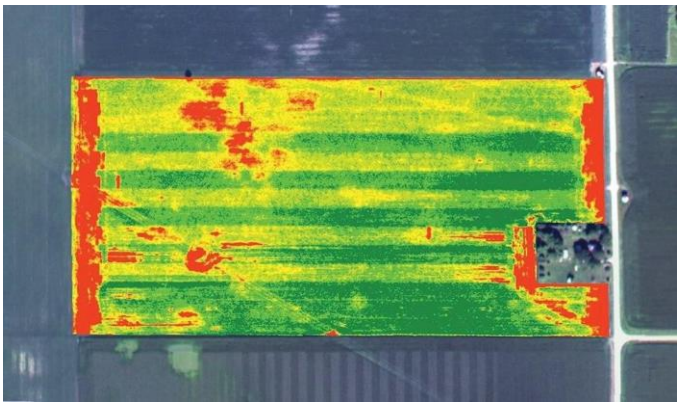


Рис. 1. Нормализованный вегетационный индекс, или карта NDVI
(показатель актуального состояния культурных растений)

Отметились и инновационные системы в животноводстве: компания «R-SEPT» совместно со Сколково разрабатывает на основе европейских технологий инновационную систему добровольного доения.Данная система предназна-

чена для коровников с беспривязным содержанием, где доение и кормление происходит автоматически. Также внедренная в коровник система анализирует состояние животных, позволяет проводить каждодневный мониторинг здоровья и подбирать соответствующий корм. Роботизация заменит труд более чем 5 работников (доярок, ветеринаров и обслуживающего персонала). Данная разработка наиболее актуальна для крупных фермерских хозяйств с большим поголовьем скота и соответственно с большим количеством работников. Потенциально, при поддержке государства, данными системами можно обеспечить малое и среднее фермерство, что позволит животноводству выйти на совершенно новый уровень.

Перед Россией и Республикой Башкортостан остро стоит вопрос о выходе на лидерские позиции по различным отраслям экономики. АПК является одним из самых востребованных в настоящее время, очевидно, что это будет не просто, учитывая климатические и политические факторы национального рынка, но на стороне РФ и РБ, в частности, большое количество инновационных возможностей как технологических, так и экономических.

Для полноценного выхода российского сельского хозяйства на международный уровень необходимо улучшить множество производственных процессов, научиться грамотно применять инновационные технологии, а также необходима постоянная поддержка от государства в виде субсидий и целевых программ. Подводя итоги, стоит сказать о самом важном – положении в инновационной деятельности. Инновации возможно реализовать только лишь в системно развивающейся экономике, с грамотным планированием и поддержкой.

СПИСОК ЛИТЕРАТУРЫ:

1. https://old.sk.ru/news/b/press/archive/2018/08/09/pervaya-rossiyskaya-avtomaticheskaya-ferma.aspx
2. https://www.alb.aero/services/karta-ndvi/
3. https://www.presscentr.rbc.ru/tpost/7isivp0xu1-tsifra-i-iskusstvennii-intellekt-vishli
4. Богачев А.И. Инновационная деятельность в сельском хозяйстве России: современные тенденции и вызовы // Вестник НГИЭИ. 2019. №5 (96). URL: https://cyberleninka.ru/article/n/innovatsionnaya-deyatelnost-v-selskom-hozyai-stve-rossii-sovremennye-tendentsii-i-vyzovy (дата обращения: 21.03.2021).

5. Эминова Э. М., Баширова А. А., Белан А. И. Особенности управления инновационным развитием в АПК региона // РППЭ. 2016. №5 (67). URL: https://cyberleninka.ru/article/n/osobennosti-upravleniya-innovatsionnym-razvitiem-v-apk-regiona (дата обращения: 21.03.2021).
6. ГусмановР. У. Эффективность использования инноваций в сельскохозяйственном предприятии / И. А. Зарипов, Р. У. Гусманов // Достижения науки и техники АПК. – 2007. – № 2. – С. 5.
7. Кадомцева М. Е. Анализ инновационного развития отраслей агропромышленного комплекса России // Вестник ВГТУ. 2014. №26. URL: https://cyberleninka.ru/article/n/analiz-innovatsionnogo-razvitiya-otrasley-agropromyshlennogo-kompleksa-rossii (дата обращения: 22.03.2021).
8. Клименко Ю. И. Задачи системы сельскохозяйственного консультирования по инновационному развитию производства // APRIORI. Серия: Естественные и технические науки. 2014. №1. URL: https://cyberleninka.ru/article/n/zadachi-sistemy-selskohozyaystvennogo-konsultirovaniya-po-innovatsionnomu-razvitiyu-proizvodstva (дата обращения: 23.03.2021).

УДК 336.7

Н. С. ВИНОКУРОВА, Д. А. БИКМЕТОВА
bikmetova.bikmetova-dana@yandex.ru, Natalya9V@yandex.ru
Науч. руководитель – канд. экон. наук, доц. Ю. Т. МАНСУРОВА

Уфимский государственный авиационный технический университет

РОЛЬ ИННОВАЦИЙ В ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ БАНКОВСКОЙ СФЕРЫ

Аннотация. В данной статье подробно рассмотрены инновации, влияющие на безопасность банковского сектора. В работе отражаются основные инновации в банковской сфере, приводится структура инноваций в российских банках, рассматриваются основные риски, возникающие при использовании инноваций, также предложены решения для устранения данных рисков и мероприятия поэффективному процессу внедрения инноваций.
Ключевые слова: банковская деятельность; инновации; экономическая безопасность.

Банковская деятельность – это банковские функции и иная деятельность кредитной организации, которые непосредственно направлены на получение прибыли из банковских операций и сделок. С развитием науки и технологий, банковская система стала незаменимой частью денежного хозяйства.

Одним из ключевых факторов успешного развития деятельности банка является последовательное внедрение инноваций.Под инновацией в банковской сфере понимается конечный результат научно-технической деятельности банка, получивший воплощение в виде обновленного или улучшенного продукта, или услуги, направленный на лучшее удовлетворение существующих потребностей клиентов или создание новых в процессе управления ресурсным потенциалом банка.

В современной российской банковской сфере происходят стремительные процессы цифровизации банковских процедур. Данные нововведения отражают положительное влияние на экономическую безопасность банковской деятельности. Однако последствия введенных инноваций в систему безопасности не однозначны. С одной стороны, снижаются транзакционные издержки, с другой появляются новые угрозы, которые увеличивают риски.

Рассмотрим самые распространенные инновации в банковской среде и какие риски они представляют.

Самой распространенной инновацией в банковской среде является интернет – банкинг. Он дает возможность совершать различные банковские операции через интернет. Благодаря интернет-банкингу появляется возможность в любое время проверить состояние счета, перевести денежные средства как на свои, так и на чужие счета, совершать операции с кредитами и многое другое. Данные операции совершаются очень быстро в онлайн формате, через личный кабинет и приложение от соответствующего банка.Такой способ осуществления банковских операций значительно экономит время клиентов, поэтому в настоящее время использование интернет –банкинга достаточно перспективно.

Еще одной внедренной инновацией служит такая функция как бесконтактная оплата. В новые выпускаемые карточки от банков устанавливают NFC чип, с помощью которого клиенты получают возможность осуществлять оплату и переводы денежных средств касанием банковской карточки. Такой чип может быть установлен так же на телефон, чаты или карту. При использовании карты не будет возникать проблемы с банкоматами, когда они «съедают» карту.

Еще одной инновацией может стать биометрическая идентификация клиентов. В настоящее время развитие технологий предоставляет возможность совершать какие-либо функции, основанные на отпечатке пальца. Не исключено, что в ближайшем будущем банки захотят применить данные технологии в своей деятельности. Например, вместо ввода ПИН - кода нужно будет приложить палец к сенсору и покупка будет оплачена. Тогда и не нужно будет носить с собой подтверждающие личность документы.

Использование таких технологий поможет в ускорении работы с клиентами и совершении банковских операций. Так же, скорее всего, с рынка уйдут пластиковые карты и можно будет расплачиваться телефоном или при совершенной технологии биометрической идентификации можно будет расплатится, приложив палец без всякой карты.

На рисунке можно увидеть структуру инноваций в российских банках по продуктам в %, 2020 год (рис.1).

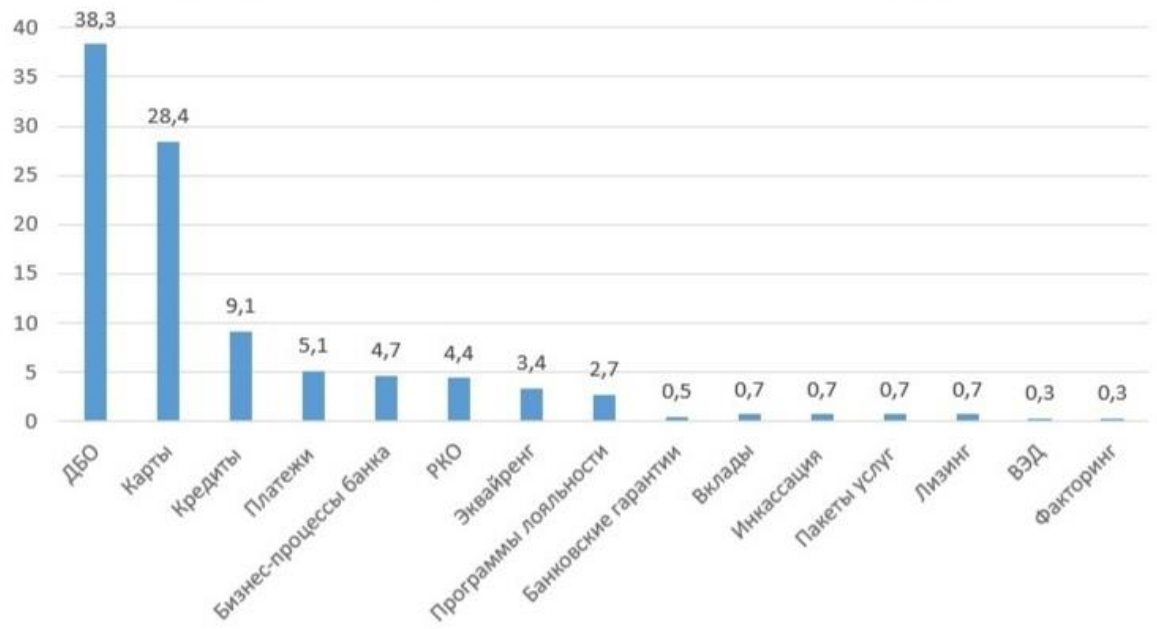


Рис. 1. Структура инноваций в российских банках по продуктам

Итак, анализируя статистику за 2020 год самая большая доля использования инноваций клиентами приходится в дистанционном банковском обслуживании (38,3%) и использование банковских карт (28,4%).

Не смотря на положительные стороны введенных инноваций, рост популярности использования мобильных приложений, оплаты через электронные карты, повышает риск:

1) кражи паролей к кредитным картам;

2) распространения на черном рынке базы данных пользователей;

3) при утери банковской карты, возможны списания с нее денежных средств через бесконтактную оплату;

4) мошенничество со стороны лиц, не являющихся работников банков, но представляющиеся таковыми;

5) отмывание нелегально полученных денежных средств через банки.

Все эти риски провоцируют недоверие со стороны частных клиентов к банку и таким инновациям.

Для того, чтобы решить данные проблемы, следует:

1) для ликвидации риска кражи паролей банки уже предусмотрели решение через использование электронные цифровые подписи, то есть привязка номера телефона к банковской карте.Единственное, что нужно сделать – это убедить клиентов в необходимости данной функции.

2) чтобы обеспечить гарантию сохранения базы данных пользователей, необходимо иметь эффективный внутренний контроль за системой, а также следить за профессиональной этикой сотрудников. Были случаи, когда личные данные клиентов банка были выставлены на черном рынке, это произошло по вине сотрудника банка, а значит руководство не досмотрело за компетентностью сотрудника. Для ликвидации подобных случаев нужно внимательнее подходить к найму и подбору работников, а также заключать договора о неразглашении данного рода информации о клиентах и следить за их уровнем знания установленных правил и обязанностей в банке;

3) когда банки внедряют инновации, связанной с предоставлением банковских услуг через приложение и интернет, возникают риски потери или ошибке данных при переводе. Это происходит из-за неисправности серверов банка или ошибки в системе. Для решения этой проблемы необходимо обеспечить контроль за работой серверов и нанять соответствующих специалистов для обеспечения их стабильной деятельности.

4) банки могут внедрять биометрические идентификационные устройства для защиты денежных средств при операциях, например,необходимо будет проверить отпечатки пальцев клиентов, прежде чем провести операцию.

5) также требуется осуществить наблюдение за выполнением этапов, стадий инновационного процесса во времени и синхронизацией всех видов деятельности;

6) подготовить соответствующий персонал для осуществления инноваций.

Кроме того, для обеспечения эффективного процесса внедрения инноваций нужно обеспечить осуществление следующих задач:

– оценки мировых тенденций научно-технического развития;

– разработка стратегии инновационной политики и механизмов ее осуществления;

– формирование стратегических целей инновационной деятельности;

– разработка планов и программ инновационных проектов;

– разработка организационно-производственной структуры управления инновационной деятельностью;

– планирование организации инновационного процесса.

Таким образом, с ростом инноваций в банковской сфере появляются риски, угрожающие экономической безопасности банка, появляются все новые мошеннические схемы, поэтому банки должны анализировать риски, быстро и качественно удовлетворять потребности быстрорастущего рынка, больше инвестировать в системы защиты, начиная от корпоративной сетевой структуры и кончая продуктовой безопасностью.

СПИСОК ЛИТЕРАТУРЫ

1. Будович Ю.И. Влияние научно-технического прогресса на экономическую безопасность банковского сектора /Рыжова И.А. // Экономика и бизнес. – 2019 г. С. 113-120.
2. Гультяев, В. Ю. Виды современных электронных банковских инноваций / Гультяев В.Ю. // Молодой ученый. – 2015 г. С. 405-407. URL: https://moluch.ru/archive/92/20097/ (дата обращения: 1.08.2021).
3. Казанская, Е. А. Инновации в банковской сфере / Казанская Е. А. // Молодой ученый. – 2019 г. С. 297-301. URL: https://moluch.ru/archive/119/32960/ (дата обращения: 2.08.2021).
4. Макарова Ю. Что будет с банковским сектором в будущем – итоги конференции РБК / Макарова Ю. // РКБ. – 2021 г. URL: https://trends.rbc.ru/tre nds/futurology/60b7 8acb9a7947b0ed4e93c0(датаобращения: 2.08.2021).
5. Мэтт МиллсТехнологические тенденции, принятые банковскими организациями в 2021 году // ITIGIC. – 2021 г. URL: https://itigic.com/ru/technology-trends-adopted-by-banking-organizations-in-2021/ (датаобращения: 3.08.2021).
6. Толмачева Е. Тренды мобильного банкинга 2021 / Толмачева Е. // RusBase. – 2020 г. URL: https://rb.ru/opinion/bank-trends/ (датаобращения: 2.08.2021).
7. Филиппов А. Основные тренды банковской системы РФ на 2021 год / Филиппов А. // Банки Сегодня. – 2020 г. URL:https://bankstoday.net/last-articles/eshhe-bolshe-tsi frovyh-tehnologij-osnovnye-trendy-bankovskoj-sistemy-rf-na-2021-god (дата обращения: 1.08.2021).

УДК 338

Р. В. ГАЙСИН, А. И. ЛАТЫПОВ
latypov.amir@yandex.ru ,romangaysin1505@icloud.com
Науч. руководов. – асс. С. С. ВАСИЛЬКЕВИЧ

Уфимский государственный авиационный технический университет

РАЗРАБОТКА СИСТЕМЫ МАРКЕТИНГОВОГО ОБЕСПЕЧЕНИЯ ЭЛЕКТРОКАРА «TESLAMODELX»

Аннотация. В данной статье рассматриваются проблемы и цели внедрения электрокара«TeslaModelX» на рынок в городе Москва.
Ключевые слова: маркетинг; товар, электрокар «TeslaModelX»; портрет покупателя; цена; опрос; реклама; продвижение; отдел маркетинга; проблема.

TeslaModel X – третий экземпляр в линейке Теслы, объединивший в себе уже немалый опыт, которым располагает корпорация. Автомобиль является представителем нового типа электромобилей. Авто TeslaModel X выполнен в стиле кроссовер. Внешний вид автомобиля соответствует ультрасовременному дизайну.

В данной статье рассматривается проблема: какие требования предъявляют покупатели к товарам данного рода.

Цели данной статьи разделены на описательные, поисковые и экспериментальные. Данное уточнение позволяет определить задачи и направления, позволяющие ввести новый товар –электрокара «TeslaModelX»на рынок.

Описательные цели, к ним относятся:

– определить уровень дохода населения в городе Москва. Данные «Росстат» (информационный барьер) [1];

– определить численность мужского населения в возрасте от 30-50 лет, у которых доход в месяц больше чем 100 тысяч рублей в городе Москва. Данные «ФСГС» (информационный барьер) [1];

– определить число мест в Москве, где можно зарядить электрокар (информационный барьер);

– определить уровень инфляции в городе Москва на 2019 г. (рыночный барьер) [2];

– определить уровень деловой активности. Данные инвестиционного портала города Москвы (рыночный барьер);

– определить данные по объему продаж автомобилей «Tesla» в городе Москва. Данные «Официальный сайт компании «Tesla» (информационный барьер) [3].

Поисковые цели:

– определить, часто ли москвичи посещают автосалоны, выставки, проходящие в городе Москва. Можно определить путем наблюдения на различных интерактивных выставках и демонстрациях электрокаров (демографический барьер);

– выяснить сложившееся общественное мнение о марке на протяжении всего времени существования компании. Сложившееся общественное мнение можно определить путем опроса. Его проведение будет производиться следующим образом: опрос реальных покупателей и опрос потенциальных покупателей (психологический барьер);

– определить является ли важным интерьер салона «Tesla» в городе Москва. Сложившееся общественное мнение можно определить путем опроса. Его проведение будет производиться следующим образом: опрос реальных покупателей и опрос потенциальных покупателей (психологический барьер);

– определить насколько нормативно – правовая база России благоприятна для внедрения на рынок. Можно определить путем обращения в федеральную службу по надзору в сфере защиты прав потребителей и благополучия человека (политический барьер);

– определить является ли важным качество обслуживания при покупке автомобиля в городе Москва. Рекомендуется проводить наблюдение в салоне «Tesla» за обслуживанием и взаимодействием персонала магазина с покупателями (информационный барьер);

– определить какие марки машины предпочитают лица мужского пола в городе Москва. Рекомендуется проводить анкетирование на демонстрациях и выставках автомобилей, где будут указываться параметры наиболее привлекательные для потребителей (психологический барьер);

– определить число потенциальных покупателей, способных по уровню получаемых доходов приобрести электрокар «TeslaModel X». Источник – анкетирование (экономический барьер).

Экспериментальные цели:

Увеличится ли объем продаж, если открыть салон в Санкт-Петербурге.Эксперимент: компания «Tesla» откроет салон в городе Санкт-Петербург. Цель открытия нового магазина – привлечь покупателей и повысить объем продаж.

Основными характеристиками электрокара «TeslaModel X» являются:

– длина кузова: 4,005 метра;

– ширина кузова: 2,083 метра;

– высота кузова: 1,626 метра;

– мощность мотора: 518 лошадиных сил;

– емкость аккумулятора:90 кВт;

– запас хода: 489 км;

– цена: 11300000 рублей.

Данный товар ориентирован на мужчин в возрасте от 30-50 лет (со сложившейся карьерой и высоким уровнем дохода). Они финансово независимы, и могут позволить себе приобретение дорогих автомобилей.

Для привлечения внимания потенциальных покупателей к товару проводился опрос. Рекламой электрокаров занималось рекламное агентство «i-Media». Реклама будет направлена непосредственно на целевой сегмент. В основе нашей рекламы будут проявляться практичности, удобства и эксклюзивности, а также образ владельца электрокара.

При помощи данного агентства, мы расширим свои возможности контакта с «избранной» аудиторией, у которой будет желание приобрести электрокар. Наша адресная программа будет включать в себя:

– престижные кофейни в городе Москва, например, «NordCoffe», «Double B», «KrispyKreme»;

– уютные рестораны в городе Москва, например, в стеклянных небоскребах, ресторан «SkyLounge», «Сахалин», «Roski», «WhiteRabbit»;

В перечисленных локациях планируется демонстрировать рекламные ролики TeslaModel X, где будет изображен продукт компании «Tesla».

Также, задачей выбранного нами рекламного агентства «i-Media» будет грамотная разработка наших социальных сетей, вирусной рекламы и web-дизайн.

Основными носителями рекламы будут социальные сети, такие как Инстаграм, ВКонтакте, Telegram, Twitter, YouTube, Tik-Tok, Twitch, В них планируется продвижение аккаунтов с качественным контентом и эстетичным визуалом страниц.

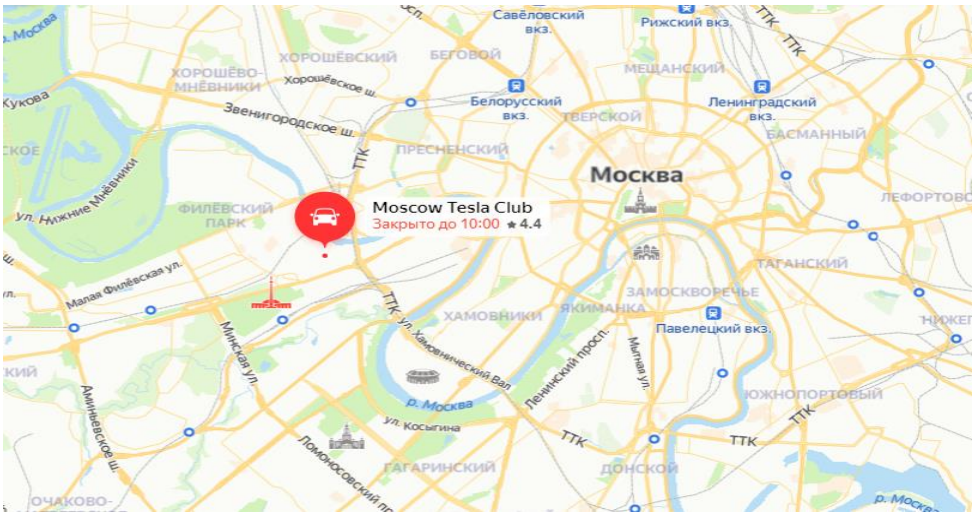


Рис. 1. Магазин «MoscowTeslaClub» на карте Москвы

Проведенный анализ маркетинговой среды показал, что электрокар «TeslaModel X»имеет определенный портрет покупателя: потенциальных клиентов, что облегчает внедрение товара для определенной доли населения. До-

стижение поставленной цели и решению проблемы поспособствует усиленная работа отдела маркетинга и активная работа с потенциальными клиентами.

СПИСОК ЛИТЕРАТУРЫ

1. Федеральная служба государственной статистики: [сайт]. URL: https://rosstat.gov.ru/folder/12781 (дата обращения: 15.11.2020).
2. Федеральная служба государственной статистики Москвы: [сайт]. URL: http://www.moscow.gks.ru/ (дата обращения: 15.11.2020).
3. Официальный сайт компании TeslaMotors: [сайт]. URL: https://www.tesla.com/ (дата обращения: 15.11.2020).
4. Ф. Котлер, Маркетинг менеджмент, Пер. с англ.- С. Жильцов, издательство – Питер, 12-е издание, 2007.- 814с. (дата обращения: 15.11.2020).
5. Тасс информационное агентство России: [сайт]. URL: http://www.tass.ru/ (дата обращения: 15.11.2020).
6. Ф.Котлер, Основы маркетинга. Пер. с англ.–М.: Прогресс, 2005. – 736 с. (дата обращения: 20.11.2020)
7. Родионова Л.Н., Руднева Ю.Р., Пашин С.Т. Методические указания к выполнению курсовой работы по дисциплине «Маркетинг» для студентов спец. 08.01.05. – Уфа, Изд-во «Диалог», 2007 (дата обращения: 20.11.2020).
8. Родионова Л. Н.Р60 Маркетинг. Коммуникации в маркетинге: учебное пособие / Уфим. гос. авиац. техн. ун-т. – Уфа: РИК УГАТУ, 2019. – 223 с. (дата обращения: 20.11.2020).
9. Карты Москвы 2ГИС: [сайт]. URL: https://2gis.ru/moscow/ (дата обращения: 01.12.2020).
10. Центральный банк Российской Федерации: [сайт].URL: http://www.cbr.ru/ (дата обращения: 20.11.2020).
11. Московская биржа: [сайт]. URL: http://www.moex.com/ (дата обращения: 20.11.2020).
Экспорт и Импорт России по товарам и странам: [сайт]. URL: http://ru-stat.com/ (дата обращения: 03.12.2020).
12. EUROPAGES: [сайт]. URL:https://www.europages.com.ru/ (дата обращения: 10.12.2020).
РБК: [сайт]. URL: https://ufa.rbc.ru/ (дата обращения: 10.12.2020).
13. Официальный сайт компании LucidMotors: [сайт]. URL: https://www.lucidmotors.com/ (дата обращения: 10.12.2020).
14. Официальная сайт рекламного агентства i-Media: [сайт]. URL: https://www.i-media.ru/ (дата обращения: 10.12.2020).
15. Официальный магазин Tesla в городе Москва: [сайт]. URL: https://moscowteslaclub.ru/ (дата обращения: 10.12.2020).

УДК 338

Д. А. ГРИГОРЬЕВА, Д. А. СЕРГЕЕВА
gridasha@gmail.com,dashas2029@mail.ru
Науч. руководов. – асс. С. С. ВАСИЛЬКЕВИЧ

Уфимский государственный авиационный технический университет

РАЗРАБОТКА СИСТЕМЫ МАРКЕТИНГОВОГО ОБЕСПЕЧЕНИЯ МОМЕНТАЛЬНОЙ КАМЕРЫ «POLAROID Z340»

Аннотация. В данной статье рассматриваются проблемы и цели внедрения фотоаппарата «Polaroid Z340» на рынок в городе Москва.
Ключевые слова: маркетинг; товар; фотоаппарат «Polaroid Z340»; портрет покупателя; цена; опрос; реклама; продвижение; отдел маркетинга; проблема.

Фотоаппарат-полароид – это необычный атрибут, который должен быть в каждом доме. Он позволит ретушировать фотографии на самом экране полароида, а также мгновенно печатать их. Для каждого человека, фотоаппарат приобретает особое значение, поскольку поможет запечатлеть и оставить не только в памяти, но и на фотокарточках самые яркие, волнительные и важные моменты в жизни людей.

В данной статье рассматривается проблема: какие требования предъявляют покупатели к товарам данного рода.

Цели данной статьи разделены на описательные, поисковые и экспериментальные. Данное уточнение позволяет определить задачи и направления, позволяющие ввести новый товар – фотоаппарат «Polaroid Z340» на рынок.

Описательные цели, к ним относятся:

– определить общественное отношение к марке «Polaroid»;

– выяснить, как формировалась цена на «Polaroid Z340»;

– определить, какие мероприятия будут проводиться компанией «Polaroid» для привлечения покупателей;

– выявить основные предпочтения покупателей при выборе фотоаппаратов-полароидов;

– определить количество магазинов в городе Москва. Данные «Карты Москвы 2ГИС» [10];

– определить данные по объему продаж фотоаппаратов «Polaroid» в городе Москва. Данные «Официальный сайт компании «Polaroid»» [2].

Поисковые цели:

– поиск конкурентов на российском рынке компании «Polaroid»;

– выявить конкурентные преимущества компании «Polaroid»;

– определить динамику объема российского рынка моментальных камер;

– определить численность женского и мужского населения в возрасте от 17 до 50 лет, у которых доход в месяц больше чем 45 тысяч рублей в городе Москва. Данные «ФСГС» [1];

– определить источник, из которого покупатели узнали о «Polaroid Z340»;

– определить отношение покупателей к марке «Polaroid» в городе Москва в 2020 году и готовы ли они порекомендовать данный товар друзьям, коллегам [3];

– определить модели фотоаппаратов, которые предпочитают люди в возрасте от 17 до 50 лет в городе Москва [3];

– определить, какие функции фотоаппарата важны для покупателей в городе Москва [3].

Экспериментальные цели:

– определить, увеличится ли объем продаж при запуске акции, если при покупке товара «Polaroid» аксессуар будет идти в подарок при оставлении отзыва. Эксперимент: компания «Polaroid» запустила акцию в магазинах своего представителя, что при покупке товара, консультант предложит оставить отзыв о магазине «PolaStore», качестве его обслуживания и почему он приобретает товар компании «Polaroid», за что ему в подарок на выбор предоставят либо картридж для фотоаппарата, либо два набора кассет (фотобумаги), например, цветную и черно-белую или две одинаковых;

– определить, увеличится ли объем продаж на 7%, если будет предоставляться скидка 5% на приобретение следующего товара компании «Polaroid». Эксперимент будет проводиться в течение года.

Основными характеристиками фотоаппарата «Polaroid Z340» являются:

– разрешение матрицы: 14 Мпикс;

– максимальное разрешение: 4320 х 3240;

– диагональ ЖК-экрана: 2.7 дюймов;

– время работы таймера: 10 с;

– формат кадра (фотосъемка): 4:3, 3:2, 16:9;

– максимальный объем карты памяти 32 Гб;

– объем встроенной памяти 32 Мб;

– размер: 65х155х128 мм;

– вес: 620 г, с элементами питания.

Данный товар ориентирован на людей в возрасте от 17 до 50 лет, как мужского, так и женского пола, которые любят делать фотографии и фотографироваться, тех, кто предпочитают напечатанные фотокарточки, а не цифровые, которые хотят запечатлеть моменты своей жизни не только в памяти, но и в фотоальбоме.

Основными клиентами данного товара являются, во-первых, это фотографы, те, которые занимаются этим на профессиональной основе, во-вторых, это те, кто просто любит фотографировать, либо хотел фотоаппарат с мгновенной печатью.

В официальном магазине компании «Polaroid» – «PolaSotore» (рис.1) при покупке будет предоставлена анкета с опросом, в котором можно будет узнать пожелания покупателей, где будут указываться возраст покупателя и его предпочтительные модели фотоаппаратов, а также технические составляющие, например, функции, а также необходимую информацию для улучшения качества товара и роста продаж, аналогичный опрос будет представлен на официальном сайте магазина и компании в разделе «анкетирование». Также сотрудник магазина будет рассылать интернет-опросы на почту потребителям, где будут вопросы о качестве и узнаваемости товара «Polaroid», а также консультант может при личной беседе с покупателем узнать его отношение к марке «Polaroid». На рисунке 1 представлены торговые посредники в городе Москва [4].

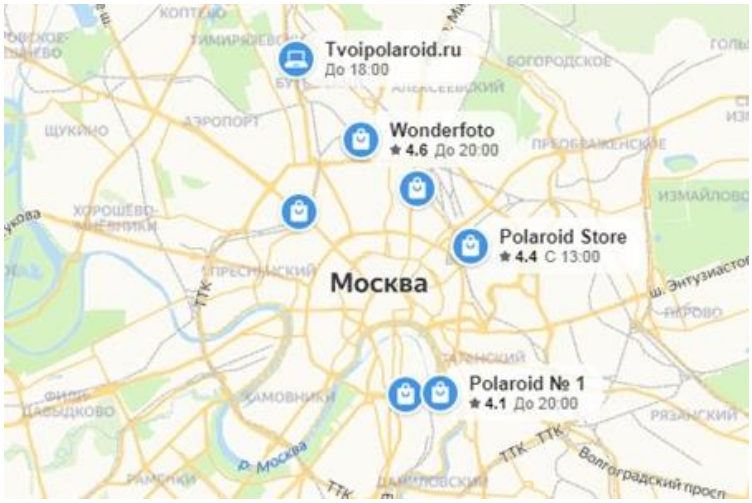


Рис. 1. Магазины «Polaroid» в городе Москва

Основными носителями рекламы будут социальные сети, такие как Instagram, ВКонтакте и TikTok. В них планируется продвижение аккаунтов с качественным контентом и эстетичным визуалом страниц. Например, показывая скрытые возможности фотоаппарата-полароид или как сделать интересные снимки в домашних условиях на данный товар. При помощи данного агентства, мы расширим свои возможности контакта с «избранной» аудиторией, у которой будет желание приобрести моментальную камеру.

Радио для рекламы использоваться не будет, так как это не целесообразно с таким сегментом товаров, как у нас.

Планируется рассылка писем на почту покупателей, в которых будет говориться о том, что в скором времени в продаже появится новый товар, с приложенными к письму видеороликом и описанием товара. Данная рассылка будет добровольна, этот пункт указывается в анкете. Видео должно быть заразительным и мотивировать покупателей на приобретение товара.

Проведенный анализ маркетинговой среды показал, что фотоаппарат «Polaroid Z340» имеет определенный портрет покупателя: потенциальных клиентов, что облегчает внедрение товара для определенной доли населения. Достижение поставленной цели и решению проблемы поспособствует усиленная работа отдела маркетинга и активная работа с потенциальными клиентами.

СПИСОК ЛИТЕРАТУРЫ

1. Федеральная служба государственной статистики: [Электронный ресурс]// URL: https://rosstat.gov.ru/
2. Федеральная служба государственной статистики Москвы: [Электронный ресурс]//URL: http://www.moscow.gks.ru/
3. Официальный сайт компании Polaroid: [Электронный ресурс]//URL: https://eu.polaroid.com
4. Ф. Котлер, Маркетинг менеджмент, Пер. с англ.- С. Жильцов, издательство – Питер, 12-е издание, 2007.– 814с. (дата обращения: 15.11.2020).
5. Тасс информационное агентство России: [Электронный ресурс]//URL: http://www.tass.ru/
6. Ф.Котлер, Основы маркетинга. Пер. с англ.–М.: Прогресс, 2005. – 736 с. (дата обращения: 20.11.2020)
7. Родионова Л.Н., Руднева Ю.Р., Пашин С.Т. Методические указания к выполнению курсовой работы по дисциплине «Маркетинг» для студентов спец. 08.01.05. – Уфа, Изд-во «Диалог», 2007 (дата обращения: 20.11.2020).
8. Родионова Л. Н.Р60 Маркетинг. Коммуникации в маркетинге: учебное пособие / Уфим. гос. авиац. техн. ун-т. – Уфа: РИК УГАТУ, 2019. – 223 с. (дата обращения: 20.11.2020).
9. Цены на пластмассу: [Электронный ресурс]//URL: https://plastinfo.ru/
10. Карты Москвы 2ГИС: [Электронный ресурс]//URL: https://2gis.ru/moscow/
11. Центральный банк Российской Федерации: [Электронный ресурс]//URL: http://www.cbr.ru/
12. Московская биржа: [Электронный ресурс]//URL: http://www.moex.com/
13. Экспорт и Импорт России по товарам и странам: [Электронный ресурс]//URL: http://russtat.com/
14. EUROPAGES: [Электронный ресурс]//URL:https://www.europages.com.ru/
15. РБК: [Электронный ресурс]//URL: https://ufa.rbc.ru/
16. Официальный сайт Canon: [Электронный ресурс]//URL: https://store.canon.ru
17. Официальный сайт Fujifilm: [Электронный ресурс]//URL: https://www.fujifilm.eu/
18. Официальный сайт Vogue: [Электронный ресурс]//URL: http://www.vogue.com/
19. Официальный сайт рекламного агентства Ingate: [Электронный ресурс]//URL: https://www.ingate.ru/
20. Официальный магазин Polaroid в городе Москва PolaStore: [Электронный ресурс]//URL: https://pola-store.ru/ 21. Официальный сайт магазина Apple: [Электронный ресурс]//URL: https://www.apple.com/ru/
22. Официальный сайт магазина ShureStore: [Электронный ресурс]//URL: https://shure-shop.ru/
23. Анкетирование от компании Polaroid: [Электронный ресурс]//URL: https://docs.google.com/

УДК 33.336.74

А. Р. ГУДЫМЕНКО, Р. Р. МУЛЮКОВА
Rinatochka-m@mail.ru
Науч. руководв. – канд. экон. наук, доц. А. Н. ШЕРЫШЕВА

Уфимский государственный авиационный технический университет

ЦИФРОВЫЕ ДЕНЬГИ: ПРЕИМУЩЕСТВА, РИСКИ, ПЕРСПЕКТИВА ВЛИЯНИЯ НА ЭКОНОМИКУ

Аннотация. Причины развития криптовалюты. Влияние на экономику и денежную массу Российской Федерации. Протест различных государств «крипту». Цифровой юань, цифровое евро, цифровой рубль.
Ключевые слова: денежное обращение; цифровые деньги; блокчейн; цифровые технологии; криптовалюта; цифровой рубль; юань и евро; цифровизация национальных валют.

Исторически сложилось так, что денежное обращение стало являться важнейшим элементом экономики. И в течение вот уже последних 20 лет, как в России, так и в других странах идет постепенная цифровизация денежной системы, это связано с развитием технологий, а точнее цифровых технологий.

Данная тема достаточно актуальна на сегодняшний день, сейчас в период цифровизации электронные деньги становятся неотъемлемой частью рыночной экономики и их роль только растет, а с появлением новых денежных форм появляется мобильность в платежах.

Кроме того наряду с наличными все больше используются безналичные деньги для оплаты товаров и услуг, осуществления платежей и переводов.

Если рассматривать цифровые деньги, то одной из их разновидностей является криптовалюта. Это актив, который используется в качестве средства обмена и считается надежным, потому что в его основе лежит криптография.

Криптовалюта, говоря простыми словами, это цифровое платежное средство, а именно виртуальные денежные средства, которые не имеют выражения в металлических или бумажных деньгах и существуют только в электронном виде.

Ключевой особенностью криптовалют является децентрализация, то есть отсутствие определенного внутреннего или внешнего администратора. Именно

поэтому некоторые государства категорически против использования криптовалюты, ведь главным преимуществом использования крипта является: анонимность, что говорит о том, что практически невозможно вычислить, где, чьи активы находятся на пространствах Интернета, а также волатильность (формируется угроза финансовой безопасности любого государства).

Так, например, в Китае власти сообщают о желании ужесточить контроль в отношении использования платформ, позволяющих торговать гражданам криптовалютой на зарубежных площадках.

Кроме того, о желании регулировать криптовалютную сферу заявила и Россия. Так, считается, что если процесс обмена не контролировать, то это может вызвать тяжелейшие экономические и социальные последствия.

Также за развитием криптовалют наблюдает и Евросоюз – он не принял официального решения по отношению легализации или регулирования, однако как альтернатива, все чаще там упоминается такое понятие, как «цифровой евро».

Итак, в январе 2020 года Европейский центральный банк (ЕЦБ), который регулирует выпуск и обращение евро, вместе с несколькими другими центробанками вошел в рабочую группу по исследованию CBDC(государственных цифровых валют).

Дискуссии о важности цифрового евро продолжались достаточно долго, однако статистика гласит, что в Европе электронные платежи непопулярны. Так, например, в марте 2020 года 76% всех платежей были совершены в евро, а спрос на новые наличные превышает уровень роста ВВП.

В Китае же ситуация совершенно другая, в стране действует официальная цифровая валюта – цифровой юань. Цифровой юань – это цифровая форма физической валюты Китая, при этом распространяется центральным банком Китая среди провайдеров второго уровня, также включая государственные банки и провайдеров онлайн-платежей, таких, как Alipay и WeChatPay.

Наряду с цифровым евро и юанем несомненно следует рассмотреть цифровой рубль.

По данным ЦБР, цифровой рубль – дополнительная форма российской национальной валюты, которая будет эмитироваться Банком России вцифровом виде. Цифровой рубль сочетает в себе свойства наличных и безналичных рублей.

Так как в последние годы растет использование безналичных денег, цифровой рубль может стать новым удобным дополнительным средством расчета, как для покупателей, так и для продавцов, в том числе на отдаленных, малонаселенных и труднодоступных территориях, где доступ к финансовой инфраструктуре ограничен.

На сегодняшний день во многих странах активно развиваются цифровые национальные валюты, вследствие чего необходимо создать технологическую взаимосвязь систем, ведь при их отсутствии вряд ли будет возможно разграниченное и рациональное использование цифровых валют.

СПИСОК ЛИТЕРАТУРЫ

1. Звягин Л. С. Цифровая экономика и криптовалюты: вызов или угроза традиционному обществу. E-Management. 2018;1(2):80-92. DOI: 10.26425/2658-3445-2018-2-80-92
2. Клейнер Г. Б. Системный учет последствий цифровизации общества и проблемы безопасности. 2018;210(2):63-73.
3. Равал С. Децентрализованные приложения. Технология Blockchain в действии. Пер. с англ. СПб.: Питер; 2017. 192 с.

УДК 331.1

А. П. ЕГИАЗАРЯН, С. И. ТЫЖБЫР
annaegiazaryan2000@gmail.com
Науч. руководитель – канд. экон. наук, доц. И. А. НАГИМОВА

Уфимский государственный авиационный технический университет

МЕТОДЫ СНИЖЕНИЯ СОПРОТИВЛЕНИЯ ИННОВАЦИЯМ В КАДРОВОМ МЕНЕДЖМЕНТЕ

Аннотация. Цель исследования – оценить и раскрыть все методы создания условий эффективной деятельности персонала. В данной статье рассматривается термин мотивации. Анализируются и оцениваются важные показатели относительно этого термина. Авторами рассмотрены и раскрыты два вида мотивации персонала, а также их применение на практике. Основное внимание уделяется человеческим потребностям и инстинктам. В результате определено, что мотивация играет огромную роль в успешном развитии любой компании.
***Ключевые слова*:** деятельность; мотивация; нематериальная мотивация; персонал; потребности; результат; руководитель; рынок труда; финансовая мотивация.

Мотивация является важным фактором возникновения у человека желания достижения быстрого и качественного результата. Что мы понимаем под словом мотивация? Значение слова (от лат. movere) — «двигаю». Если простыми словами, мотивация — это побуждение к действию, движению. То есть является основным инструментом управления персоналом.

Существуют различные методы мотивации. И все эти методы можно разделить на 2 категории. Это нематериальная и материальная, т.е. финансовая мотивация.

Все люди разные, и у каждого свои потребности. Но зачастую, когда человек приходит устраиваться на работу, первым делом его интересует вопрос «сколько?». Сколько будут ему платить за ту или иную работу. А уже потом он задается другими вопросами: что делать, какой график, коллектив и т.д.

Финансовая мотивация является очень важной, и сейчас обсудим ее ключевые элементы. Цель финансовой мотивации: системный интерес сотрудника к достижению результатов в труде. Для руководителя деньги – инструмент мотивации. Какие могут быть варианты финансовой мотивации? Рассмотрим отдельно каждый:

– фиксированная оплата. Когда оплата стабильна, то есть, фиксирована, это слишком просто. Такой вид оплаты желания работать не вызывает. Наоборот демотивирует сотрудников. Они будут абсолютно не заинтересованы активно работать.

– Оплата за результат. Тут начинаются проблемы с дисциплиной. Человек начинает наплевательски относиться к расписанию. Учитывая тот факт, что ему платят за результат, он считает приходить во столько, во сколько захочет.

– Фиксированная + за результат. Наиболее рациональная и оптимальная система финансовой мотивации. Фиксированная плата позволяет руководителю требовать от сотрудника каких-то базовых вещей, например: заполнять в системе все данные о клиентах, либо приходить вовремя на работу. Далее основная часть – это процент от продаж (т.е. это результат), стимулирует сотрудника интенсивнее выполнять свою работу, чтобы получить больше заработной платы.

– Бонусы. Бонусы это то, что стимулирует делать какие-то конкретные действия. Бонусы позволяют замотивировать сотрудника делать какие-то узкие вещи внутри компании, которые сейчас необходимы. Например: У нас затоварен склад, нам нужно продать конкретную продукцию. Мы ставим бонусы: продаешь именно эту продукцию и получаешь дополнительную премию. И это работает.

– Планы. Чем чаще дается план, тем лучше сотрудники работают. План на месяц не очень хорошо работает, план на неделю уже лучше, в идеале ставить план каждый день.

– Система штрафов. Также является одним из видов материальной мотивации. К штрафам можно отнести:

1) взыскание денег с работника компании за невыполнения нормативов и стандартов;

2) взыскание денег с сотрудника за его плохую работу;

3) дополнительные рабочие часы за плохую работу, либо же наоборот сокращение рабочих часов.

Надо понимать, что финансовая мотивация людей мотивирует до тех пор, пока не закрыты базовые потребности. Т.е. когда человеку начинает хватать на жизнь, тогда деньги перестают его мотивировать. К чему это приводит? Сотрудник не заинтересован в работе, он стоит на месте, компания не развивается, находится в состоянии застоя. А значит, бизнес зашел в тупик. Чтобы такого не происходило, сотрудники должны быть всегда замотивированы.

Итак, рассмотрим инструменты нематериальной мотивации:

– Внимание руководителя. Само по себе внимание является инструментом мотивации людей. Руководитель для сотрудника лицо авторитетное. Обращая внимание к деталям работы сотрудника, руководитель поощряет его и это сильно мотивирует и ценится. И наоборот лишение внимания может оказаться сильным инструментом наказания.

– Интересная работа. Необходимо помогать людям найти то, что им интересно. Предлагать участвовать в новых проектах, подключаться к более сложным задачам. Если работа наскучит, сотрудник перестанет делать ее нормально, как бы хорошо его не заинтересовывали материально. Многих людей добивает рутина и монотонность. Нужно что-то новое.

– Лояльность руководителя. Руководитель начинает хвалить, показывать (вербально и невербально) поддержку. Очень важный нюанс, эту лояльность разделять, не пытаться относиться к ним как к детям. В чем отличие детей и сотрудников. Детей мы любим просто за то, что они есть, и неважно как они себя ведут хорошо или плохо. А вот с сотрудниками не так. Лояльность они должны заслужить результатом. Пока он есть – вы лояльны. Это тонкий инструмент, который всегда работает.

– Доверие. Мощнейший мотивационный инструмент. Когда руководитель советуется, подключает к разработке стратегических решений, либо оставляет

кого-то из своих сотрудников за главного, во время своего отсутствия, это поднимает работника на более высокий уровень и очень окрыляет.

– Перспектива и карьера. Люди очень любят пирамидальную модель общества. Когда ты четко видишь, как ты можешь расти. Сделать хотя бы небольшую градацию и у сотрудников уже есть повод бороться за то, чтобы перейти на следующую ступень карьерного развития. Это очень сильный инструмент. Но для большей эффективности карьерная лестница должна быть условная, т.е. что не навсегда младший специалист стал старшим, а до тех пор, пока выполняет условия (например, мин план плюс какие-то дополнительные показатели). Этот инструмент отличен тем, что для руководителя он бесплатный. Он придумывает эту пирамидку и люди в нее играют как в компьютерную игру, а для руководителя это почти ничего не стоит, то есть вместо того, чтоб существенно увеличить сотруднику зарплату, можно просто повысить его в должности. И люди будут это очень ценить и стремиться достичь все больших высот.

– Признание. Людям очень хочется, чтобы их внешне признавали. Самый простой вариант: чаще говорить людям прилюдно спасибо. Фото на доске почета – это вообще ничего не стоит, а для людей очень-очень большой повод порадоваться.

– Обучение. Для многих людей обучение – один из важнейших стимулов в жизни, который они мало где могут получить. Если вы начинаете в них вкладываться и обучать, то люди будут это очень ценить.

– Дополнительный отпуск. Либо продляете на несколько дней отпуск, либо даете дополнительный внеочередной отпуск на неделю за большие достижения на работе.

– Снижение уровня контроля. Это отличный инструмент, когда мы за какие-то подвиги начинаем снижать требования по типу заполнения

ежедневного отчета, либо же время начала рабочего дня, появляется интерес держать планку, чтоб не потерять эти бонусы со стороны руководителя.

И вот мы рассмотрели два основных вида мотивации, на самом деле есть еще третий, очень сильный вид мотивации – это мотивация средой, когда мы создаем такую среду для людей, что они не могут не меняться, а только стараются работать эффективно, добиваясь лучших результатов. Такая среда создается лишь при правильном подходе руководителя к материальной и нематериальной мотивации.

Анализируя методы мотивации, мы выделили самые нестандартные, которые применяются за рубежом, так как грамотное стимулирование сотрудников предоставляет возможность:

1) Минимизировать текучесть кадров;

2) Привлекать лучших сотрудников в свою компанию;

3) Выявлять и поощрять тех, кто этого заслуживает.

Самые нестандартные способы мотивации сотрудников за рубежом это:

1) Применение необычных названий для должности, например Стив Джобс изменил название должности «офисного консультанта» на «гений»;

2) Одна из зарубежных компаний позволяет сотрудникам приводить в офис домашнего питомца, называя это «днем пушистых»;

3) В Японии компания предоставляет отгул женщинам, которые расстались с любимым;

4) Также в Японии практикуют ситуацию, когда компания сама беспроцентно кредитует своих сотрудников. Компания берет на себя все расходы в случае дорогостоящей учебы работника и его детей.

5) Во Франции практически 69% жителей считают лучшей нематериальной мотивацией скользящий или гибкий график работы, вплоть до фриланса и компании идут на эти условия, для повышения трудоспособности коллектива.

Навык создания правильной системы мотивации – это очень важно Сегодня рынок труда в большом дефиците квалифицированных специалистов.

В одиночку хорошего бизнеса не построишь. А для того, чтобы компания успешно развивалась, необходим стабильный эффективный коллектив. Все

вышеприведенные инструменты мотивации персонала помогут руководителю стимулировать сотрудников на эффективную деятельность, тем самым решится проблема текучки кадров. Это также позволит сэкономить драгоценное время и средства на поиск и адаптацию новых специалистов, а также поможет сформировать крепкий надежный коллектив профессионалов.

СПИСОК ЛИТЕРАТУРЫ

1. Аблязов, Р.С. Соревновательный способ мотивации как метод повышения производительности труда [Текст] / Р.С. Аблязов // Аграрная наука. – 2014. – № 9. – С. 5-7.
2. Базаров, Т.Ю. Управление персоналом [Текст] / Т.Ю. Базаров. – М.: Наука, 2015. – 402 с.
3. Варданян, И.С. Предложение по совершенствованию системы нематериального стимулирования [Текст] / И.С. Варданян // Управление персоналом. – 2015. – № 4. – С. 42-46.
4. Гонова, А.А. Основные направления повышения эффективности системы мотивации персонала на предприятии [Текст] / А.А. Гонова // Проблемы региональной экономики. – 2014. – № 1/2. – С. 207-208.
5. Колесников, Б.И. Совершенствование мотивации эффективной деятельности работников предприятия [Текст] / Б.И. Колесников. – М. : ВИНИТИ РАН, 2015. – 131 с.
6. Макарова, А.О. Анализ методов и видов стимулирования труда на российских предприятиях [Текст] / А.О. Макарова // Молодой ученый. – 2013. – №6. – С. 376-379.
7. Мишурова, И.В. Управление мотивацией персонала [Текст] / И.В. Мишурова. – М.: Феникс, МарТ, 2016. – 272 с.
8. Надеждина, В. Эффективная мотивация персонала. Как добиться максимум результата при минимуме затрат [Текст] / В. Надеждина. – М.: Харвест, 2015. – 254 с.
9. Шапиро, С.А. Мотивация и стимулирование персонала. – М.: ГроссМедиа, 2015. – 112с.

УДК 332.1

А. Т. ЗАКИРОВА, А. А. КОМЫШЕВА
zak1rovaaigul@yandex.ru,komusheva01@gmail.com
Науч.руководов.–канд. экон. наук, доц. Ю. Т. МАНСУРОВА

Уфимский государственный авиационный технический университет

АНАЛИЗ АСПЕКТОВ ИННОВАЦИОННОГО РАЗВИТИЯ РЕСПУБЛИКИ БАШКОРТОСТАН

Аннотация. Данная статья посвящена оценкероли инноваций в развитии Республики Башкортостан, анализу уровня и качества инновационного развития разных инфраструктур в Республике. Рассмотрены различные новые проекты ивыявлены основополагающие проблемы развития инновационной системы Республики Башкортостан и разработана система инновационной политики направленная на повышение эффективности использования инновационного потенциала.
Ключевые слова: инновации; инновационное развитие регионов;импортные технологии;инновационный потенциал; информационная инфраструктура; цифровые технологии, технологическая платформа.

«Наш современный образ жизни создан не политиками. До 1700 года люди были бедны как церковные мыши. Жизнь их была короткой и жестокой. И дело не в том, что тогда не было хороших политиков, они встречались. Но тогда люди начали активно изобретать: электричество, паровые двигатели, микропроцессоры, понимание генетики и медицины и так далее. Да, стабильность и образование очень важны, я не буду с этим спорить, но настоящий двигатель прогресса – это инновации» сказал Билл Гейтс американский предприниматель и общественный деятель 1955. Действительно, инновации – настоящий двигатель прогресса. Ведь именно создание и освоение новых технологий, приводитк совершенствованию и эволюции человечества.

Актуальность инновационного развития регионов обусловлена тем, что от инновационной активности и восприимчивости региональных отраслей зависит конкурентоспособность России в мировой экономике.

Для развития регионов России в последние годы характерны:

– высокая доля промышленности в ВВП (ВРП), при этом низкая доля в сфере услуг;

– склонность к увеличению износа основных фондов;

– низкая доля высокотехнологической продукции;

– увеличение зависимости от импортных технологий.

На данный момент, менее изученным является развитие инновационной системы на мезоуровне, то есть на уровне регионов и в особенности старопромышленных регионов в условиях санкций западных стран, к которым можно отнести и Республику Башкортостан.

Республика располагает разнообразной экономической базой и имеет огромный инновационный потенциал: Башкортостан – признанный научный центр России во многих областях науки и техники, здесь существуют научные прикладные разработки мирового уровня, высшие учебных заведения, отраслевые исследовательские институты.

Формирование инновационной системы Республики Башкортостан началось с 2005 по 2010 год в рамках реализации Программы социально-экономического развития, далее с 2010 по 2014 год и в 2020 году получила наиболее активное развитие.

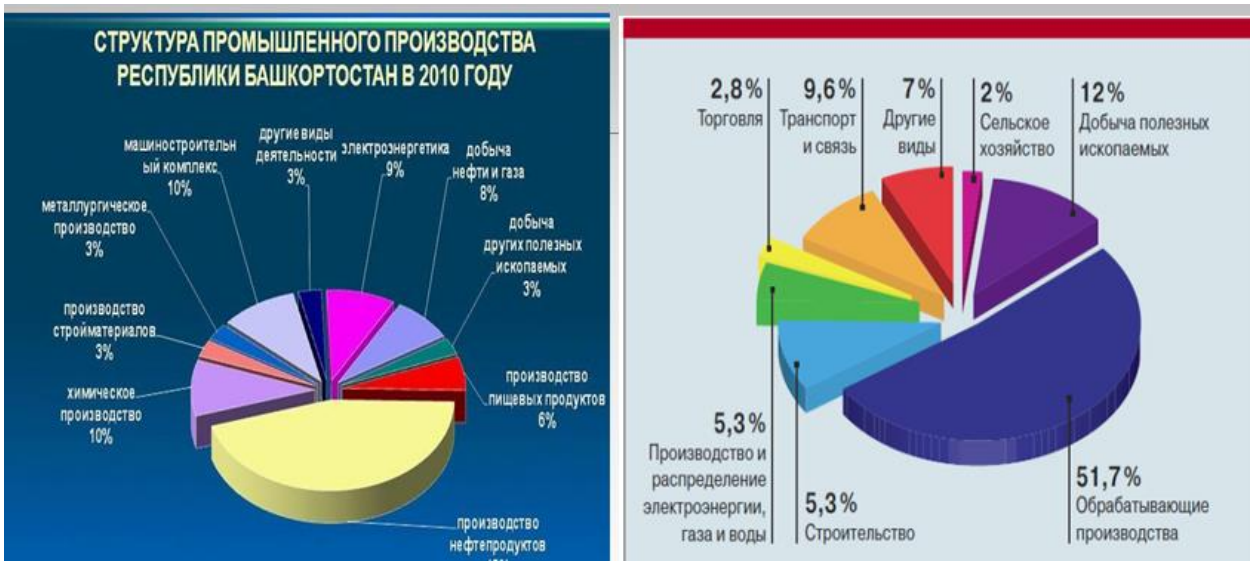


Рис. 1. Формирование инновационной системы Республики Башкортостан с 2010 по 2020 гг.

Кроме того, в республике сформированы элементы региональной инновационной системы, включающие в себя несколько секторов.

Также, по данным рейтинга инновационно-активных субъектов России за 2019 год, Башкортостан, оказавшись на 12 строчке, стабильно занимает место в группе средне-сильных инноваторов.

По ряду следующих показателей Республика находится в первой десятке субъектов РФ:

1) поступление патентных заявок (6 место);
2) выдача патентов (8 место);
3) использование передовых производственных технологий (7 место);
4) объем инновационных товаров и услуг (8 место);
5) созданные передовые технологии (39 место);
6) объем инновационных товаров в ВРП (22 место);
7) доля затрат на научные исследования и разработки в ВРП (36 место).

Далее, рассмотрим инновационную обстановку в различных структурах за последние три года, подведя итоги через более значимые достижения.

Информационная инфраструктура

В 2019 году в республикеблагодаря федеральному проекту «Информационная инфраструктура» 1191 учреждение подключили к высокоскоростному Интернету.

Также, завершено строительство 59 точек коллективного доступа (Wi-Fi).

Запущен проект «Доступный Интернет» для обеспечения интернетом 262 малонаселенных пункта.

В микрорайонах Уфы внедрена подсистема интеллектуального видеонаблюдения, из 951 видеокамеры с высоким качеством.

При реализации проекта «К 100-летию Республики Башкортостан», услугами сотовой связи обеспечены 40 населенных пунктов,.

Цифровое государственное управление

В 2018 году созданы «Единый интернет-портал Республики Башкортостан в сфере бизнеса и инвестиций», для взаимодействия с предпринимателями.

И «Лесная карта Башкортостана», сделавшая открытой информацию об использовании лесов и направленная на их сохранение.

В 2019 году Порталы «Электронная приемная органов власти Республики Башкортостан» и «Голос Республики Башкортостан» основные инструменты взаимодействия государства и общества в Интернете.

Реализован проект единой системы оплаты проезда «АЛГА».

Воплощен механизм подачи заявлений в электронном виде через региональный портал «Госуслуги Башкортостан» .

Кадры для цифровой экономики

В 2019 году к системе «Образование», осуществляющей онлайн контроль в обучении, присоединились все образовательные организации региона.

В течение 2019 года продолжила работу система «Электронное образование Республики Башкортостан». Успехом стало размещение на ней электронных курсов в области нефтегазовой промышленности.

В 2019 году Башкортостан вошел в пилотный проект по бесплатному обучению цифровым компетенциям. В нем приняли участие 11 образовательных организаций из Республики. Обучением которых, занимался и Уфимский государственный авиационный технический университет.

Цифровые технологии

В 2019 году для республиканских инновационных компаний выделено более 90 миллионов рублей и обеспечена методическая поддержка.

Также четыре инновационных компании региона выиграли гранты Фонда содействия инновациям.

С 1 января 2020 года госкомитет РБ по информатизации стал министерством цифрового развития государственного управления.

Благодаря изменениям в агропромышленном комплексе, аграрии Республики могут прямо с рабочих мест обмениваться с Минсельхозом всей необходимой документацией.

Несмотря на сложившуюся ситуацию в 2020 году, инновационное развитие Республики Башкортостан не стояло на месте.

В процессе мер по борьбе с распространением инфекции COVID-19 запущены: ситуационный центр по обеспечению устойчивого функционирования экономики, единый колл-центр для приема обращений граждан, оказавшихся в трудной жизненной ситуации.

Несмотря на это, существует широкий спектр нерешенных проблем, основными из которых являются:

– низкий уровень спроса на результаты инновационной деятельности со стороны реального сектора экономики;

– дисбаланс, в направленности научных исследований на потребности новых высокотехнологичных отраслей экономики, которые в настоящее время практически отсутствуют Башкортостане.

– неразвит рынок интеллектуальной собственности;

– концентрация развития инновационной инфраструктуры, в крупных городах и, в особенности, в г.Уфе;

– разобщенность, т.к многие научно-исследовательские учреждения федеральные, а отраслевые институты региональные или частные, что приводит к неэффективному использованию финансовых ресурсов.

Ключевой, является проблема повышения эффективности использования инновационного потенциала. Для рационального решения перечисленных проблем предлагается использовать некоторые типы инновационной политики:

– политики, ориентированной на государственную поддержку научных исследований в государственных и негосударственных инновационных предприятиях;

– политики, ориентированной на спрос научно-технических разработок со стороны реального сектора экономики;

– политики, направленной на совершенствование инновационной деятельности, посредством создания общего центра координации и четким разделением сфер деятельности;

– политики, направленной на стимулирование спроса инноваций в предпринимательском секторе, технологическое перевооружение ,выпуск и экспорт новой высокотехнологичной продукции;

В заключении можно сделать вывод, что для развития инновационной системы необходимо обеспечение как количественного, так и качественного приращения элементов инновационной системы.

Также необходимо продолжить работу по развитию таких конкурентоспособных инновационных комплексов, которые могут дать наибольший эффект, в среднесрочной перспективе.

Технологической платформой для реализации комплексных инициатив могут выступать: научно-технический сектор, технопарки, вузы и др. субъекты инновационной инфраструктуры, имеющие необходимый для этого потенциал.

СПИСОК ЛИТЕРАТУРЫ

1. Вагапов, Р.Ф., Гузаиров, М.Б., Инновационный Башкортостан в РФ. Вагапов, М.Б. Гузаиров // Научно - популярный журнал - 2010. - № 3. [Электронный ресурс].Режим доступа: https://elibrary.ru/contents.asp?id=36902636. (дата обращения: 02.09.2021).
2. Вагапов, Р.Ф. Инновационный потенциал / Р.Ф. Вагапов, Е.А. Артемова. - Уфа: Издательство Министерство промышленности и инновационной политики РБ, 2007[Электронный ресурс]. Режим доступа:https://elibrary.ru/item.asp?id=44703477. (дата обращения: 03.09.2021)
3. Комплексный сборник Республика Башкортостан в цифрах. В 2-х ч. /.Башкортостанстат. - Уфа, 2010 [Электронный ресурс]. Режим доступа: https://bashstat.gks.ru/storage/mediabank/GHHcC2tr/komplexnyi-sbornik-2019.pdf. (дата обращения: 05.09.2021).
4. Министерство промышленности и инновационной политики Республики Башкортостан [Электронный ресурс]. Режим доступа:http://www.minpromrb.ru/. (дата обращения: 05.09.2021).
5. Министерство цифрового развития государственного управления Республики Башкортостан. [Электронный ресурс]. Режим доступа:https://it.bashkortostan.ru/presscenter/news/338137/. (дата обращения: 06.09.2021).

УДК 316.6

А. А. ИЛЬИНА
litra.anya1999@mail.ru
Науч. руководв. – канд. пед. наук, доц. А. Ю. ФАРРАХОВА

Уфимский государственный авиационный технический университет

САМООРГАНИЗАЦИЯ УЧЕБНОЙ ДЕЯТЕЛЬНОСТИ СТУДЕНТОВ

Аннотация. В статье анализируется понятие самоорганизации, рассмотрены отечественные исследования выделенной проблемы, выделены показатели самоорганизации. Представлены результаты определения уровня самоорганизации у студентов по опроснику самоорганизации деятельности (ОСД) Е. Ю. Мандриковой. Описаны мероприятия, направленные на улучшение самоорганизации. Материал в целом отображает актуальность проблемы самоорганизованностимолодежи в современном обществе.
***Ключевые слова*:** самоорганизация; студент; тайм-менеджмент.

Учителя часто пишут в ученический дневник лаконично: «дисциплина – 2» или «нарушает дисциплину». Слово дисциплина после школы слышится редко, однако правил, которые мы должны соблюдать, с возрастом становится больше, так как степень ответственности возрастает. В детстве за нас отвечают родители; потом мы отвечаем за свою учебную деятельность; оканчивая школу, отвечаем за свою жизнь и свой выбор; позже несем ответственность за других (за детей или коллег, в том случае, когда занимаем руководящую должность). Оказывается, та дисциплина, на которую мало обращается внимания в школе, формирует в человеке необходимый навык самоорганизации. Те, у кого этот навык сформирован, успешно контролируют свое поведение в школе, систематически выполняют домашнее задание, грамотно распределяют свое время.

Понятие самоорганизации можно выразить фразеологизмом: «держать себя в руках». Для того чтобы сформировать более точное определение, обратимся к словарям и исследователям.

Понятию «самоорганизация» тождественно понятие «синергетика» – «(от греч. synergos — совместно действующий) – термин нем. физика Германа Хакена (1971) для новой науки, имеющей принципиально междисциплинарный характер…самоорганизация представляется как эмерджентное (внезапно воз-

никающее) свойство системы… Одно из таких свойств –самоорганизация, которая проявляется в самосогласованности (когерентности) взаимодействия подсистем, что дает возможность говорить о возникновении упорядоченных структур (паттернов) или даже новой системы…чрезвычайно интересно рассмотреть процессы эволюции как процесс самоорганизации. Эволюцию можно рассматривать как неограниченную последовательность процессов самоорганизации»[8].

Примечательно, что термин «самоорганизация» отсутствует в толковых словарях Ожегова С.И., Даля В.И. Поэтому, чтобы сформировать понятие, обратимся к двум семантическим единицам «само» и «организация».

Часть слова «само» может употребляться в шести значениях. Нам подходят:

1) направленности чего-нибудь на себя, исхождения от себя или осуществления для себя;

2) обращенности к самому себе, в самого себя или направленности на самого себя;

3) совершения чего-н. без посторонней помощи; без постороннего участия[6].

Организация рассматривается нами во втором значении – организованность, планомерное, продуманное устройство, внутренняя дисциплина.

На основе рассматриваемых примеров определения самоорганизации, составляем термин самостоятельно: самоорганизация – личный процесс, обращенный и направленный человеком к самому себе, который возникает внезапно и проявляется в когерентности взаимодействия подсистем.

К структурным компонентам самоорганизации относят: мотив, стиль деятельности, самопознание. Мотив определяет направление деятельности. Стиль деятельности включает в себя те методы, который человек выберет для того чтобы организовать свою деятельность. Это может быть тайм-менеджмент, план, различные практики. Самопознание включает в себя учет эмоциональ-

ных, физических и личных особенностей для того чтобы успешно выстроить деятельность, и рефлексию для работы над ошибками или проживании успеха (хвалить себя не менее важно, чем уметь корректировать деятельность).

Необходимость навыка самоорганизации заметна во время обучения в высшем учебном заведении. Кроме организации режима своего дня, студенту приходится осваивать программу, значительная часть которой осваивается студентом самостоятельно. Например, для специальности: 38.05.01 – «Экономическая безопасность», общая трудоемкость дисциплины «математический анализ» во втором семестре составляет 180 часов. На самостоятельную работу студента, согласно программе дисциплины, отводится 81 час[11]. По философии из 72 часов дисциплины 36 отводится на самостоятельную[12].

Вообще, важно уметь распределять приоритеты и собственные в силы при планировании деятельности, так как в противном случае могут последовать неприятные явления в виде усталости, прокрастинации, разочарования и отсутствия желания продолжать работу.

Актуальность данного исследования возросла в период дистанционного обучения, когда у студентов и учеников появилось больше свободного времени, но не все смогли правильно его распределить и сохранить успешную успеваемость. В домашней атмосфере учиться гораздо сложнее, нежели в аудитории, находясь под непосредственным контролем преподавателя, в обществе заинтересованных студентов.

Понятие самоорганизация может рассматриваться в зависимости от показателей. Так, можно рассмотреть четыре [5] аспекта самоорганизации в зависимости от того, как проявляются качества самоорганизованного человека: личностный, деятельностный, интегрированный, технический.

Изучение себя – личностный аспект самоорганизации, где рассматривается механизм воли, эмоциональная устойчивость, интеллектуальное развитие. В рамках такого аспекта утверждается, что самоорганизация – следствие работы человека над своим характером.

В рамках деятельностного аспекта, рассматривается обучение как основная деятельность для формирования навыка самоорганизации. То есть, понимая самоорганизация как качество, которое формируется на практике, в процессе выполнения заданий, контроля, работы над ошибками.

В интегрированный аспект входят личностный и деятельностный, то есть, самоорганизация рассматривается как следствие приспособления определенного человека в некоторых условиях.

Технический аспект включает различные методики для совершенствования навыка самоорганизации. Они не зависят от обстоятельств и ситуации, в которой находится человек, а также от его личностных особенностей. Методики обобщены и подходят разным людям для работы в различных сферах. Например, тайм-менеджмент [13].

Для определения уровня самоорганизации существует множество методик. Например, опросник «самооценка организованности» Ильина Е.П. или «опросник самоорганизации деятельности» (ОСД)Мандриковой Е. Ю. Мы остановились на опроснике самоорганизованности, так как он есть в открытом доступе [7]. Он предназначен для диагностики сформированности навыков тактического планирования и стратегического целеполагания.

Опросник самоорганизации деятельности состоит из двадцати пяти утверждений, правдивость которых респонденту предлагается оценить по шкале от одного до семи, где единица обозначает полное несогласие, семерка – полное согласие, а четверка является серединой.

В нашем опросе участвовали пятьдесят человек. Для идентификации мы предложили два вопроса, ответы на которые содержат информацию о поле и занятости респондентов:

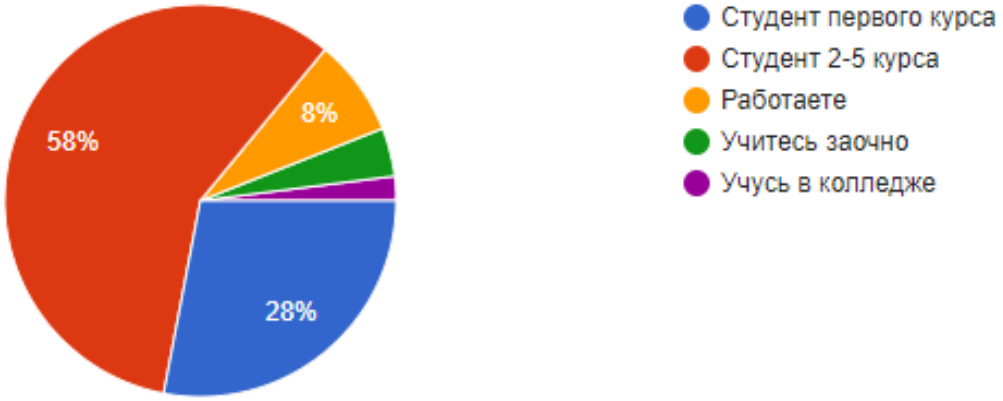


Рис. 1. Особенности выборки

Итогом опросника являются данные шести шкал, которые свидетельствуют о степени сформированности качества, необходимого для успешной самоорганизации [4]: планомерность, целеустремленность, настойчивость, фиксация, самоорганизация, ориентация на настоящее.

По итогам тестирования мы составили портрет студента, самоорганизация которого находится на среднем уровне (рис. 2.)

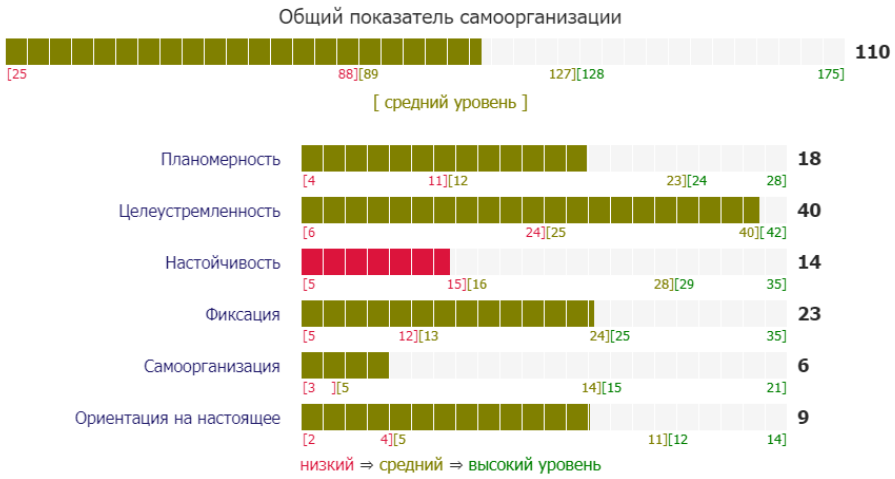


Рис. 2. Результаты исследования

Ни одна из шкал не демонстрирует высокого уровня сформированности качества. Близка к высокому уровню «целеустремленность», измеряющая способность концентрации на цели. Во время учебы в университете целей много: от выполненного домашнего задания до участия в научных конференциях, так

что сформированность навыка объяснима ритмом обучения. Низкий уровень у одной шкалы – шкалы настойчивости. Это свидетельствует об отсутствии приложения волевых усилий для завершения какого-либо дела. Причин для этого много: поступление в университет не собственному желанию; выбор профессии, которая не вызывает интереса; состояние здоровья; бытовая обстановка. Шкалы «планомерность», «фиксация» и «ориентированность на будущее» имеют средний уровень сформированности, что безусловно радует, так как подобный уровень является хорошей базой для совершенствования самоорганизации.

Портрет студента, исходя из полученных данных, можно интерпретировать, как способного сочетать структурированный подход к организации времени своей жизни со спонтанностью и гибкостью, умеющего ценить время и извлекать ценный опыт из многоплановости своей жизни.

Для того чтобы навык самоорганизации совершенствовался, а деятельность студента становилась плодотворнее, мы рекомендуем придерживаться нескольких правил:

1) Соблюдать режим дня. Это важно, так как от этого зависит состояние здоровья и настроение.

2) Заниматься спортом. Спорт помогает снять эмоциональное напряжение, может помочь сформировать новый круг общения, улучшает самочувствие и благотворно влияет на здоровье.

3) Читайте классическую литературуЧтение расширяет кругозор человека, обогащает его внутренний мир, делает умнее и положительно сказывается на памяти.

4) Планируйте свой день. Это лучше делать перед сном. Подумайте, что необходимо сделать в соответствии с расписанием и дедлайнами, распишите, представьте, сколько времени понадобиться, составьте план. Не забудьте оставить время для отдыха.

5) Ставьте цели. Вспомним якутскую пословицу: «Помыслы и стремления сильны, как текучая вода».

Соблюдение этих пяти правил значительно улучшит результаты деятельности студентов.

СПИСОК ЛИТЕРАТУРЫ

1. Баженова Н.Г. Исследование влияния курса обучения в вузе на психологические характеристики самоорганизации студентов, участвующих в общественных организациях // Психология, социология и педагогика. 2015. № 8 [Электронный ресурс]. URL: http://psychology.snauka.ru/2015/08/5657
2. Дьяков С. И. Самоорганизация в системе психологических критериев определения человека как субъекта жизни // Сибирский психологический журнал. - 2016. - №59.
3. Котова С.С. Психологические особенности самоорганизации учебной деятельности студентов // Научные исследования в образовании. - 2007. - №4.
4. МЕТОДИКА: Опросник самоорганизации деятельности(ОСД) (Мандрикова Е.Ю.) // cpd-program.ru URL: https://cpd-program.ru/methods/tsq.htm
5. НАТА КАРЛИН Самоорганизация личности // Sunmag. - 20 января 2014. - №https://sunmag.me/sovety/20-01-2014-samoorganizatsiya-lichnosti.html
6. Ожегов С. И. Толковый словарь русского языка [Текст] : 72500 слов и 7500 фразеологических выражений / С. И. Ожегов, Н. Ю. Шведова ; Российская АН, Ин-т рус. яз., Российский фонд культуры. - 2-е изд., испр. и доп. - Москва :Азъ, 1994. - 907, [1] с.;
7. Опросник самоорганизации деятельности (Е. Ю. Мандрикова) // https://studme.org/URL:https://studme.org/174463/pedagogika/oprosnik_samoorganizatsii_deyatelnosti_mandrikova
8. Психологический словарь / Под ред. В.П. Зинченко, Б. Г Мещерякова. - 2-е изд., перераб. и доп. - М.: Педагогика-Пресс, 1999. - 440 с., ил.
9. Самоорганизация студентов первого курса: Учеб. пособие / П. Е. Рыженков, Е. В. Марусова, Л. М. Хаславская и др.; Под ред. П. Е. Рыженкова. — Новосибирск: Изд-во Новосиб. ун-та, 1990. — 120 с.
10. Сунгурова Н.Л., Иващенко А.В., Карабущенко Н.Б. Особенности самоорганизациитдеятельности студентов с разными стратегиями сетевой коммуникации // Психология. Историко-критические обзоры и современные исследования. 2017. Т. 6. № 5А. С. 160-171.
11. Рабочая программа учебной дисциплины "Математический анализ" // https://lk.ugatu.su/lk/ URL: https://lk.ugatu.su/Curriculum/
12. Рабочая программа учебной дисциплины "Философия" // https://lk.ugatu.su/lk/ URL: https://lk.ugatu.su/Curriculum/
13. Тайм-менеджмент — 7 главных принципов по управлению временем + обзор книг, курсов и приложений, а также реальные примеры из жизни (мой опыт) // https://hiterbober.ru/ URL: https://hiterbober.ru/psychology-of-success/tajm-menedzhment-upravlenie-vremenem.html

УДК 338.47

Д. Е. КИРИЛЛОВА, Г. Р. МУЛАБАЕВА
kiriilliva.daria88@mail.ru, guzelkamullabaeva@mail.ru
Науч. руководв. – канд. экон. наук, доц. Ю. Т. МАНСУРОВА

Уфимский государственный авиационный технический университет

ВНЕДРЕНИЕ ИННОВАЦИЙ КАК СПОСОБ ПОВЫШЕНИЯ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ В ТРАНСПОРТНОЙ ОТРАСЛИ

Аннотация. В данной статье рассмотрены основные проблемы введения инноваций в транспортную отрасль. Описаны приоритетные инновационные обработки, способствующие повышению эффективности и оптимизации в данной отрасли.
Ключевые слова: транспорт; транспортная отрасль; инновации в сфере транспортной отрасли.

Важность и актуальность развития транспорта как составляющего элемента обеспечения экономической безопасности обусловливается ее особым значением в системе безопасности страны

Основной причиной введения инноваций в транспортную отрасль заключается в невысоком темпе доставки товаров и пассажиров, а также неудовлетворительное качество автотранспортного сервиса, которое обуславливается низкими промышленными возможностями транспортной отрасли.

С точки зрения экономической безопасности инновации в транспорте должны обеспечивать:

– рациональную организованность процесса оказания транспортных услуг;

– сохранность транспортируемых грузов;

– безопасный и бесперебойный процесс эксплуатации транспортно-технических и информационных средств.

Государство проявляет интерес в развитии транспортной отрасли. Например, в Транспортной стратегии Российской Федерации на период до 2030 года приоритетным стратегическим направлением является удовлетворение потребностей социально-ориентированного прогресса экономики и общества в качественных транспортных услугах, в качестве национального приоритета вы-

делено повышение качества жизни населения и конкурентоспособности национальной экономики.

В последнее время стали проявляться ограничения перспектив социально-экономического роста, обусловленные не удовлетворительным состоянием и недостаточным уровнем развития в транспортной отрасли. Например, средняя скорость доставки товаров в Российской Федерации составляет 300 км в сутки, а в таких странах как Китай, США, Германия – 1400 за сутки.

Если в России инвестиции в развитие транспортной отрасли уходит 2-2,2% от ВВП, то в странах с высокоразвитой инфраструктурой уходит около 3-4%, а в Китае – 6%.

Итак, Выделяют 4 вида транспорта: автомобильный, железнодорожный, речной и авиационный. Рассмотрим направления инновационного развития в каждом из них.

Самым активным видом транспорта считается автомобильный, особенно в крупных городах, что играем первостепенную роль в загрязнении атмосферы. Протяженность автомобильных дорог составляет около 871,5 тыс. км. По этим дорогам осуществляется перевозка около 50% всех грузов.

Основными направлениями инновационного развития автомобильного транспорта являются:

– внедрение экологически чистых автомобилей;

– развитие и внедрение интеллектуальной системы в автомобильный транспорт;

– введение платных дорог для уменьшения дорожных пробок.

Введение платных дорог позволит разгрузить основные транспортные узлы, сократить количество пробок в час пик, и самое главное – даст возможность понять водителю, что для него важнее – скорость или отсутствие платы за передвижение. Главными преимуществами также является хорошее освещение на всем участке, прямой кратчайший маршрут, экономия на расходе топлива, высококачественное дорожное покрытие. В настоящее время планируются плат-

ные дороги и в Башкортостане. Первой дорогой, за проезд по которой придется платить, станет «Восточный выезд». Объект планируется достроить к 2024 году.

Идет активное развития транспорта для перевозки грузов и пассажиров, что также считается одной из проблем мегаполисов. В сфере общественного транспорта для повышения уровня доступности транспортных средств населению предлагается интеллектуальный общественный транспорт. Благодаря этой системе пассажиры смогут с помощью интернета узнавать количество свободных мест, время прибытия и скорость движения ближайшего автобуса, маршрутного такси, поезда метро или пригородной электрички. А транспортные компании смогут узнавать об увеличении числа пассажиров на той или иной остановке, проводить мониторинг, что позволит своевременно направлять туда необходимые средства передвижения.

Железнодорожный транспорт считается не менее рентабельным. Основными преимуществами является высокий уровень грузоподъемности, средняя себестоимость и проходимость в различных погодных условиях. Протяженность отечественных железных дорог составляет приблизительно 86 тыс. км. Это позволяет России стоять на третьем месте в мировом рейтинге вслед за США и Китаем.

Направления инновационной деятельности будут являться:

– внедрение электронной кодовой автоблокировки;

– разработка системы координатного управления движением поездов на базе цифрового радиоканала и т.д.

Существует проект, носит название «Высокоскоростное железнодорожное сообщение». Финансирование проекта на участок Москва-Казань обходится стоимостью около 1,7 триллиона рублей [1].

Речной транспорт такжезанимает важное место в транспортной системе, так как речная трасса выгоднее по протяженности и огибает многие города, и, соответственно, себестоимость перевозок не высокая.Протяженность внутрен-

них водных путей составляет 102 ты. км., в мировом рейтинге занимает второе место после Китая.

Но из-за недостатка вложения инвестиций, производство кораблей и других видов речного транспорта имеют очень низкие обороты.

Сейчас российскими инженерами разработаны абсолютно новые высокоскоростные корабли, которые позволяют оптимально использовать топливо, при этом увеличивать крейсерскую скорость. Передвижение кораблей может осуществляться за счет образований на поверхности воздушных пузырьков, благодаря непрерывному потоку воздуха, или по-другому его называют суперкавитацией.

Также возобновились проекты по производству экранопланов, прекратившегося в начале 1990-х. Этот аппарат способен скользить над водой или земной поверхностью. Могут использоваться в качестве пассажирского, грузового, спасательного транспорта и т.д. Также в будущем времени планируется введение уже беспилотных ссуд.

Выделяют гражданскую и военную авиацию. Рассмотрим гражданскую. В России более 630 аэропортов, 532 тыс. км. воздушных трасс, в мировом рейтинге Россия занимает пятое место.

Основные направления инновационной деятельности в гражданской авиации:

– в первую очередь, это совершенствование системы управления авиацией, для более ускоренной координации полетов;

– разработка более мощных и многофункциональных типов воздушного транспорта, способных благополучно выходить из аварийных ситуаций и преодолевать длительные расстояния;

– повышение эффективности использования топлива, применение новейших технологий расходных материалов с рациональными вложениями финансов и с минимальным загрязнением окружающей среды.

Отличным примером внесения большого вклада в будущее российской авиации служат ученые Уфимского Государственного Авиационного Технического Университета. Они защитили проект по созданию электродвигателя для пилотируемых и беспилотных летательных аппаратов в правлении Фонда перспективных исследований. Данную разработку под руководством Флюра Исмагилова и Вячеслава Вавилова признали «прорывной технологией». Данная разработка первой получила финансирование Фонда в Республике Башкортостан.

На данный период времени, ученые УГАТУ участвуют в реализации масштабной государственной научно-исследовательской работы «Электролет СУ-2020», которая предполагает создание самолетов с гибридными силовыми установками (ГСУ), существенно сокращающими расход топлива и вредных выбросов.

Для воздушнойгрузоперевозки разрабатывается «Автономный (беспилотный) транспорт», который позволит обеспечить как экономическую безопасность, так и транспортную. Предназначен для перевозки грузов мелкими партиями, сокращенный период доставки. За счет высокого интеллекта робот самостоятельно планирует маршрут. Контроль системой будет осуществляться оператором.

СПИСОК ЛИТЕРАТУРЫ

1.https://ac.gov.ru/uploads/_Projects/PDF/KPMI/8._Паспорт_федерального_проекта_Высокоскоростное_железнодорожное_сообщение.PDF(дата обращения 08.09.2021).
2. https://anomtu.ru/proekty/zheleznodorozhnyy-transport/podprogramma-zheleznodorozhnyy-transport/ (дата обращения 08.09.2021).
3. http://synergy-journal.ru/archive/article3335 (дата обращения 08.09.2021).
4. https://e100.eu/ru/blog/strategiya/tekhnologicheskie-innovatsii-v-transportnoj-otrasli (дата обращения 08.09.2021).

УДК 33.338

Д. Р. ХАКИМОВА, М. М. ШАБАНОВА
Milina.shabanova2000@mail.ru
Науч. руководитель – канд. экон. наук, доц. П. А. ТУКТАРОВА

Уфимский государственный авиационный технический университет

ИННОВАЦИОННЫЕ МЕТОДЫ СОВЕРШЕНСТВОВАНИЯ СИСТЕМЫ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

Аннотация. В статье раскрыты основные проблемы экономической безопасности предприятия. Рассмотрены данные об инновационной активности предприятий. Предложены методы совершенствования системы экономической безопасности.
Ключевые слова: система экономической безопасности; экономическая безопасность предприятия; инновации.

Вероятные пути создания подходящего инновационного климата в российской экономике начали активно развиваться в начале 80-х годов прошлого века. В современных условиях предприятие функционирует в сложной, динамической внешней среде, выводя на первый план его количественные и качественные характеристики для выживания и обеспечения развития в нестабильных условиях, трудно прогнозируемых и непредсказуемых внешних и внутренних факторов. Проблема формирования состояния экономической безопасности предприятия находится в области научного исследования проблем инновационного развития.

Инновации помогают предприятию быть конкурентоспособным, защищают от многих рисков.

В современных условиях спрос на IT- специализации особенно велик.

Под воздействием современных изменений, тенденций и процессов как в технике, так и в экономике формируются новые потребности, которые не могут быть удовлетворены за счет имеющихся результатов деятельности людей.

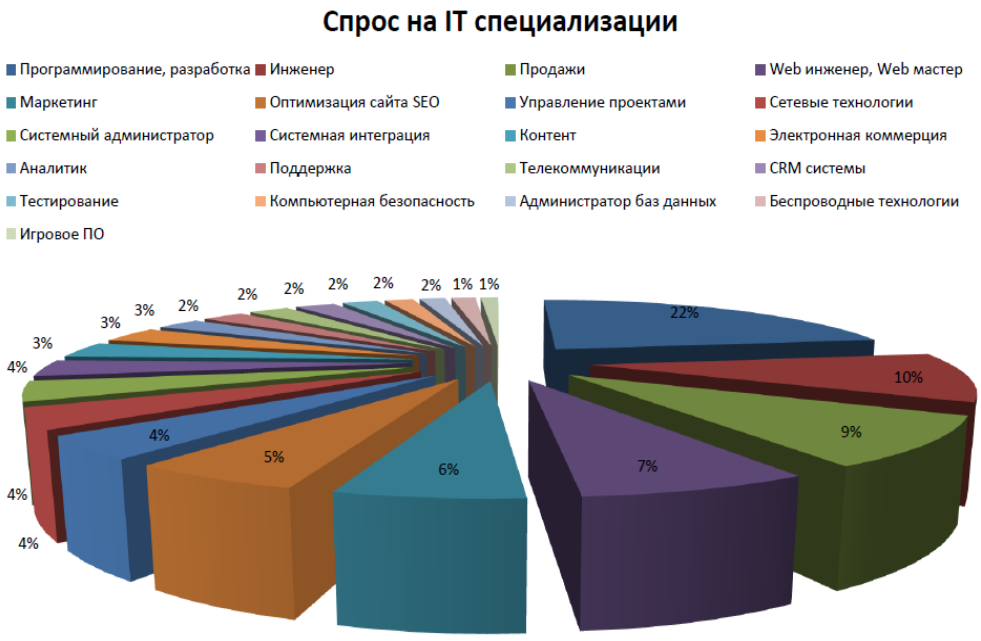


Рис. 1. Спрос на IT специализации

Процесс формирования и актуализации экономической безопасности предприятия зависит от степени инновационности экономики государства в целом и инновационности экономики предприятия частности.

Рассмотрим статистические данные за 2017-2019г.г. об инновационной активности предприятий.

Таблица 1

Статистические данные за 2017-2019г.г. о инновационной активности предприятий

	Код по ОКВЭД2 ОК 029-2014 (КДЕС Ред. 2)[2)]	2018	2019
Всего		12,8	9,1
из них по видам экономической деятельности:			
выращивание однолетних культур	01.1	4,0	4,8
выращивание многолетних культур	01.2	1,4	2,4
выращивание рассады	01.3	5,6	5,0
животноводство	01.4	4,2	4,0
смешанное сельское хозяйство	01.5	9,4	2,8
деятельность вспомогательная в области производства сельскохозяйственных культур и послеуборочной обработки сельхозпродукции	01.6	3,4	4,3

Окончание табл. 1

промышленное производство		15,6	15,1
из них:			
добыча полезных ископаемых	B	7,9	6,8
обрабатывающие производства	C	23,2	20,5
из них:			
производство пищевых продуктов	10	14,2	12,0
производство напитков	11	10,1	7,9
производство бумаги и бумажных изделий	17	20,3	14,7
деятельность в сфере телекоммуникаций	61	12,4	12,6
разработка компьютерного программного обеспечения, консультационные услуги в данной области и другие сопутствующие услуги	62	10,1	11,1
деятельность в области информационных технологий	63	5,0	5,5
деятельность в области права и бухгалтерского учета	69	2,8	1,9
деятельность головных офисов; консультирование по вопросам управления	70	4,0	3,6
деятельность в области архитектуры и инженерно-технического проектирования;	71	12,4	9,7

Экономическая безопасность призвана создать условия для эффективной деятельности предприятия и, в результате достижения целей бизнеса в условиях конкуренции и хозяйственного развития, путем своевременного выявления и ослабления действия различных опасностей и угроз.

Для осуществления предприятием инновационной деятельности, оно должно иметь такую структуру и такую систему, которые способствовали бы созданию благоприятных условий для предпринимательства, а также созданию атмосферы восприятия инновационных возможностей.

Для создания экономической безопасности необходимо оптимизировать ее систему. Система безопасности строится на основе средств и методов, которые помогают противодействовать угрозам, то есть, поддержать безопасное состояние предприятия.

Рассмотрим угрозы, которым можно противостоять с помощью инновационных методов.

Таблица 2

Методы предотвращения угроз экономической безопасности предприятия

Угроза	Метод
промышленно-экономический шпионаж	использование подавителей сигнала GPS, видеокамер, специальная техника для вычисления скрытого оборудования, работающих на предприятии, использование специальных средств защиты конфиденциальной информации, а именно средства шифрования и криптографии
хищения материальных средств	установление видеокамер, установление сигнализаций, сейфа с Face-ID, электронного сейфа
издержки производства	усиление маркетинговых коммуникаций (PR в интернете), модернизация и автоматизация производства, таргет-костинг, бенчмаркинг издержек
подрыв делового имиджа и репутации	управление социальными сетями, бренд-менеджмент, создание контента, стратегический охват, создание цифровых, поисковая оптимизация
низкая квалификация персонала	проверка квалификации через специальные компьютерные программы, повышение квалификации онлайн

Современные угрозы требуют инновационных мер их устранения.

Были выделены основные угрозы экономической безопасности предприятия, такие как:

1. Промышленно-экономический шпионаж, данную угрозу можно предотвратить с помощью средств шифрования и криптографии. Согласно законодательству ЕАЭС они предназначены для защиты информации от несанкционированного доступа при ее передаче по каналам связи и (или) при ее обработке и хранении.

2. Хищение материальных средств, здесь можно использовать инновационный сейф с использованием Face-ID. Открытие сейфа возможно после приложения пальца к дактилоскопическому сканеру или благополучного прохождения пользователем Face-ID-идентификации.

3. Издержки производства, к данной угрозе мы предложили такие методы как таргет-костинг и бенчмаркинг издержек.

4. Подрыв делового имиджа и репутации, данную угрозу можно решить с помощью поисковой оптимизации. Поисковая оптимизация – это комплекс мер по внутренней и внешней оптимизации для поднятия позиций сайта в результатах выдачи поисковых систем по определенным запросам пользователей, с целью увеличения сетевого трафика и потенциальных клиентов и последующей монетизации (получение дохода) этого трафика.

5. Низкая квалификация персонала, к данной угрозе мы предложили проверку квалификации через специальные компьютерные программы и повышение квалификации онлайн.

Таким образом, можно сделать вывод о том, что для нормального функционирования предприятия и для поддержания его экономической безопасности необходимо применение инновационных методов, которые направлены на создание и материализацию нововведений на предприятии, реализацию таких инициатив, которые вызывают качественные изменения в его работе, приводят к рациональному использованию материальных и других ресурсов.

СПИСОК ЛИТЕРАТУРЫ:

1. Андрейчиков, А. В. Стратегический менеджмент в инновационных организациях : системный анализ и принятие решений / А. В. Андрейчиков, О. Н. Андрейчикова. – М. : Вуз. учебник : ИНФРА-М, 2013. – 394 с.
2. Бланк И.А. Управление финансовой безопасностью предприятия / И.А. Бланк. – Киев: Эльга, 2013. –776 с.
3. Кормишкина, Л.А. Экономическая безопасность орг.(предп.): Учебное пособие / Л.А. Кормишкина, Е.Д. Кормишкин, И.Е.Илякова. – М.: Риор, 2012.– 208 с.
4. Разработка и принятие решения в управлении инновациями / И. Л. Туккель. – СПб. : БХВ-Петербург, 2011. – 342 с.

УДК 33.338

Р. М. ХАКИМОВА, М. В. ХОДАЕВА
hakimova.regina2014@yandex.ru, hodaeva.maria@gmail.com
Науч. руководит. – ст. преп. И. В. ДМИТРИЕВА

Уфимский государственный авиационный технический университет

ПРИМЕНЕНИЕ ИННОВАЦИОННЫХ ТЕХНОЛОГИЙ В СИСТЕМЕ ВЫСШЕГО ОБРАЗОВАНИЯ

Аннотация. В статье рассматривается влияние пандемии на развитие инноваций в сфере высшего образования. Определены положительные и отрицательные стороны внедрения инновационных технологий в систему высшего образования.
***Ключевые слова*:** инновационные технологии; искусственный интеллект; высшее образование.

Сложившаяся ситуация в 2020 году – глобальное распространение коронавирусной инфекции, заставила все сферы общества экстренно перейти на дистанционную форму работы. В частности, это коснулось высшего образования. Тема дистанционного обучения конечно же рассматривалась как одна из перспектив развития образования, но настолько резкий переход к данной форме сразу же сказался на качестве услуг обучения студентов. Выявились проблемы в отсутствии методик введения практик и лекций через экраны ноутбуков, качественная проверка выполненных заданий студентов тоже оказалась под вопросом, также пострадали взаимоотношения между участниками образовательного процесса в качестве «преподаватель – студент». Введение дополнительных способов и методов обучения, основанных на технологических новинках, позволило более грамотно и рационально организовать процесс обучения. В связи со сложившийся обстановкой в мире, рассматриваемая тема инноваций в сфере высшего образования будет актуальна.

Одним из этапом инноваций в сфере высшего образования является использование онлайн-платформ. Организация лекций и практик на таких сервисах как Zoom, GoogleMeet, Webex, Skype и многих других. Но при первых месяцах работы возникали проблемы как у преподавателей, так и у самих сервисов. Серверы онлайн-платформ просто были не рассчитаны на такой огромный

поток пользователей, поэтому первое время происходили «зависания систем», «вылеты из конференций». Также вузы не имели собственные программные обеспечения, которые бы позволяли заниматься со студентами из дома.

Резкий переход проведения занятий дистанционно отразились на преподавателях. Так, согласно исследованию НИУ ВШЭ, одними из ключевых проблем, с которыми сталкивались преподаватели были (рис. 1):

– сложность к присоединению всех студентов к конференциям;

– прерывания и перебои во время проведения конференций;

– низкая скорость интернет-соединения[1].

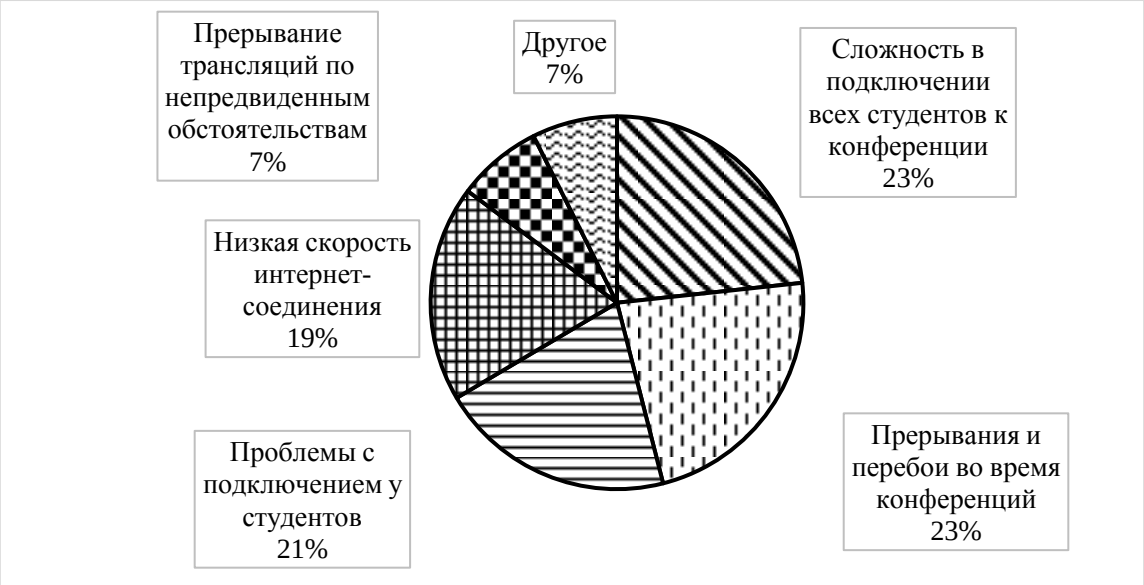


Рис. 1. Результаты исследования среди преподавателей

Также не все преподаватели были оснащены методическими и техническими средствами для реализации процесса обучения вне вуза.

В исследовании приведена статистика ответов, касающихся нагрузки преподавателей вовремя проведение онлайн-лекций и практик. Согласно опросу, увеличение нагрузки отметили больше 80% преподавателей. Такие результаты опроса связаны в первую очередь с тем, что им пришлось быстро осваивать новые форматы обучения, к парам теперь нужно готовиться по-другому, нарушились первичные практики проведения лекций и практик.

Что касается студентов, то большинство из них, а именно 59%, согласно исследованию НИУ ВШЭ, оценивают нагрузку от обучения в период пандемии как увеличившеюся (рис. 2).

Рис. 2. Диаграмма ответов студентов касательно нагрузки обучения период пандемии

В связи с этим, многие компании использовали период пандемии и переход на дистанционную деятельность как способ проявить себя и получить выгоду.

В области высшего образования различными организациями и компаниями были предложены следующие инновации.

Коллаборативные инструменты – они позволяют поддерживать онлайн-обучение с помощью чат-ботов: платформ и приложений, способствующих взаимодействию между равноправными участниками; а также групп, блогов.

Также одной из инновационных систем в высшем образовании является созданное компанией DogheadSimulations программное обеспечение виртуальной реальности rumii, которое работает с гарнитурами Oculus Go VR [2]. Такие технологии позволяют виртуально перемещаться студентам в любые точки мира, для более подробного изучения. Исследования Университета штата Пенсильвании показали, что студенты, у которых в процессе обучения была задействована данная программа, выполняли задачи в два раза быстрее, чем студенты, которые использовали обычные компьютерные программы.

Recorder Pen – ручка, которая превращает рукописный текст в печатный.

В университете студенты большую часть информации пишут от руки карандашами и шариковыми ручками. Но при этом все более заметная часть домашних заданий выполняется на компьютере. Для того, чтобы объединить эти

два мира, и создана электронная ручка Recorder Pen, превращающая рукописный текст в печатный.

Искусственный интеллект внедрили в сферу высшего образования, который облегчил работу как преподавателям, так и студентам. Теперь вместо того, чтобы сидеть за проверкой кучи домашнего задания и контрольных работ, преподаватель может отдать всю работу ИИ и проверять лишь правильность оценки.

Так же появилось новое приложение «Study Blue» для смартфонов, которое помогает во время обучения. Файлы хранятся в удобном формате и можно с легкостью разобраться в домашнем задании и конспектах, что помогает студенту быть более организованным. Преподавателям удобно отслеживать статистику посещений, в которой отображаются имена, продолжительность работы и прогресс студентов в процентах [3].

Система высшего образования и ее подача студентам давно должна была поддаться инновациям, и пандемия как раз заставит задуматься о возможных изменениях и улучшениях в этой области. Инновационные технологии в сфере высшего образования оказывают как положительное, так и отрицательное влияние на процесс обучения.

Плюсы:

– онлайн-обучение позволило студентам из разных уголков учиться в комфортной и одинаковой среде из любой точки мира;

– преподаватели избавились от той горы отчетов и справок, что позволяет им больше преподавать и саморазвиваться.

– разные инновационные технологии дают огромный простор для нестандартных форматов и подходов в обучении.

– с помощью алгоритмов и чат-боттов можно автоматизировать и обеспечить более организованный процесс обучения.

Минусы:

– дистанционное обучение оказалось большим стрессом как для студентов, так и для их родителей;

– невозможность преподавателей обратить внимание на каждого студента и проследить за их усвоением материала;

– при нахождении дома студенту трудно сосредоточиться на учебе и во-время онлайн уроков идет постоянное отвлечение на какой-либо гаджет;

– у преподавателей отсутствовала база для такого формата обучения и им приходится на ходу осваивать новые программы и технологии;

– главная проблема в том, что не у всех студентов есть хороший компью-тер и быстрый интернет так нужный для такого формата обучения.

На наш взгляд, инновационные технологии в сфере высшего образования принесли по большей части пользу для студентов и преподавателей. Сокраще-ние бумажных работ, часов в ожидании лекций и пар, очередей в университете, огромных трат времени на дорогу и питание, все это позволяет студентам быть более мобильными, развиваться в параллельных сферах, поддерживать баланс труда и отдыха.

СПИСОК ЛИТЕРАТУРЫ

1. Барышев Р.А. Активная информационная система вуза в информационно-образовательной среде // Педагогика: журнал. 2017. №3. С. 28-33.
2. Жулин А.Б. Аналитический бюллетень НИУ ВШЭ об экономических и социальных по-следствиях коронавируса в России и мире // Высшая школа экономики. 2020. № 2.
3. Садырин, В.В. Сетевое взаимодействие педагогических вузов: механизмы формирования и развития / В.В. Садырин, М.В. Потапова, Д.В. Татьянченко // Педагогическое образование и наука: журнал.. 2017. №1. С. 19-25.

УДК 338.46

Т. И. ЧАПЛИНА
Gfhbubkcob@mail.ru
Науч. руководит. – канд. экон. наук, доц. Ю. Т. МАНСУРОВА

Уфимский государственный авиационный технический университет

ВЛИЯНИЕ ИННОВАЦИЙ НА СФЕРУ ЗДРАВООХРАНЕНИЯ

Аннотация. Данная статья посвящена изучению инноваций управления персоналом в сфере здравоохранения, анализу уже существующих инноваций, актуальности и описанию проблем, предложений по методам их решения. Будут представлены анализ и статистика в 2020 – 2021 годах.
Ключевые слова: здравоохранение; управление; персонал.

Актуальность проблемы заключается в том, что инновации это такие нововведения, которые необходимы для прогресса в любой сфере. Сейчас в 2021 году инновации управления персоналом как никогда, кстати, так как во время пандемии сфера здравоохранения несет огромную ответственность за жизни людей. Для того чтобы специалисты сферы здравоохранения выполняли качественно и оперативно свою работу, нужно чтобы медицинским персоналом грамотно управляли, позволяли расти как специалистам, так и старались делать все для эффективной работы.

Инновации управления персоналом являются необходимым условием для отлаженной работы сферы здравоохранения. Они могут быть определены как «те изменения, которые помогают медицинским работникам уделять больше внимания пациентам в результате повышения эффективности работы всех специалистов системы здравоохранения».

В 2020 году случилась пандемия COVID – 19, которая нанесла удар на всю сферу здравоохранения, поэтому сейчас, в период пандемии инновации важны еще больше, потому что работники здравоохранения нуждаются в четком управлении, чтобы не возникал хаос, забастовки и массовые увольнения.

Основная проблема, актуальность, которой очень важна это – медицинский персонал. Именно они попали под удар в первую очередь, и именно они нуждаются в инновациях.

Рассмотрим в таблице 1 проблемы медицинского персонала и методы их решения.

Таблица 1

Проблемы и методы их решения

Проблемы	Инновации	Последствия введения инноваций
Защита медицинского персонала	Создали многоразовые противоэпидемические костюмы, которые помогают защитить от возможного заражения опасными инфекциями, в данном случае COVID – 19.	Начальство пытается уберечь своих сотрудников, так как медицинский персонал всегда был на вес золото, а что касается мед. работников, которые действительно могут выполнять свою работу качественно, то их найти еще тяжелее.
Ненормированный рабочий день и сверхурочный труд	Мы предлагаем ввести карточки, которые будут отслеживать за переработкой сотрудников и не позволять им этого делать.	Мы считаем, что это позволит избежать усталости, потери концентрации, а самое главное ошибок, которые могут повести за собой непоправимый вред.

Хороший пример инноваций в сфере управления персоналом это разработка тренинга командообразования, целью которого является развитие позитивного отношения в коллективе и развитие чувства уверенности в себе и членах команды.

Основные инновации управления персоналом в сфере здравоохранения:

1. Проведение сотрудниками консультации в режиме онлайн;
2. Составление сотрудниками электронных карточек пациентов;
3. Компьютеризация всех рабочих мест сотрудников;

Внедрение инноваций в государственных учреждениях происходит под четким контролем государства, так как оно финансирует данный процесс. В частных же клиниках этим обычно занимаются инвесторы.Оценка инноваций в сфере здравоохранения должна быть направлена на выявление преимуществ новых методик, превосходящих существующие аналоги.

Круг проблем, которые являются сдерживающими факторами для развития и продвижения инноваций это:

1) отсутствие целевого финансирования инноваций и инновационных инициатив в рамках функциональных систем, обеспечивающих развитие и продвижение инноваций - медицинских инновационных кластеров и, что особо актуально - отсутствие «заказчика» на инновационный продукт.

2) низкая развитость инфраструктуры, которая бы выводила научные разработки в область практического здравоохранения.

Среди подготовленных на настоящий момент баз для введения инноваций, отмечены клиники университетов, НИИ и клиники федерального уровня.Плохо оценены для ввода инноваций негосударственные медицинские организации, клиники регионального уровня и областного уровня.

В заключении хотелось бы сказать о том, что инновации управления персоналом в сфере здравоохранения очень важны, так как в сложившейся ситуации, связанной с пандемиейCOVID – 19 сфера здравоохранения остается на первом месте и персонал этой сферы должен функционировать в полную силу.

СПИСОК ЛИТЕРАТУРЫ

1. Емельянов Ю.С. Формирование кластеров в сфере науки и инноваций // Эконом, науки. 2011. № 8 (81);
2. Стародубов В.И., Сон И.М., Леонов С. А., Стерликов С.А. Оценка эффективности деятельности региональных систем здравоохранения // Менеджер здравоохранения. 2010;
3. Беляков В.К., Пивень Д.В., Антонов Д.П. О проблемах инновационной политики в отечественном здравоохранении и необходимости создания кластеров медицинских инноваций // Менеджер здравоохранения. 2010.

УДК 338.28

А. В. ЧЕХ, Д. Л. ДЖАЛИЛОВ
xxx_frost@bk.ru /d.dzhalilov15@mail.ru
Науч. руководитель–канд. экон. наук, доц. Ю. Т. МАНСУРОВА

Уфимский государственный авиационный технический университет

ИННОВАЦИИ В СФЕРЕ ОБРАЗОВАНИЯ

Аннотация. Данная статья посвящена инновация в сфере образования, анализу уровня и качества инновационного развития данной сферы в стране. В ходе работы были выявлена проблема того, что многие образовательные учреждения были не готовы к дистанционном обучению, рассмотрены некоторые из новых тенденций, которые лягут в основу образования в 2021 году. Выявлены основные проблемы инновационной составляющей в образовательной отрасли страны, а также предложены пути решения данных проблем.
***Ключевые слова*:** инновационные технологии в образовании; учебное учреждение; дистанционное обучение; учителя; ученики.

Образование является неотъемлемой частью общества, отражает все процессы, которые происходят в нем. Интеллектуальные и духовные ресурсы созданные в образовательных учреждения играют важную роль в развитии как самого общества, так и во всех отраслях, где люди принимают участие в разных родах деятельности. Поэтому реформы, происходящие в обществе, всегда вызывают нововведения в образовании.

Инновационные технологии в образовании – это образовательный процесс построенный на качественно иных принципах, средствах, методах и технологиях и позволяющих достигнуть образовательных эффектов, характеризуемых:

Усвоением максимального объема знаний;

Максимальной творческой активностью;

Широким спектром практических навыков и умений.

Цель инновационных технологий в образовании – это формирование активного и творческого будущего специалиста, который способен самостоятельно строить свою познавательную деятельность.

2020 год привнес глобальные изменения в систему образования многих стран мира, несопоставимые ни с каким другим годом. COVID-19 создал мно-

жество проблем, но также открыл новые возможности для инноваций в секторе образования.

Положительным фактором является то, что мы, как отрасль, не придерживались «догм прошлого». За место этого весь сектор образования сплотился, принял общие решения и начал действовать с новой отправной точки. Руководители школ, преподаватели в университетах и учителя в равной степени стали приспосабливаться к новой действительности.

Инновационные подходы и решения дистанционного обучения были придуманы и реализованы как никогда раньше. Практики, которые ранее казались неосуществимыми, теперь получили путевку в жизнь благодаря слаженным действиям преподавателей, которые воспользовались возможностью отыскать новые методы сделать обучение легким, простым, доступным и также сумели сохранить мотивацию и интерес детей и их родителей в течение всего года.

Вспоминая прошедший год, настало время сконцентрироваться на тенденциях, которые будут определять будущее образования. Эта пандемия дала этому сектору великолепную возможность весьма быстро опробовать изменения, на внедрение которых потребовалось бы намного больше времени. Рассмотрим некоторые из новых тенденций, которые лягут в основу образования в 2021 году.

Образовательные технологии Цифровые платформы очень сыграли на руку , когда из-за пандемии COVID-19 школы и университеты перешли на дистанционное обучение.

Использование цифровых платформ и обучения с использованием видео сделало онлайн-обучение увлекательным для учащихся, столкнувшихся с трудностями, и это скорее всего будет актуально на протяжении 2021 года.

Индивидуальное обучение. Благодаря дистанционному обучению большое количество студентов теперь стали обучаться индивидуально. Это позволяет преподавателям персонализировать обучение отталкиваясь от потребностей студента.

Мы считаем, что индивидуальное обучение наиболее подходящее для развития в дальнейшей перспективе, потому что при данном виде обучения у преподавателя есть возможность найти к каждому ученику свой подход.

Гибридное обучение. Поскольку многие страны решают открывать школы поэтапно, также и Россия пользуется возможностью гибридного обучения. Гибридное обучение кажется самым лучшим вариантом обучения из всех на данный момент возможных, который выберет как школы и университеты России ,так и большинство школ и других учебных заведений по всему миру.

Данный вид обучения дает возможность найти баланс между дистанционным обучением и всем привыкшим к обучению в классе, что делает его наиболее интересным и инновационным. Эта набирающая рост тенденция в образовании, похоже, идет в ногу с меняющейся ситуацией во всем мире.

На наш взгляд, гибридное обучение не особо будет практиковаться в дальнейшем, потому что как для школьников, так и для студентов возможна трудность получения к удаленному доступу, чтобы провести занятие на дому. Также подобное обучение может отнимать намного больше времени и сил, потому что ученику придется ехать домой либо в образовательное учреждение.

Проектное обучение. Школы, которые ценят и продвигают обучение на основе проектов (PBL), более широкое использование инструментов Edtech из-за удаленного обучения предоставило обучающимся школьникам и студентам платформу для совместных работ над проектами в группах. Это дало возможность каждому студенту и школьнику шанс быть на связи друг с другом, а также очень облегчило преподавателям выполнение учебной программы.

Хоть и в 2021 году школы будут открываться для посещения данный тип обучения будет хорошо приспособлен в будущем для того, чтобы школьники, а также студенты могли иметь быстрый доступ к изучаемому материалу, а также возможность совместно изучать его и создавать разные проекты основываясь на полученных знаниях не выходя из системы.

С нашей точки зрения, проектное обучение очень хорошо подойдет для выполнения разных заданий как совместных, так и индивидуальных. Также подобный вид дает открытый доступ к образовательным источникам, чтобы ученики могли изучать материал в индивидуальном порядке. Если мы будет рассматривать такой тип обучения для развития в дальнейшей перспективе, то он будет не так хорош, как индивидуальное обучение, но также может активно использоваться в различных учебных учреждениях.

Повышение квалификации учителей. Пандемия привел к тому, что преподаватели были вынуждены изучать новые способы обучения школьников и студентов, а также использовать инновационные технологии по-максимуму. Для каждого преподавателя данный период был очень сложен, потому что никто из них никогда не практиковал подобные тип обучения.

Лаборатория медиакоммуникаций в образовании НИУ «Высшая школа экономики» при поддержке Общероссийского профсоюза образования и других организаций провела опрос «Проблемы перехода на дистанционное обучение в РФ глазами учителей». Были опрошены 22 600 учителей из 73 регионов страны. Ниже представлена статистика демонстрирующая низкие технологические возможности для обучения:

Рис. 1. Оснащение техническими устройствами средних образовательных учреждений

Рис. 2. Основные проблемы, с которыми сталкивается учителя и дети на дистанционном обучении

Самый главный вывод, которые большинство школ сделали это то, что дистанционное обучение — это гораздо более сложный процесс, чем передача информации онлайн. Кроме того, стало понятным, что такое обучение невозможно без IT-инфраструктуры и обеспеченности компьютерами и гаджетами большей части учеников, а также без квалифицированных учителей.

В ходе проведенных исследований аналитическим агентством RAEX была сформирована следующая статистика:

Рис. 3. Преимущества и недостатки дистанционной формы обучения

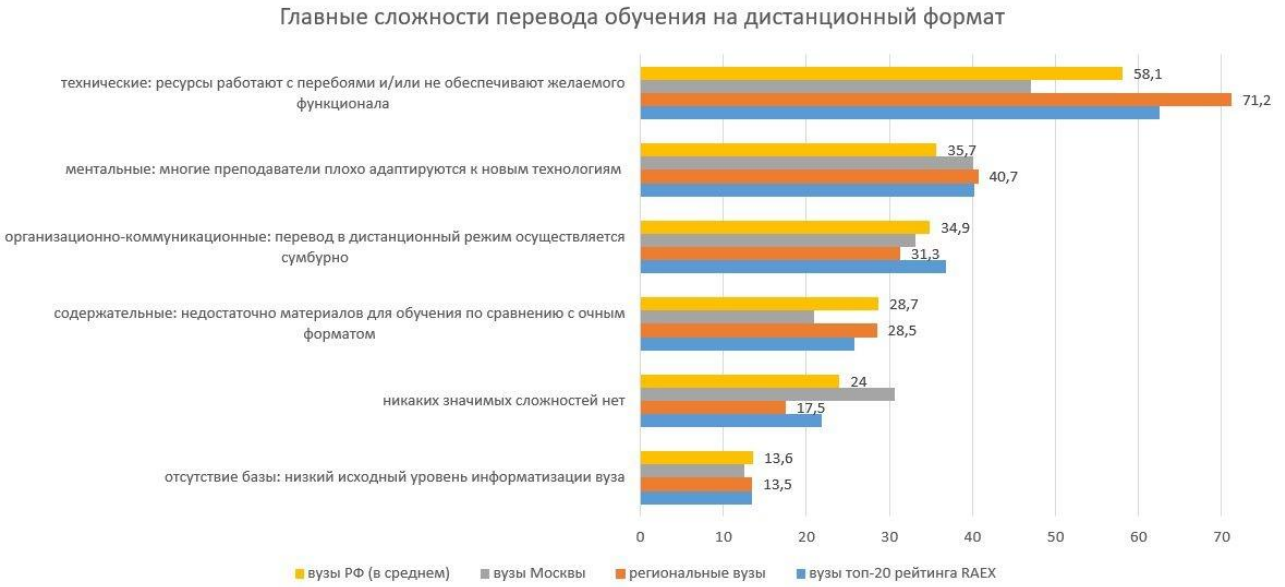


Рис. 4. Главные сложности перевода обучения на дистанционный формат

Рис. 5. Какие дистанционные возможности доступны студентам

Главный недостаток дистанционного обучения — дефицит общения: 70,2% студентов заявили, что им не хватает очного общения с сокурсниками и преподавателями. 36,9% молодых людей признались в том, что им трудно организовать свою работу. А 33,8% отметили такой недостаток, как урезанный формат обучения, при котором нет лабораторных работ и практикумов.

Более половины студентов считают главным преимуществом дистанционной формы обучения возможность планировать свое время и больше успевать: с таким выводом согласны более половины опрошенных .

Из выше представленной информации можно сделать вывод, что каждый преподаватель был вынужден проявлять свои творческие решения в данной ситуации на ходу, чтобы обучение никогда не стояло на паузе, а шло, как и до этого. Каждый преподаватель проделал огромную работу не смотря на возникающие трудности с дистанционным обучением. Необходимо поддерживать и продолжать развивать такой формат обучения, потому что ситуация с вирусом в мире нестабильная и никто не может знать, что может произойти через день или год. Поэтому нужно постоянно развивать данный тип обучения, хоть и не со студентами, но хотя бы давать опыт преподавателям в работе с дистанционным форматом, чтобы те в свою очередь имели возможность давать знания ученикам без каких- либо трудностей.

СПИСОК ЛИТЕРАТУРЫ

1. Сектор образования в 2021 году https://skyteach.ru/2021/03/08/5-veshhej-kotoryx-stoit-ozhidat-ot-sektora-obrazovaniya-v-2021-godu/. (дата обращения: 22.03.2021).
2. Инновационные технологии в образовании https://nsportal.ru/shkola/materialy-metodicheskikh-obedinenii/library/2020/11/30/doklad-innovatsionnye-tehnologii-v (дата обращения: 22.03.2021).
3. Инновации в сфере образования https://infourok.ru/user/dergachyov-dmitriy-vyacheslavovich/blog/innovacii-2020-kak-vyzhat-maksimum-iz-obrazovatelnyh-tehnologij-203042.html (дата обращения: 22.03.2021).

СЕКЦИЯ 5.10
МОДЕЛИРОВАНИЕ И ИССЛЕДОВАНИЕ ОПЕРАЦИЙ В ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКИХ СИСТЕМАХ

УДК 629.735.33.015.017.2

Р. Б. БАДРЕТДИНОВА, Э. Г. ГАБИДУЛЛИНА, Р. Р. КАРИМОВ
regi.badretdinova@yandex.ru, gabidullinaeliza@yandex.ru
Науч. руководо. – канд. техн. наук, доц. Р. Р. КАРИМОВ

Уфимский государственный авиационный технический университет

ИНФОРМАЦИОННАЯ ПОДДЕРЖКА ПРОЦЕССА ПРОВЕДЕНИЯ ЛЕТНЫХ ИСПЫТАНИЙ ВОЗДУШНОГО СУДНА ПО ОПРЕДЕЛЕНИЮ ХАРАКТЕРИСТИК ЗВУКОВОГО УДАРА

Аннотация. Рассматривается задача экспресс-обработки экспериментальных данных по определению характеристик звукового удара.
Ключевые слова: воздушное судно (ВС), сверхзвуковой пассажирский самолет, шум ВС на местности, звуковой удар, измерительные микрофоны.

Актуальность

Летные испытания по определению характеристик шума воздушного судна (ВС) на местности – важная составляющая комплекса мер по снижению шума в источнике и исследования эксплуатационных приемов снижения шума.

Сверхзвуковые самолеты создают в воздухе ударные волны, которые, достигая земли, приводят к возникновению звукового удара. Звуковой удар сопровождает самолет на всем пути его сверхзвукового полета. Размеры зоны воздействия звукового удара определяется режимом полета самолета и существенно зависят от атмосферных условий. Задача определения характеристик сверхзвуковых самолетов по звуковому удару заключается с одной стороны в измерении профиля волны давления в условиях, когда сведено к минимуму влияние различных случайных факторов, а с другой - в измерении всего комплекса параметров, характеризующих условия возникновения и распространения звукового удара. Такой подход к определению характеристик звукового удара необходим при создании сверхзвуковых пассажирских самолетов.

Сложность проблемы обусловлена тем, что для существующих сверхзвуковых самолетов характеристики звукового удара приближаются к верхней гра-

нице предельно допустимых значений. Отсюда видно, что решение проблемы звукового удара требует определения характеристик звукового удара с высокой точностью в условиях, имеющих место при эксплуатации сверхзвуковых самолетов.

Постановка задачи

Целью работы является повышение эффективности системы экспресс-обработки экспериментальных данных по определению характеристик звукового удара.

Для достижения поставленной цели необходимо решить следующие задачи:

1) Разработка функциональной модели процесса летных испытаний по определению характеристик звукового удара пассажирских самолетов.

2) Разработка программного модуля экспресс-анализа экспериментальных данных.

Системные модели процесса

Функциональная модель процесса, разработанная на основе технологии IDEF0, представлена на рисунке 1.

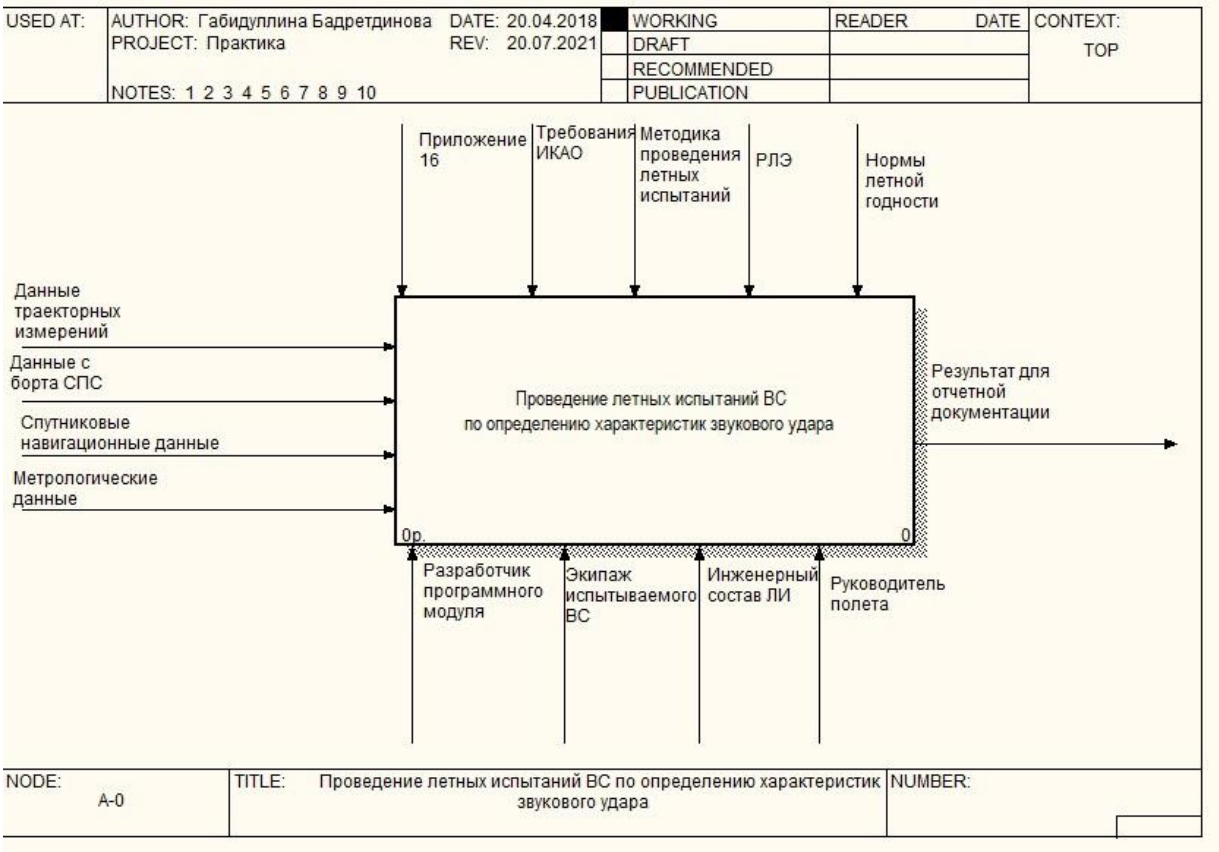


Рис. 1. Нулевой уровень функциональной модели

В ходе декомпозиции получаем три блока, которые в полном объеме характеризуют деятельность системы на всех этапах ее функционирования – это подготовка к летным испытаниям, проведение летных испытаний и обработка и анализ данных (рисунок 2).

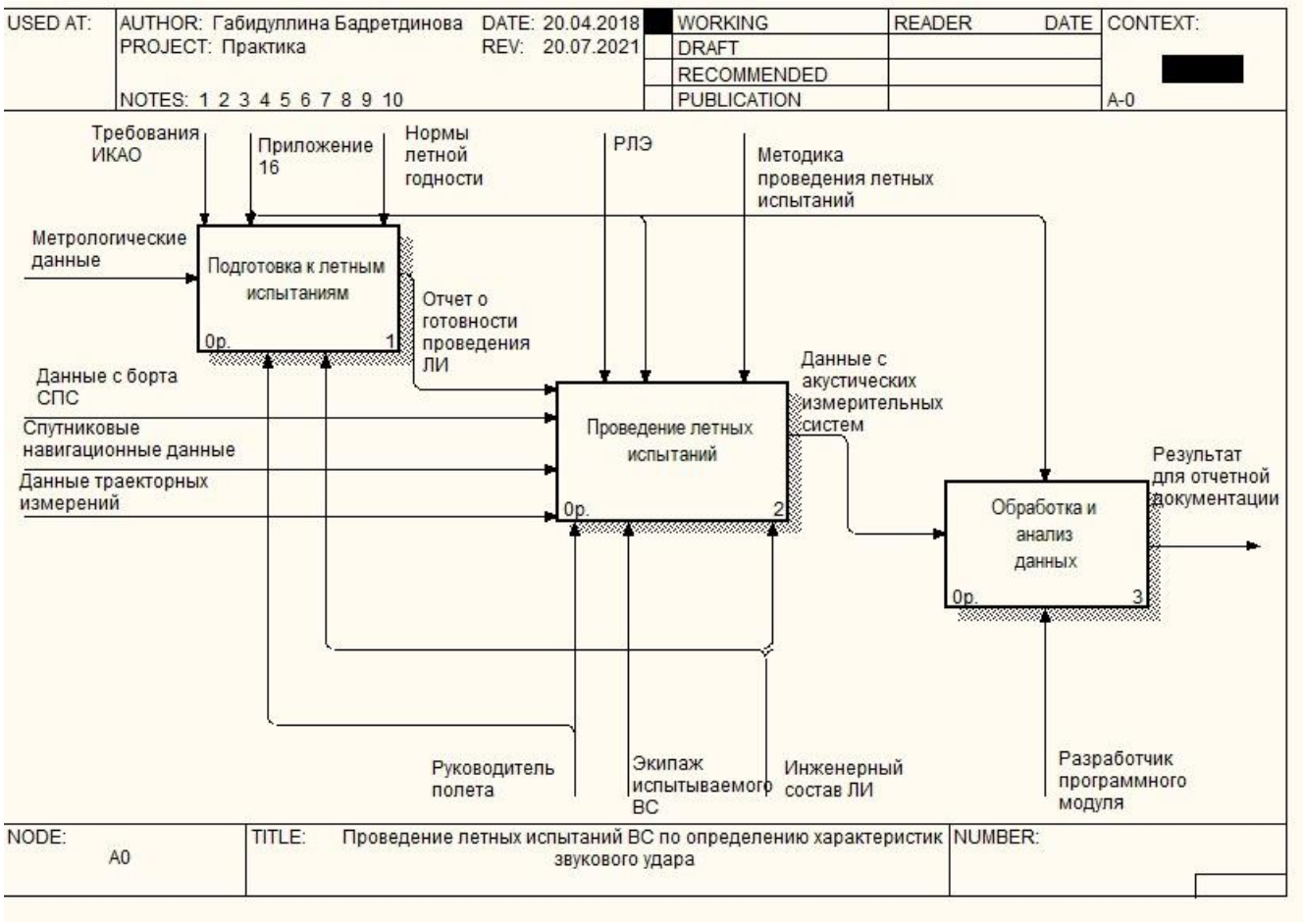


Рис. 2. Декомпозиция первого уровня функциональной модели

На рисунке 3 представлена декомпозиция блока «Обработка и анализ данных». Для предварительной обработки измерений используются данные с акустических измерительных систем, полученные после сбора данных летных испытаний. Проводится синхронизация данных. Полученный массив данных проходит автоматическую калибровку. Начинается процесс цифровой обработки откалиброванных данных, после которого формируется допуск ВС. Данный процесс производится с участием разработчика программного модуля.

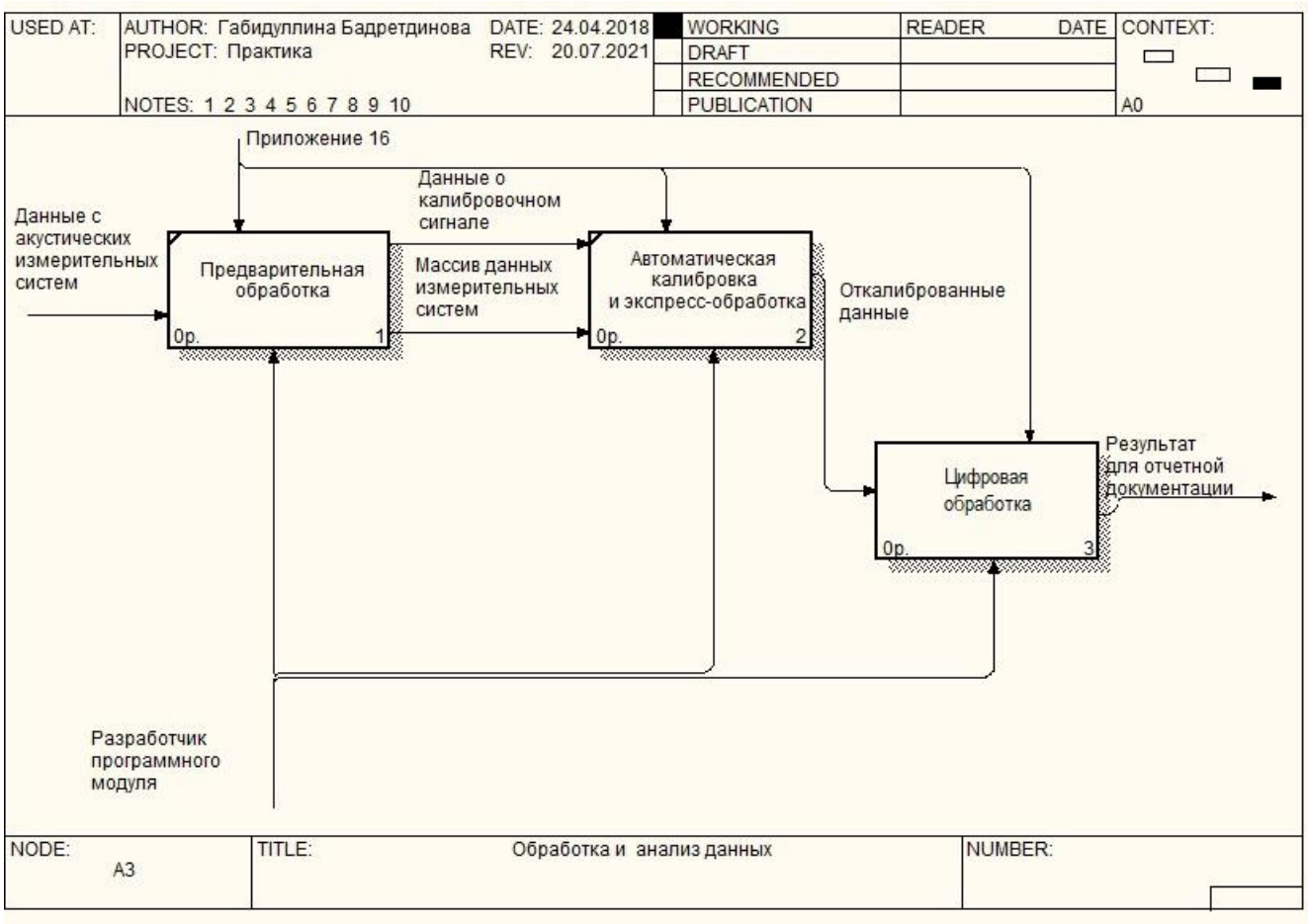


Рис. 3. Декомпозиция блока «Обработка и анализ данных»

Программная реализация процесса

Реализация процесса выполнена в виде программного модуля в MatLab. MATLAB – язык программирования высокого уровня и интерактивная среда для численных расчетов, визуализации и программирования. MATLAB широко используется во многих технических областях для анализа данных, экспериментов и разработки алгоритмов.

Данный программный модуль предлагается использовать для экспресс-обработки и анализа записанных на индикаторный блок ЭКОФИЗИКА-D уровней шума по частотным полосам.

После обработки спектров, доступной информацией будет:

1) Внешнетраекторные измерения воздушного судна.

2) Дата и время записи спектра.

3) Уровень звукового давления с частотой опроса 48000 Гц в секунду в Па.

4) Разница между полученным сигналом и отфильтрованным.

5) Калибровочное значение (Па/1_код).

Программный модуль в составе специальной организационно-технической системы должен выполнять следующие функции:

1) Оперативный импорт данных формата *.edt.

2) Вывод графика зависимости размаха сигнала в формате (24 бит) от времени в секундах.

3) Расшифровка спутникового сигнала, получение траекторных параметров воздушного судна, каждую секунду полета.

4) Получение значение звукового давления в формате (24 бит).

5) Быстрый расчет калибровочного значения.

6) Преобразование кодовых значений в физические величины.

Модуль экспресс-обработки экспериментальных данных повышает эффективность существующей системы анализа. Он позволяет снижать сроки обработки экспериментальных данных, также осуществлять обработку данных в режиме реального времени, что в свою очередь приводит к повышению процента зачетности испытательных режимов.

СПИСОК ЛИТЕРАТУРЫ

1. АР МАК, Авиационные правила, Часть 36 (АП 36), «Сертификация воздушных судов по шуму на местности», издание 2-е с поправкой 36-1, 2003.
2. ИКАО. Международные стандарты и рекомендуемая практика, Охрана окружающей среды, Приложение 16 к Конвенции о международной гражданской авиации, Том 1, Авиационный шум, 7-е издание, включающее поправки 1–11-В, Часть II, Сертификация ВС по шуму. 2014. С. 256-275.
3. Роднов А.В., Кравченко Ю.Г., Моисеев Н.А. и др. Летные исследования по оценке звукового удара от самолетов различной аэродинамической компоновки. ОАО ЛИИ им. М.М. Громова, 2002.
4. Степаненко А.Н., Наквасин А.Ю., Юнкерт А.С. и др. Исследования по повышению эффективности (сокращению сроков и стоимости) летных испытаний по определению характеристик шума ВС на местности: научно-технический отчет ЛИИ 175-16-II. Жуковский, 2016. 51 с.

УДК 001.891.57: 004.657

Р. Р. БУЛЯКОВ, Р. В. ПРОСКУРА, А. И. САДРТДИНОВА, Р. Р. КАРИМОВ
bulyakovrustam@mail.ru, reggg99@mail.ru, aigul_sadrtdinova@mail.ru, rikar@yandex.ru
Науч. руководд. – канд. техн. наук, доц. Р. Р. КАРИМОВ

Уфимский государственный авиационный технический университет

ИНФОРМАЦИОННАЯ ПОДДЕРЖКА ПРОЦЕССА ХРАНЕНИЯ И ОБРАБОТКИ ОПЕРАТИВНЫХ ДАННЫХ В ВИРТУАЛЬНОМ ТРЕНАЖЕРЕ

Аннотация. Рассматривается задача программной реализации процесса регистрации событий в виртуальном тренажере на базе интерактивной графической среды Unity 3D и сервера базы данных SQLite.
Ключевые слова: регистрация событий; обработка событий; визуализация; события; скрипты; база данных; таблицы; запросы БД; Unity 3D; SQlite.

Актуальность

В настоящее время популярность виртуальных тренажеров растет в различных отраслях промышленности. Эффект от обучения и аттестации сотрудников организационно-технической системы с применением виртуального тренажера обусловлен целым рядом психофизиологических, производственно-технических и организационно-управленческих факторов [3].

Виртуальный тренажер должен реагировать на различные события и действия обучаемого оператора, регистрировать и анализировать выполненные операции. Поэтому задача обеспечения безопасности хранения и использования данных является одной из основных.

Рассматриваемый проект тренажера разрабатывается на базе интерактивной графической среды Unity 3D. В настоящее время большинство проектов, созданных в Unity 3D, имеют подсистему хранения игровых данных. Такая подсистема должна включать в себя инструменты для загрузки данных в базу данных (БД), извлечения и дальнейшей обработки данных. Архитектура подсистемы (какие данные, как и где их хранить) часто зависит от того, что это за игра, кто в нее играет и какое количество данных необходимо сохранить. Архи-

тектура подсистемы хранения оказывает существенное влияние на производительность виртуального тренажера.

Рассматриваемый виртуальный тренажер предполагает, что каждый сценарий технологического процесса включает порядка 40 технологических операций, каждая из которых предполагает около 5 различных действий с технологическими объектами, инструментами и элементами управления. Помимо этого, виртуальный тренажер предполагает работу различных пользователей в однопользовательском режиме. Таким образом, в процессе однократного выполнения технологического сценария в виртуальном тренажере одним обучаемым (игроком) формируется около 200 относительно коротких транзакций. Формирование подсказок и проверок в процессе обучения также требуют выполнения запросов к БД.

Таким образом, необходима программная реализация подсистемы хранения и обработки оперативных данных, позволяющая:

– обеспечить безопасность данных пользователей;

– анализировать действия пользователей и их прогресс;

– оперативно получать ответы на запросы и реакции на изменения;

Для корректной работы тренажера необходимо решить задачу регистрации, обработки и распознавания событий и последующей визуализации.

Постановка задачи

Цель работы – это повышение эффективности обучения на основе информационной поддержки процесса регистрации событий в виртуальном тренажере.

Для достижения поставленной цели необходимо решить следующие задачи:

1) Разработка функциональной и информационной моделей процесса регистрации событий;

2) Обоснование выбора технологии регистрации событий;

3) Программная реализация процесса регистрации событий в виртуальном тренажере.

Под событием в виртуальном тренажере в рамках статьи упрощенно рассматривается вход-выход оператора в зону контакта технологического объекта, например, шкафа автоматизации. Также в качестве событий могут быть рассмотрены – взаимодействие с инструментом (взять, применить, положить), элементом управления (выбор элемента управления и его переключение).

Разработка функциональных и информационных моделей

Функциональная модель процесса регистрации в БД событий в виртуальном тренажере разработана на основе технологии IDEF0 (Рисунок 1).

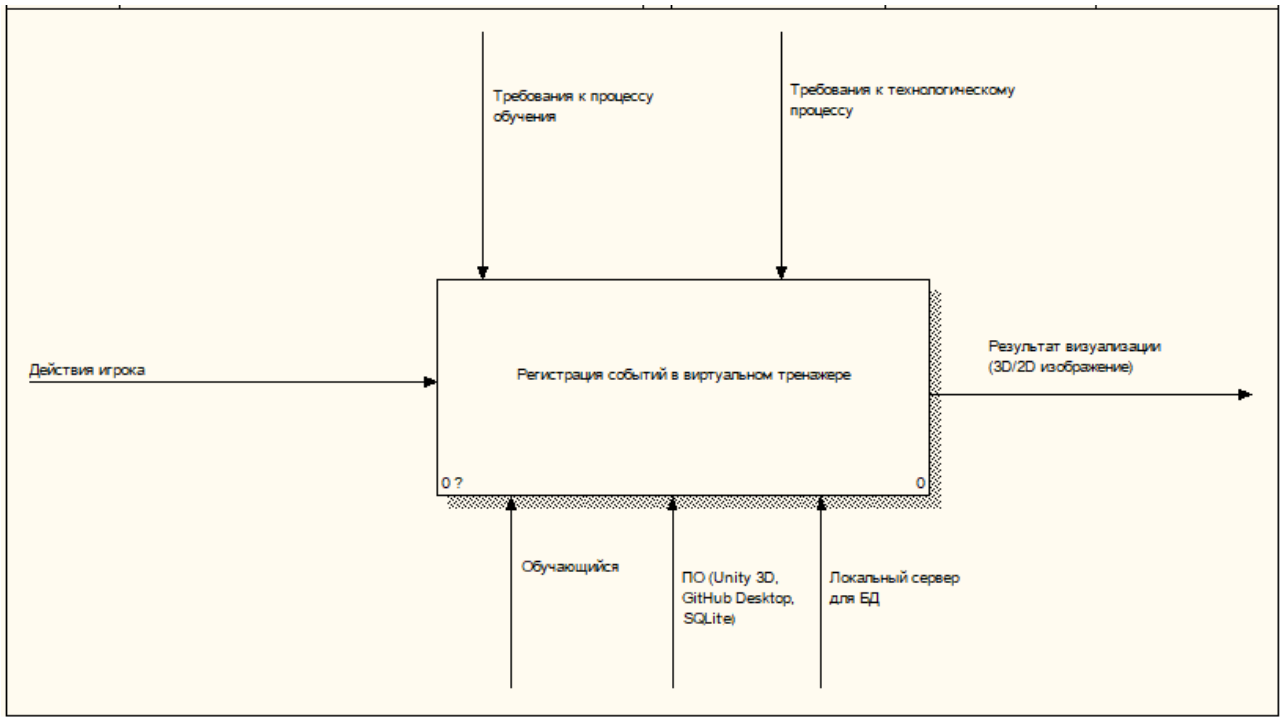


Рис. 1. Контекстная диаграмма процесса регистрации событий в виртуальном тренажере

Диаграмма декомпозиции первого уровня включает в себя следующие подпроцессы (Рисунок 2):

– Регистрация событий;

– Обработка и распознавание событий;

– Визуализация действий игрока.

Входными данными для моделирования являются действия игрока. Выходной информацией является результат визуализации 3D/2D изображение. Механизмами выступают обучающийся, ПО, локальный сервер базы данных.

Управляющее взаимодействие происходит посредством требования к процессу обучения и требований к технологическому процессу.

На основе анализа потоков данных из функциональной модели разработана информационная модель процесса на базе технологии IDEF1 (Рисунок 2).

Механизмами на данной декомпозиции являются:

– обучающийся;

– программное обеспечение (Unity 3D, GitHub Desktop, SQLite);

– локальный сервер для БД;

– скрипты;

– запросы к БД.

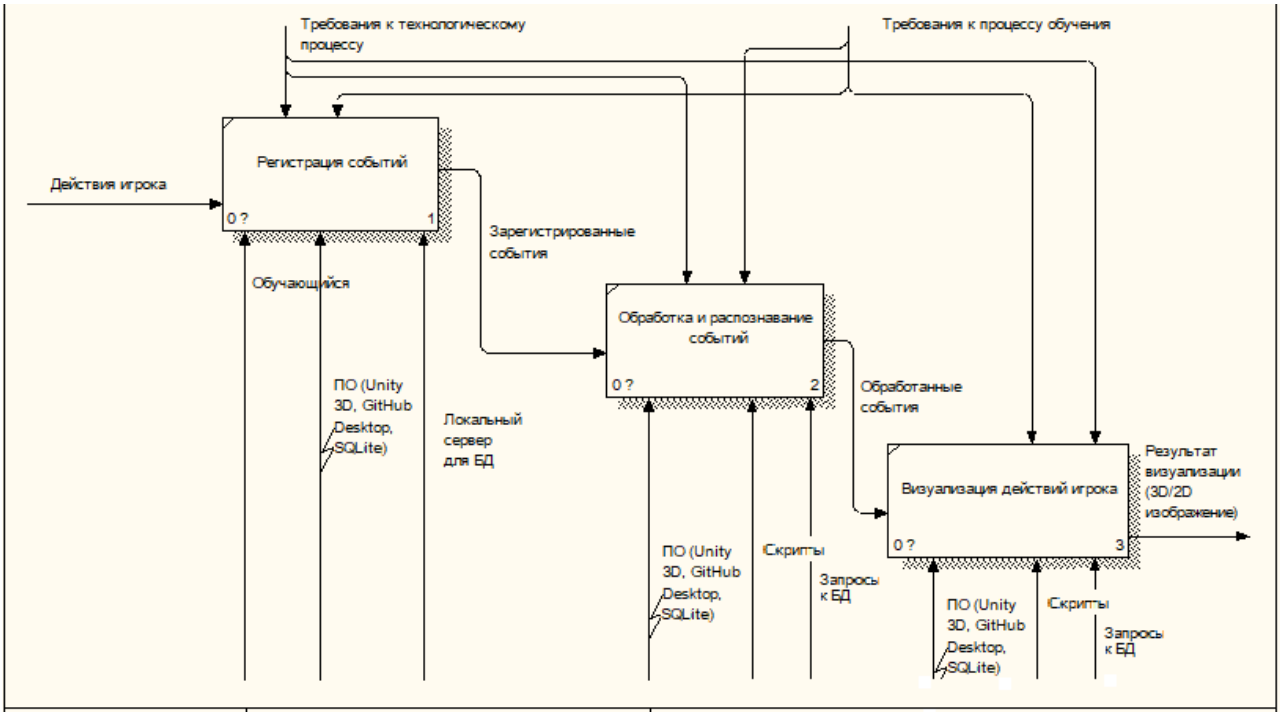


Рис. 2. Диаграмма декомпозиции первого уровня

На рисунке 3 представлена упрощенная информационная модель, используемая для реализации программного макета регистрации событий.

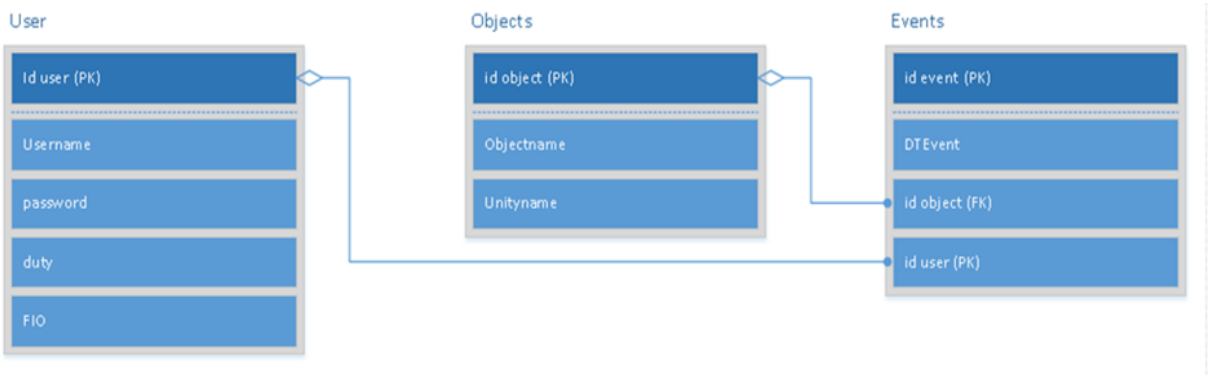


Рис. 3. Упрощенная информационная модель

Сущность User предназначена для регистрации игрока в виртуальном тренажере. Здесь каждый пользователь имеет собственное Id user (PK). Сущность Objects предназначена для указания технологических объектов сцены, каждый объект имеет собственное Id object (PK). Сущность Events предназначена для регистрации событий. Она является связующей между сущностями User и Objects.

Общая информационная модель тренажера приведена на следующей схеме (Рисунок 4).

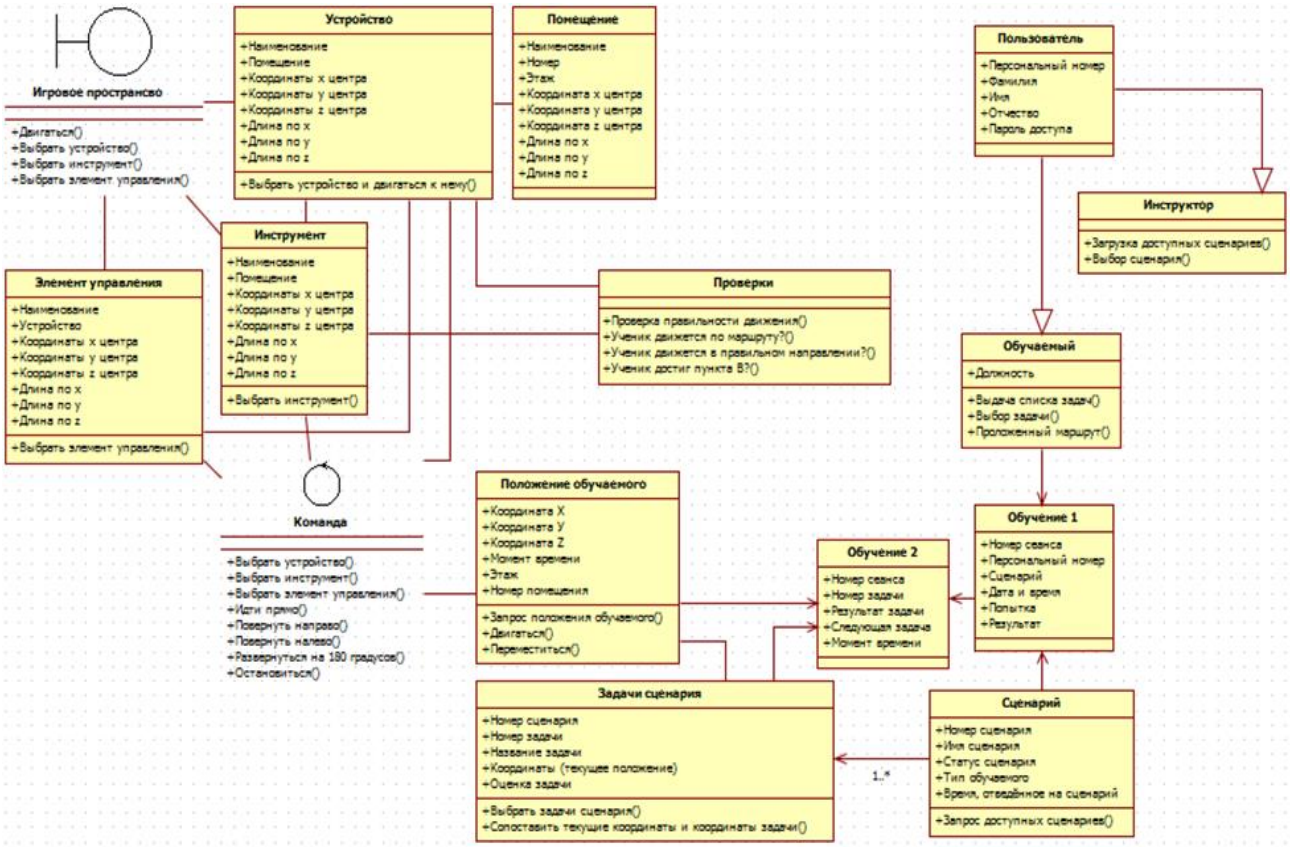


Рис. 4. Структура исследуемого объекта

Обоснование выбора технологии регистрации событий

В качестве средства реализации для решения задач в рамках данной работы, несмотря на то, что существуют аналоги сред разработки виртуальных тренажеров (Unreal Engine), будем использовать межплатформенную среду разработки Unity 3D, так как в ней уже ведется работа по проекту тренажера.

Таким образом, необходимо связать Unity 3D с какой-либо встраиваемой системой управления баз данных. На основе анализа источников, рассмотрено несколько вариантов связи виртуального тренажера с базой данных: Unity 3D + MySQL, Unity 3D + SQLite, Unity 3D +Azure (cloud), Unity 3D + PHP + MySQL.

Предпочтительным вариантом оказался SQLite в силу компактности этой встраиваемой СУБД. Размер библиотек SQLite составляет всего 250 КБ, в то время как библиотеки MySQL занимают 600 МБ, что утяжеляет сцену. Кроме того, выбранная СУБД – это проект с открытым исходным кодом на языке Си, находящийя в открытом доступе. SQLite – это серверная база данных, которая является автономной, также относится к встроенным базам данных, что означает, что механизм БД работает как часть приложения.

Unity – это межплатформенная среда разработки компьютерных игр, разработанная американской компанией Unity Technologies. Unity позволяет создавать приложения, работающие на более чем 25 различных платформах, включающих персональные компьютеры, игровые консоли, мобильные устройства, интернет-приложения и другие. Выпуск Unity состоялся в 2005 году и с того времени идет постоянное развитие [1].

SQLite – компактная встраиваемая СУБД, которая реализует быстрое, автономное, высоконадежное, полнофункциональное использование баз данных, поддерживает стандарт SQL. SQLite – наиболее часто используемая кроссплатформенная СУБД в мире, она встроена во все мобильные телефоны и большинство компьютеров и поставляется в комплекте с множеством других апробированных приложений. Формат файла SQLite стабилен, разработчики обещают

сохранить его таким до 2050 года. Исходный код библиотеки на языке Си передан в общественное достояние [2].

Программная реализация процесса

Программная реализация процесса хранения и обработки оперативных данных строится на основе прототипа сцены виртуального тренажера. В сцене задан 3D-примитив шкафа автоматизации в качестве технологического объекта, определена зона контакта (Collider) в виде прямоугольного параллелепипеда (Box Collider).

Для взаимодействия с технологическим объектом в проекте тренажера-симулятора оператор должен войти в зону контакта. При этом зоны контакта двух технологических объектов не пересекаются, что позволяет разделять программным путем события, связанные с разными объектами. Также необходимо, чтобы свойство Name каждого объекта сцены соответствовало требованиям по именованию объектов в тренажере.

Рассмотрены 2 вида событий – вход в зону контакта и выход из нее. В соответствии с упрощенной информационной моделью (рис.3) создана БД в SQLite.

Алгоритм регистрации событий включает следующие шаги:

1) соединение с БД;

2) определение типа события и идентификация объекта – вход в зону контакта или выход из нее;

3) формирование запроса к БД на добавление данных и выполнение запроса.

Процесс регистрации событий реализован в виде методов класса на языке C#: start - соединение с БД; OnTriggerEnter / OnTriggerExit - определение типа события и идентификация объекта; AddEvents - формирование запроса к БД на добавление данных и выполнение запроса.

Созданный класс может быть внедрен для использования в основной сцене виртуального тренажера с целью регистрации событий, происходящих в сцене.

СПИСОК ЛИТЕРАТУРЫ

1. [Электронный ресурс]. URL: https://unity.com/ru (Дата обращения: 13.08.2021)
2. [Электронный ресурс]. URL: https://sqlite.org/index.html (Дата обращения:13.08.2021)
3. Юмадилова И.Р., Арсланов Т.Р., Макаев Р.А., Каримов Р.Р. Информационная поддержка процесса групповой разработки виртуального тренажера для обучения персонала производственного объекта // В сборнике: МАВЛЮТОВСКИЕ ЧТЕНИЯ. Материалы XIV Всероссийской молодежной научной конференци. – Уфа, 2020. Т.5, ч.3 - С. 297-306.

УДК 681.518 (075.8)

Г. Р. ГАБДЕЛХАКОВА, Р. Р. КАРИМОВ
gulshat.gabdelkhakova@yandex.ru, rikar@yandex.ru
Науч. руководв. – канд. техн. наук, доц. Р. Р. КАРИМОВ

Уфимский государственный авиационный технический университет

ИНФОРМАЦИОННАЯ ПОДДЕРЖКА КОНСТРУКТОРСКО-ТЕХНОЛОГИЧЕСКОГО ОБЕСПЕЧЕНИЯ ИЗДЕЛИЯ НА ОСНОВЕ ИНТЕРАКТИВНЫХ ЭЛЕКТРОННЫХ ТЕХНИЧЕСКИХ РУКОВОДСТВ

Аннотация. Рассматривается задача разработки интерактивных электронных технических руководств (ИЭТР) и применения ИЭТР для информационной поддержки сложного технического изделия.
Ключевые слова: организационно-техническая система; электронное техническое руководство; информационная поддержка; сложное изделие; структура документации; модули данных.

Введение

При разработке интерактивного технических руководств важным является обеспечение унифицированной для всех ИЭТР способов взаимодействия с пользователем и стандартная техника представления информации.

Интерактивные электронные технические руководства (ИЭТР) являются действенным средством информационной поддержки изделия на этапе эксплуатации.

В общем случае ИЭТР характеризуется как комплекс взаимосвязанных технических данных, хранимых в единой или распределенной системе хранения. ИЭТР включает в себя всю информацию, относящуюся к области применения технического руководства, и проектируется с учетом последующего отображения на электронном дисплее. Элементы данных в ИЭТР логически взаимосвязаны так, что пользователь может быстро получить доступ к нужной информации. ИЭТР позволяет в интерактивном режиме предоставлять справочную и описательную информацию о проведении эксплуатационных и ремонтных процедур. Помимо текста и графических данных ИЭТР может содер жать аудио и видео данные, а также предоставлять доступ к внешним источникам информации через компьютерные сети.

Электронная система отображения, в свою очередь, обеспечивает унифицированный для всех ИЭТР способ взаимодействия с пользователем и стандартную технику представления информации.

Среди программных комплексов, предназначенных для разработки, сопровождения, изменения и публикации технической документации можно выделить TG Builder.

TG Builder это система автоматизированной подготовки сопроводительной документации в электронном и бумажном виде на сложные изделия.

На многих предприятиях с высоким уровнем автоматизации проектно-конструкторских и технологических работ схема взаимодействия отделов предприятия может быть описана следующим образом (Рисунок 1).

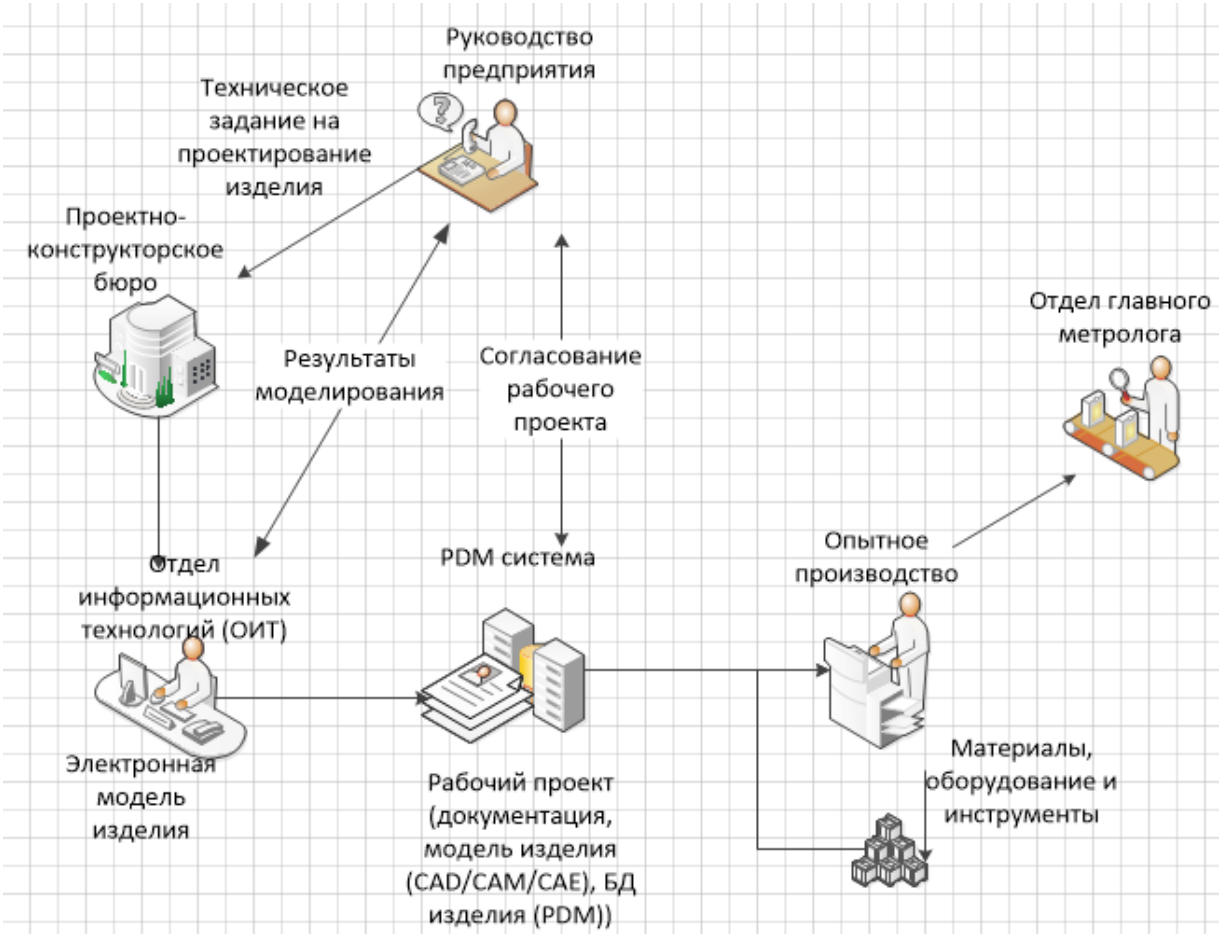


Рис. 1. Схема взаимодействия отделов предприятия в процессе конструкторско-технологического обеспечения производства

На предприятие поступает заказ на изготовление изделия. Руководство передает техническое задание на изготовление изделия в проектно-конструктор-ское бюро, которое формирует технический проект и передает его

в отдел информационных технологий для моделирования изделия. При этом отдел информационных технологий предоставляет результаты моделирования руководству.

После отработки электронной модели создается рабочий проект, который согласовывается с руководством предприятия и заказчиком. После согласования с заказчиком рабочий проект предается в опытное производство. Далее изготовленное изделие передается в отдел главного метролога, в котором производятся контрольные измерения.

Постановка задачи

Целью работы является повышение эффективности проектирования изделия на основе информационной поддержки конструкторско-технологического обеспечения, включающего поддержку изделия на основе интерактивного электронного технического руководства

Для достижения поставленной цели необходимо разработать интерактивное электронное техническое руководство сложного изделия.

Программная реализация процесса

Программная реализация процесса конструкторско-технологического обеспечения выполнена в системе TG Builder, в состав которого входят следующие модули.

Модуль TG Designer предназначен для проектирования шаблонов руководств. Шаблон руководства — это набор правил, справочников и макетов оформления, используемых в процессе подготовки документации и предназначенных для стандартизации структуры, состава и оформления документации в рамках проекта.

Модуль TG Admin предназначен для управления учетными записями пользователей TG Builder и управления шаблонами руководств, подготовленных при помощи утилиты TG Designer.

Модуль TG Builder является основным модулем продукта и непосредственно предоставляет главные функции для формирования электронного руководства.

Модуль TG Browser представляет собой систему отображения ИЭТР для передачи эксплуатантам в качестве сопроводительной документации к изделию в электронном или бумажном виде.

Создание нового проекта ИЭТР в TG Builder, задание свойства проекта, свойства задачи и исполнителей.

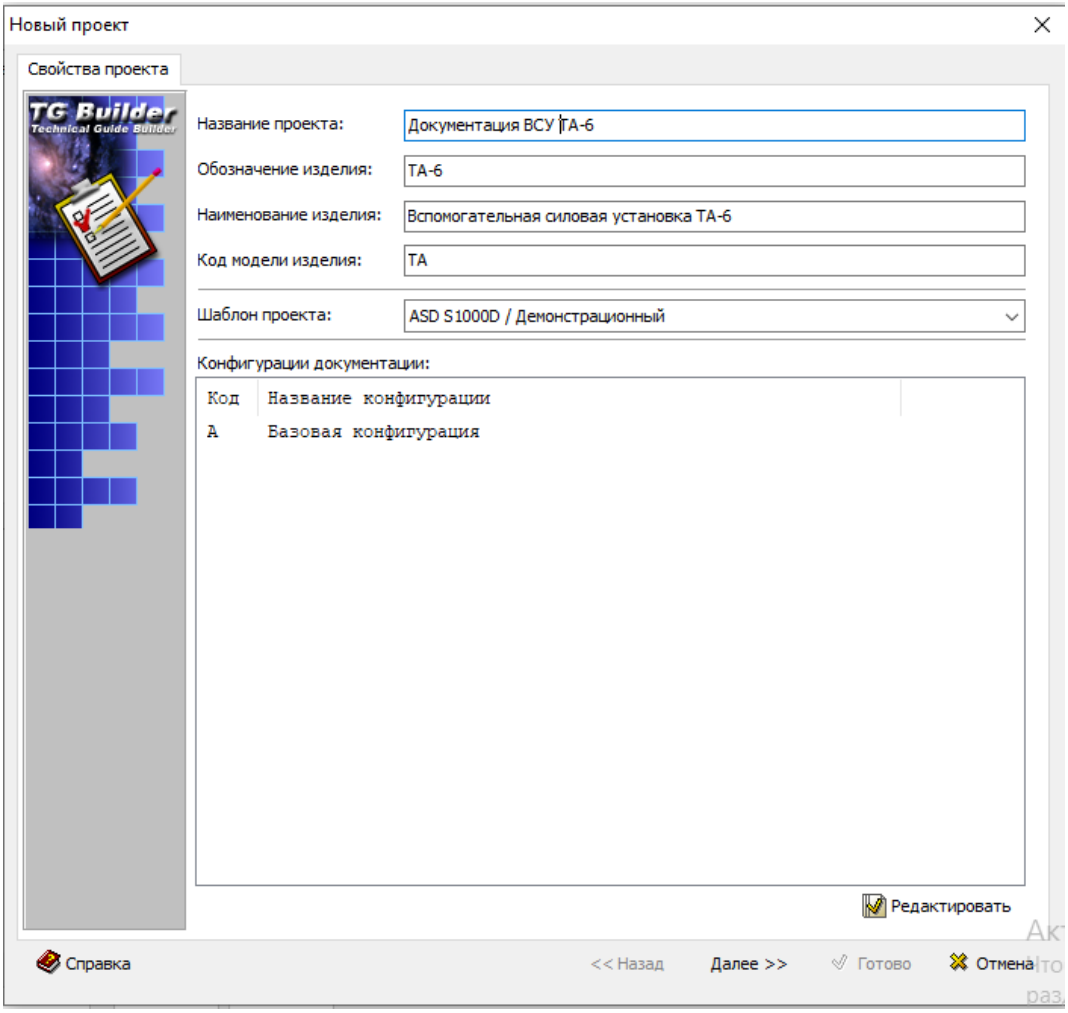


Рис. 2. Проект ИЭТР

Разработать структуру проекта, содержащую необходимые разделы и модули данных в зависимости от изделия.

Структура ИЭТР имеет следующий вид:

– Титульный лист электронного руководства;

– Перечень действующих публикаций;

– Перечень модификации;

– Введение;

– Перечень сокращений;

– Руководство по технической эксплуатации;

– Схема ВСУ ТА-6;

– Описание ВСУ ТА-6;

– Технические характеристики и общие сведения.

В модуле «Перечень модификации» содержится информация о видах ВСУ ТА-6.

В модуле «Введение» приведены общие сведения о ВСУ ТА-6.

В модуле «Перечень сокращений» содержится сокращения, используемые в руководстве по технической эксплуатации ВСУ ТА-6.

В модуле «Руководство по технической эксплуатации» содержит описание и технологию обслуживания ВСУ ТА-6.

Структура проекта представлена на рисунке 3.

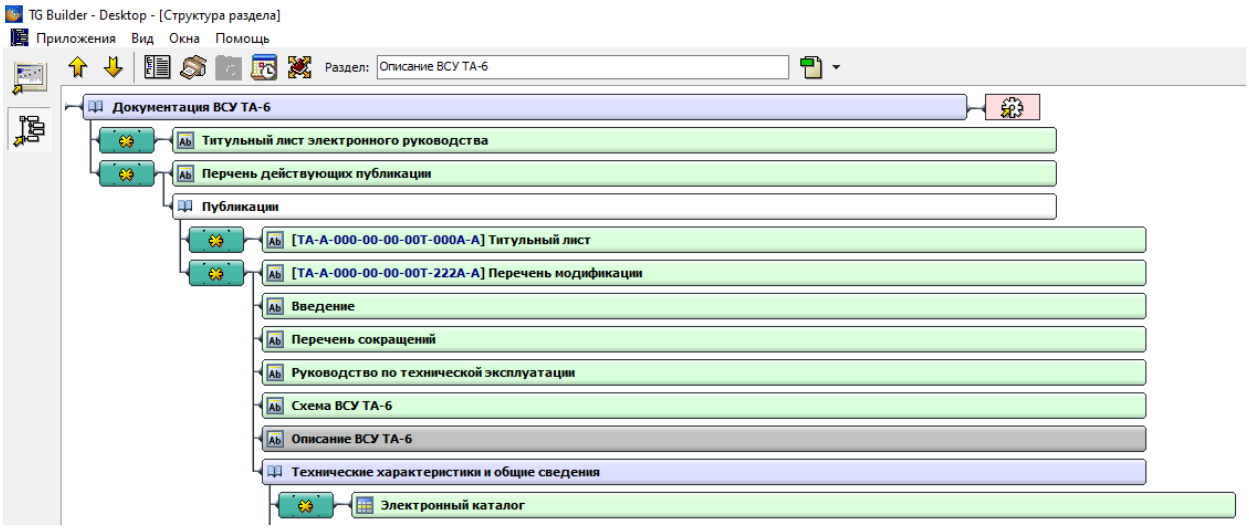


Рис. 3. Структура проекта

Для каждого модуля данных должен быть указан тип, название и код.

Каждый из модулей данных ИЭТР должен быть содержательно наполнен текстом с помощью редактора модулей данных (Рисунок 4).

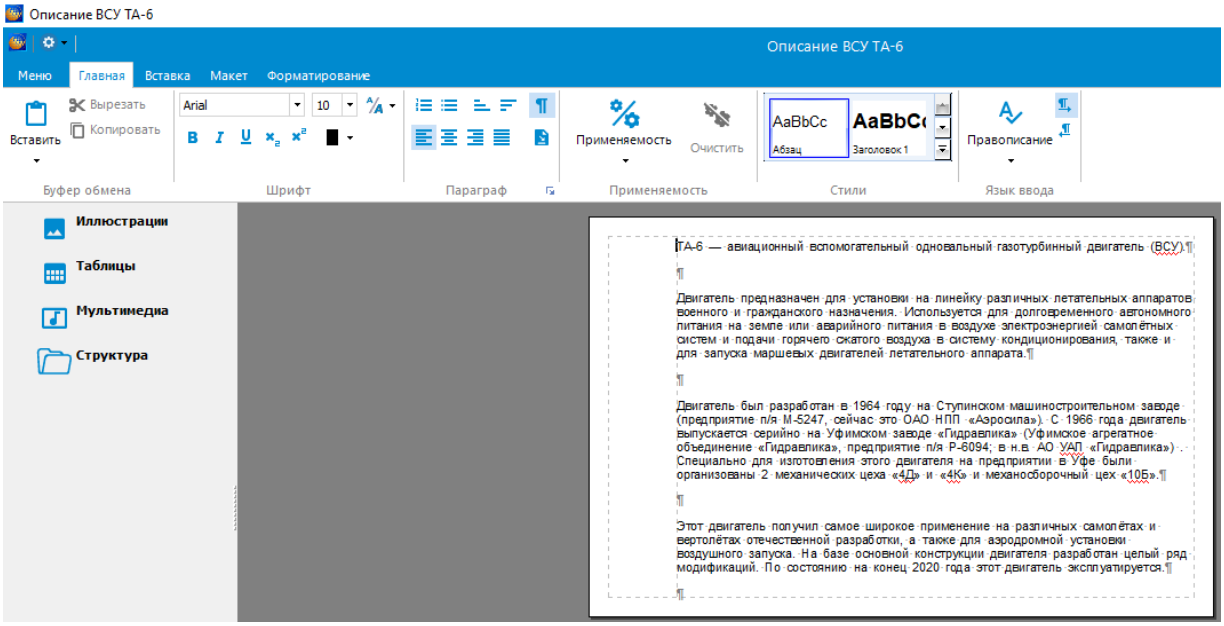


Рис. 4. Наполнение текстом

Созданный ИЭТР может быть открыт для просмотра и дальнейшего использования в модуле TGBrowser. ИЭТР представляет собой сопроводительную документацию к изделию в электронном виде (Рисунок 5).

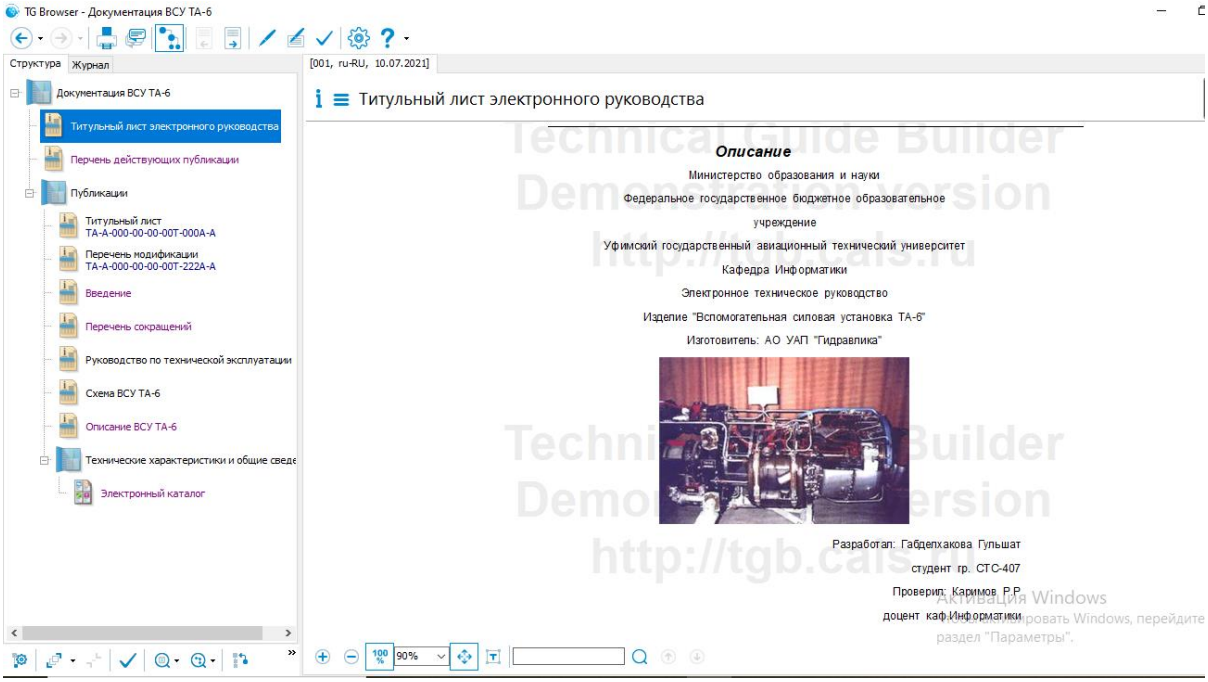


Рис. 5. Разработанный ИЭТР в TG Browser

Таким образом, ИЭТР может быть использован для решения комплекса задач, связанных с информационной поддержкой процессов эксплуатации, обслуживания и ремонта изделия.

СПИСОК ЛИТЕРАТУРЫ

1.TG Builder. Архитектура. Задачи. Возможности (Дата обращения: 19.08.2021).
2. Технологии информационной поддержки жизненного цикла изделия: Лабораторный практикум / Уфимск. гос. авиац. техн. ун-т; Сост. Р.Р. Каримов, Н.В. Кондратьева. – Уфа, УГАТУ, 2016. – 88 с. (Дата обращения:16.08.2021).

УДК 519.87

Т. И. ГАРИФУЛЛИН, Н. А. ГАРИФУЛЛИНА
murkat2007@yandex.ru

МАОУ «Лицей №58» ГО г. Уфа
Уфимский государственный авиационный технический университет

CAT NETWORK. ИНСТАГРАМ ДЛЯ КОТОВ

Аннотация. Приложение Cat Network является социальной сетью для кошек. В приложении есть два искусственных интеллекта. Первый определяет, есть ли на фото кошка, а второй - ее породу. Аналогов в Google Play Market нет.
Работа выполнена в виде индивидуального проекта при обучении в IT школе Samsung.
***Ключевые слова*:** Kotlin; большие данные; искусственный интеллект; мобильное приложение; инстаграм; кот.

Большие данные (англ. big data) – обозначение структурированных и неструктурированных данных огромных объемов и значительного многообразия, эффективно обрабатываемых горизонтально масштабируемыми программными инструментами, появившимися в конце 2000-х годов и альтернативных традиционным системам управления базами данных и решениям класса Business Intelligence. В широком смысле о «больших данных» говорят как о социально-экономическом феномене, связанном с появлением технологических возможностей анализировать огромные массивы данных, в некоторых проблемных областях – весь мировой объем данных, и вытекающих из этого трансформационных последствий.

Искусственный интеллект (ИИ; англ. artificial intelligence, AI) – свойство интеллектуальных систем выполнять творческие функции, которые традиционно считаются прерогативой человека; наука и технология создания интеллектуальных машин, особенно интеллектуальных компьютерных программ. ИИ связан со сходной задачей использования компьютеров для понимания человеческого интеллекта, но не обязательно ограничивается биологически правдоподобными методами. Проблематика машинного обучения касается процесса самостоятельного получения знаний интеллектуальной системой в процессе ее работы.

Это направление былоцентральным с самого начала развития ИИ. Одно из частных определений интеллекта, общее для человека и «машины», можно сфор-

мулировать так: «Интеллект – способность системы создавать в ходе самообучения программы (в первую очередь эвристические) для решения задач определенного класса сложности и решать эти задачи».

При обучении разработке мобильных приложений для операционной системы Android было принято решение о написании собственной версии инстаграм.

Проект содержит следующие возможности:

– создание и редактирование профиля пользователя,

– просмотр и добавление постов,

– пагинация и асинхронная загрузка записей,

– определение породы кошки, выборка и сортировка по породам.

Все данные хранятся в облачных сервисах Firebase. Для аутентификации пользователя используются почта и пароль. При регистрации создается запись в облачной базе данных со всеми данными профиля.

На главной странице пользователя ждут свежие записи.

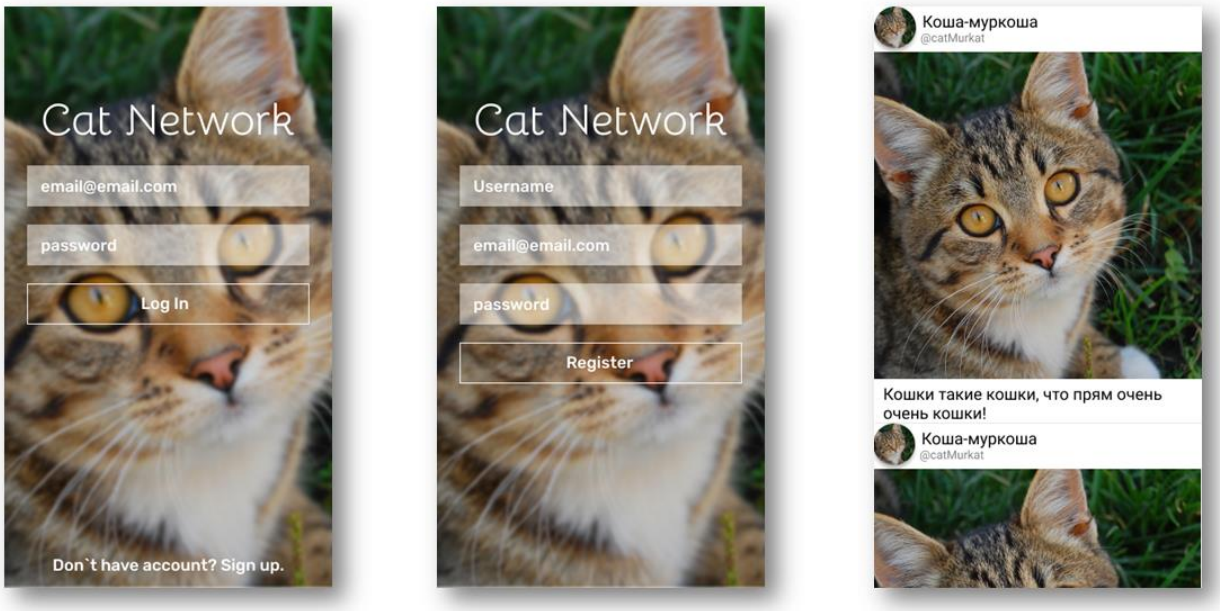
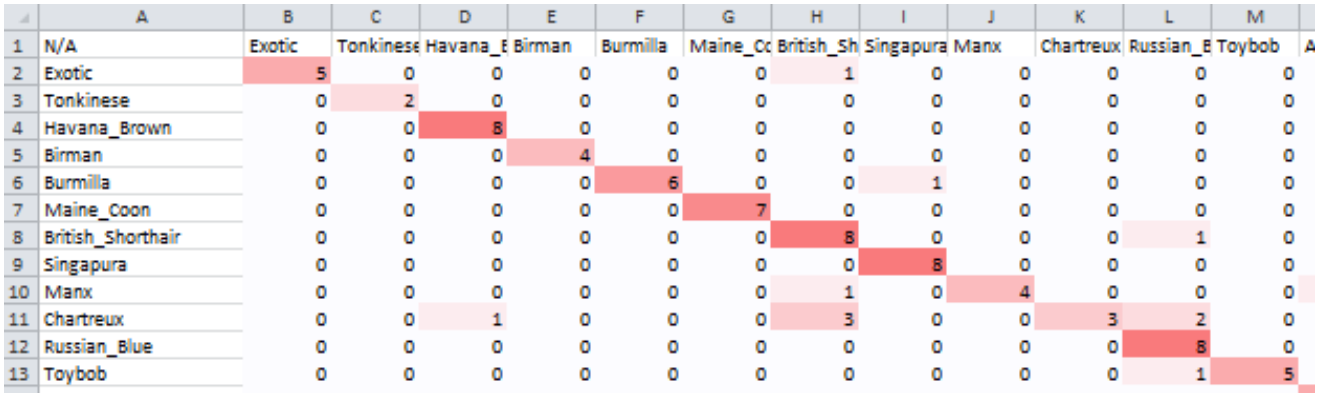


Рис. 1.

С сайта http:// cfa.org (Cat Fanciers` Association) были взяты сорок пород кошек. Далее из открытых источников было скачано по 100 фотографий каждой породы.

Результаты обучения ИИ были сформированы в файл Excel. На следующем рисунке представлена часть файла.



	A	B	C	D	E	F	G	H	I	J	K	L	M
1	N/A	Exotic	Tonkinese	Havana_B	Birman	Burmilla	Maine_Co	British_Sh	Singapura	Manx	Chartreux	Russian_B	Toybob
2	Exotic	5	0	0	0	0	0	1	0	0	0	0	0
3	Tonkinese	0	2	0	0	0	0	0	0	0	0	0	0
4	Havana_Brown	0	0	8	0	0	0	0	0	0	0	0	0
5	Birman	0	0	0	4	0	0	0	0	0	0	0	0
6	Burmilla	0	0	0	0	6	0	0	1	0	0	0	0
7	Maine_Coon	0	0	0	0	0	7	0	0	0	0	0	0
8	British_Shorthair	0	0	0	0	0	0	8	0	0	0	1	0
9	Singapura	0	0	0	0	0	0	0	8	0	0	0	0
10	Manx	0	0	0	0	0	0	1	0	4	0	0	0
11	Chartreux	0	0	1	0	0	0	3	0	0	3	2	0
12	Russian_Blue	0	0	0	0	0	0	0	0	0	0	8	0
13	Toybob	0	0	0	0	0	0	0	0	0	0	1	5

Рис. 2.

При загрузке фотографий кошек в постах ИИ определяет породу кошки и записывает информацию о породе в соответствующую переменную.

Используемые инструменты:

– Android Studio (для реализации мобильного приложения)

– Figma (для проектирования внешнего вида мобильного приложения)

– Adobe Photoshop (для создания логотипа мобильного приложения)

– Сайт firebase.google.com (помогает создавать и поддерживать работу успешных приложений).

Используемые библиотеки:

– Библиотеки, связанные с Firebase (Firestore, Storage, Authentication, Firebase ML Kit,),

– Glide (быстрая и эффективная библиотека для управления мультимедиа с открытым исходным кодом и загрузки изображений для Android, которая объединяет декодирование мультимедиа, кэширование памяти и диска, а также объединение ресурсов в простой и удобный интерфейс),

– Cat Loading (красивая анимация загрузки),

– Preferences (хранение настроек приложения в памяти устройства),

– Image Picker (простая в использовании и настраиваемая библиотека для выбора изображения из галереи или захвата изображения с помощью камеры, также позволяет обрезать и сжимать изображение в зависимости от соотношения сторон, разрешения и размера изображения),

– Paging 3(одна из новых библиотек Jetpack для эффективного управления и загрузки большого объема набора данных из различных источников данных).

Результаты работы мобильного приложения можно видеть на рисунках.

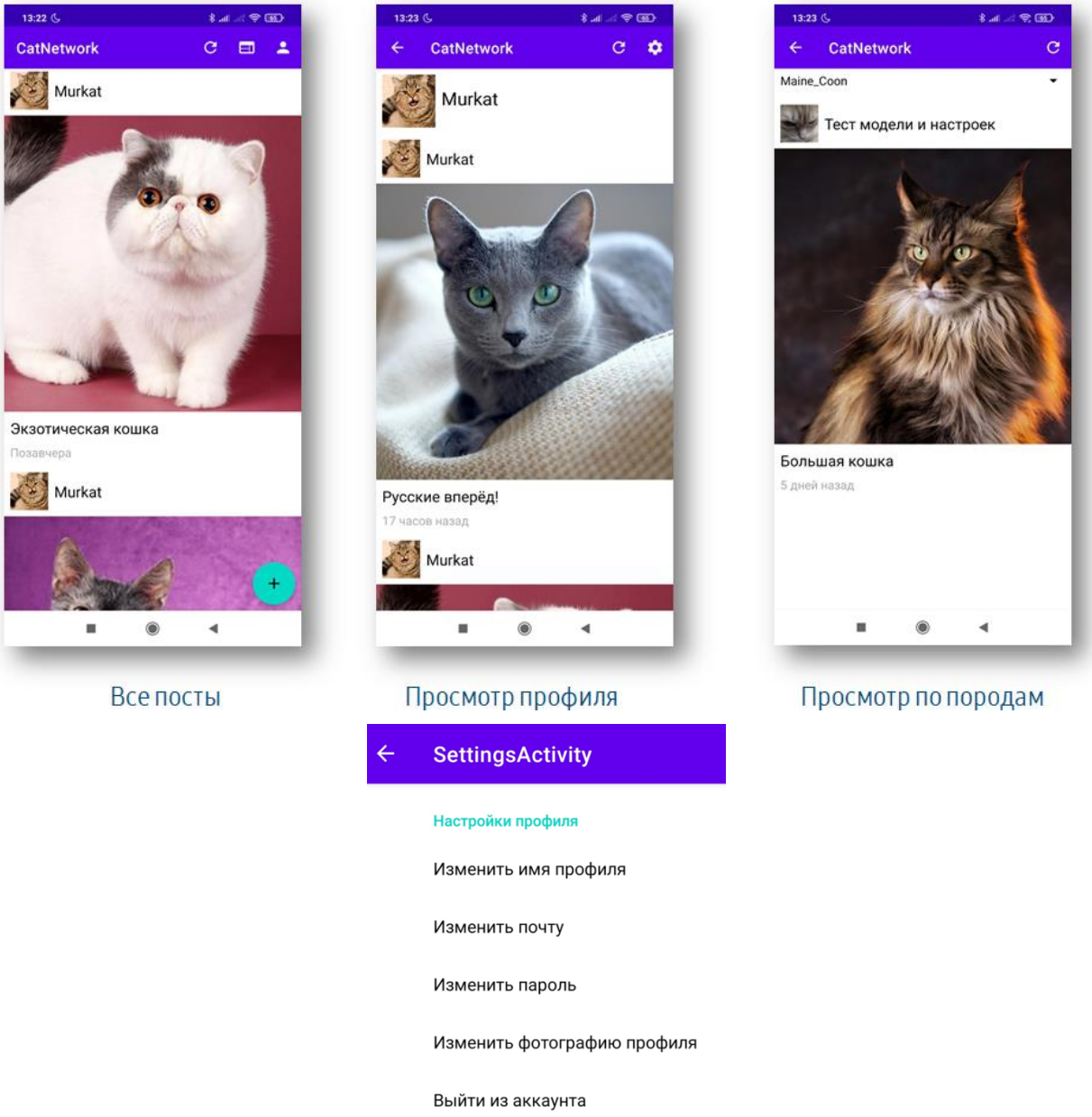


Рис. 3. Настройки пользователя

Результатом работы является мобильное приложение, обладающее функционалом, решающим поставленную цель: создание и редактирование профиля

пользователя, просмотр и добавление постов, пагинация и асинхронная загрузка записей, определение породы кошки, выборка и сортировка по породам.

Перспективы развития: русифицировать породы кошек, добавить рейтинг, реализовать подписки, добавить поддержку других пород.

СПИСОК ЛИТЕРАТУРЫ

1. Samsung Innovation Campus Bootcamp: Kotlin for Android
2. Сайт http:// cfa.org (Cat Fanciers` Association) – породы кошек
3. Сайт ru.wikipedia.org
4. Документация разработчика Android https://developer.android.com

УДК 004.946

В. А. ГЛУЩЕНКО, Д. В. ШЛЁНКИН, А. В. ШУНДЕЕВ, М. А. ИВАНОВ
val_g_2001@bk.ru, kot.dima2011@yandex.ru, artem_shundeev@mail.ru, aa4052783@gmail.com
Науч. руководит. – канд. техн. наук, доц. А. С. КОВТУНЕНКО

Уфимский государственный авиационный технический университет

РАСПОЗНАВАНИЕ ЛИЦ С ПОМОЩЬЮ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Аннотация. Рассматривается алгоритмы и технологии распознавания лиц с помощью технологий компьютерного зрения и искусственного интеллекта.
***Ключевые слова*:** компьютерное зрение; распознавание лиц; обработка изображений; распределенная система контроля версий.

Актуальность работы

В современном мире практически везде используются камеры для осуществления контроля или обеспечения безопасности в различных местах, будь то какое-либо предприятие или место большого скопления людей (университеты, школы, больницы). Но большое количество камер, например в общественных местах не гарантирует безопасность людей, потому что охранники, наблюдающие за камерами, могут видеть текущую ситуацию в целом, не сильно вглядываясь в экран, особенно когда этих камер десятки. Поэтому если на территорию с ограниченным доступом попадет человек, который не должен был там находиться, то охранник может не заметить, что это посторонний. Например, если на какое-нибудь предприятие проберется злоумышленник, то его могут не отличить от обычного сотрудника. В большинстве таких ситуаций посторонний был бы обнаружен, если бы камеры могли распознавать лица, и определять, должен ли тут находиться этот человек, или нет. Существует большое количество сфер, где распознавание лиц было бы необходимо, но в современном мире такие программы еще не сильно распространены.

Для разработки программы для классификации лиц необходимо:

1. Исследовать существующие способы распознавания лиц
2. Разработать программу распознавания лиц

3. Разработать алгоритм сохранения цифровых отпечатков новых лиц в базу данных.

Обоснование выбора программного обеспечения

Для решения перечисленных выше задач предложено использовать следующее программное обеспечение.

1. Язык программирования python с библиотекой opencv.

Библиотека opencv позволяет реализовать такой функционал, как:

– Получение изображения с потоковых камер

– Работа с изображениями и видео

– Применение множества фильтров, таких как размытие изображения, нахождение контуров объектов, побитовое наложение кадров друг на друга

2. Нейросеть для классификации лиц resnet.

Нейросеть находит на лице 128 точек и вычисляет между ними расстояние, для масштабируемости, преобразуемое в коэффициенты. Расстояния(коэффициенты) у каждого человека уникальны, и как правило совпадают максимум на 50%, поэтому если совпадение больше 60%, значит можно сделать вывод, что это один человек.

3. Система контроля версий для обеспечения эффективной командной работы над проектом. Для этой цели выбраны система Git, хостинг GitHub и его локальная версия – программа GitHub Desktop, устанавливаемая на компьютер участника группы.

Git – распределенная система управления версиями. Проект был создан Линусом Торвальдсом для управления разработкой ядра Linux, первая версия выпущена 7 апреля 2005 года.

Пример работы программы

Для сохранения цифрового отпечатка лица используем первый алгоритм, который находит все точки, и сохраняет вектор расстояний между ними (Рисунок 1).

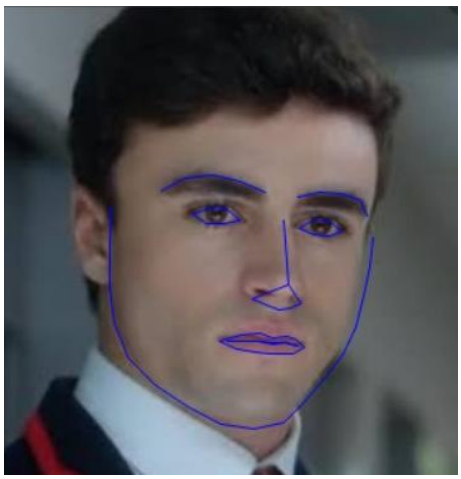


Рис. 1. Визуализация нахождения ключевых точек

Теперь во время работы алгоритма при обнаружении на камере лица будет считан его отпечаток и отправлен на сравнение в базу данных, если он совпадает с каким-нибудь отпечатком в базе данных, то на экране это лицо выделяется и высвечивается его id в системе, если же это неизвестный, то его лицо помечается красным прямоугольником (Рисунок 2).

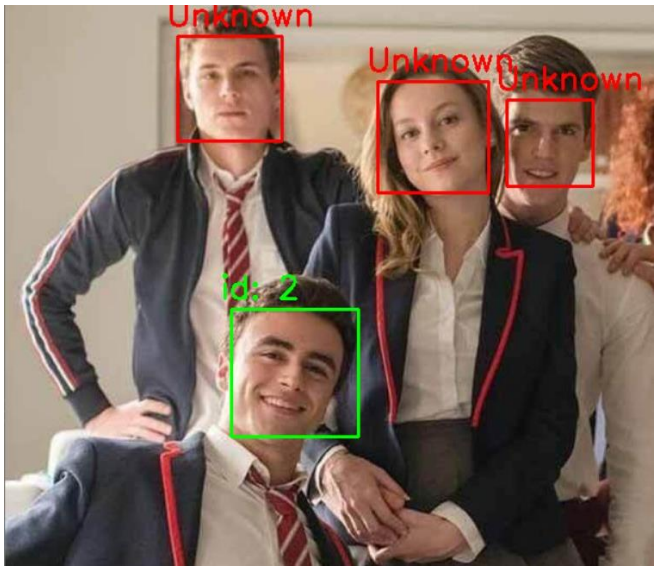


Рис. 2. Распознавание лиц

СПИСОК ЛИТЕРАТУРЫ

1. «Компьютерное зрение: технологии, рынок, перспективы», отчет TAdviser, 2018. [Электронный ресурс] – URL: https://www.tadviser.ru/index.php/Статья:Компьютерное_зрение:_технологии,_рынок,_перспективы (Дата обращения: 27.09.2021)
2. Шапиро, Дж. Стокман. Компьютерное зрение = Computer Vision. М.: Бином. Лаборатория знаний, 2006.
3. Блог Яндекса. Как это работает? Компьютерное зрение. [Электронный ресурс] – URL: https://yandex.ru/blog/company/80564 (Дата обращения: 27.09.2021)
4. Обнаружение и распознавание лиц на python [Электронный ресурс] – URL: https://robotos.in/uroki/obnaruzhenie-i-raspoznavanie-litsa-na-python (Дата обращения: 27.09.2021)

5. Распознавание объектов на Python / Глубокое машинное обучение [Электронный ресурс] – URL: https://itproger.com/news/raspoznavanie-obaektov-na-python-glubokoe-mashinnoe-obuchenie (Дата обращения: 27.09.2021)

УДК 001.891.57:519.711

М. Р. ИБАТУЛЛИН, А. М. КУБЛИЦКАЯ, Р. Р. КАРИМОВ
ibatullin.m@gmail.com
Науч. руководи. – канд. техн. наук, доц. Р. Р. КАРИМОВ

Уфимский государственный авиационный технический университет

ПРИМЕНЕНИЕ ТЕХНОЛОГИИ ТЕЛЕПОРТАЦИИ ПРИ РАЗРАБОТКЕ ВИРТУАЛЬНОГО ТРЕНАЖЕРА ДЛЯ ПРОИЗВОДСТВЕННОГО ПЕРСОНАЛА

Аннотация. Рассматривается процесс телепортации в производственных помещениях, включая алгоритма взаимодействия оператора с неподвижным объектом в помещении.
***Ключевые слова*:** виртуальный тренажер; интерактивная графическая среда; производственный объект; телепорт; контроллер персонажа; контроллер столкновений; обработчик событий.

Введение

В настоящее время на производственных объектах организационно-технических систем подготовка персонала включает тренировку и аттестацию с применением виртуальных тренажеров. Для эффективного изучения технических процессов производственных объектов в виртуальных тренажерах необходима возможность быстрого перемещения по изучаемой локации.

Данная задача может решаться с помощью телепортации оператора (игрока).

Телепортация – быстрый перенос игрового персонажа из одной определенной точки виртуальной сцены в другую. Тренажер, в котором будет реализована телепортация, разработан на движке Unity3D. Unity3D – среда разработки трехмерных компьютерных игр с широкими возможностями программирования моделей движения объектов и физики их взаимодействия [2]. В тренажере реализована трехмерная модель производственного объекта, включая производственное здание и открытую площадку, переход персонажа между самыми дальними точками сцены представляет собой рутинную операцию и может занимать несколько минут. Для оперативного перемещения из производственного здания на открытую площадку и обратно требуется установить и настроить те-

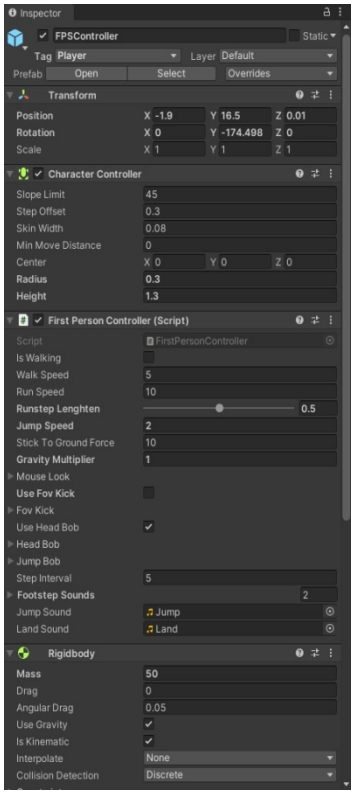
лепорты, ко-торые могут использоваться для отладки и тестирования (испытания) виртуального тренажера или иных целей.

Таким образом, целью работы является повышение эффективности разработки виртуального тренажера производственного объекта на основе технологии телепортации.

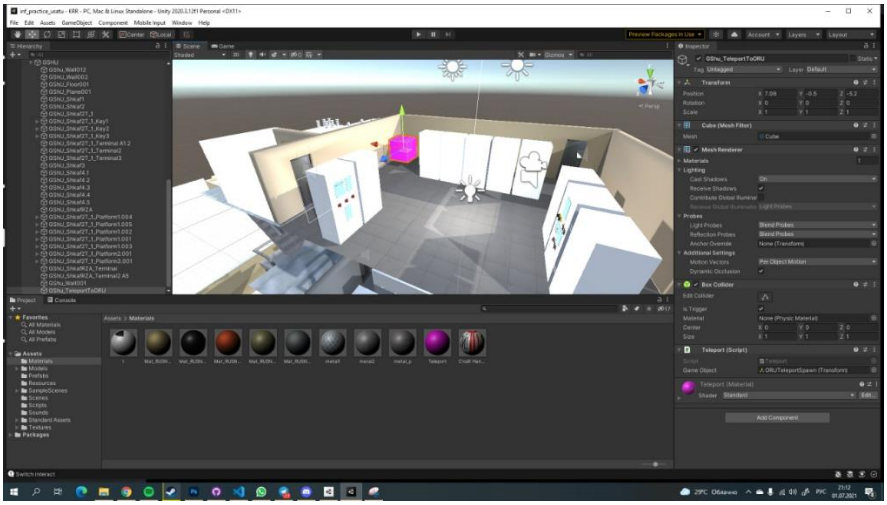
Решение поставленной задачи

Задача построения телепорта включает в себя следующие этапы: 1) настройка начальной и конечной точек телепортации (точка spawn); 2) разработка 3D модели телепорта; 3) разработка событийной модели телепорта и скрипта для переноса системы координат персонажа из начальной точки в конечную.

Устройство игрового персонажа в данном проекте представлено на рисунке 1а, одним из компонентов персонажа является Rigidbody, который отвечает за физические взаимодействия и необходим для реализации телепорта [2]. Для него нужно три компонента: скрипт, отвечающий за телепортацию, точка спавна (точка появления персонажа после телепортации), точка, откуда идет телепортация.



а



б

Рис. 1. Окно Инспектора (Inspector**) (**а**);** точка телепортации (б)

На рисунке 1б показано, как реализована точка телепортации. Упрощенная 3D модель телепорта построена в виде фиолетового куба.

Mesh render отвечает за отрисовку, box collider отвечает за фиксацию вхождения в зону коллайдера, material за цвет куба. Важным моментом является галочка на функции Is Trigger. Без нее скрипт работать не будет. Функция Is Trigger регистрирует столкновения с collider объекта [2].

Скрипт, который является компонентом телепорта, работает следующим образом: персонаж входит в коллайдер, и его координаты становятся равными координатам выбранного нами объекта. Код скрипта представлен на рисунке 2.

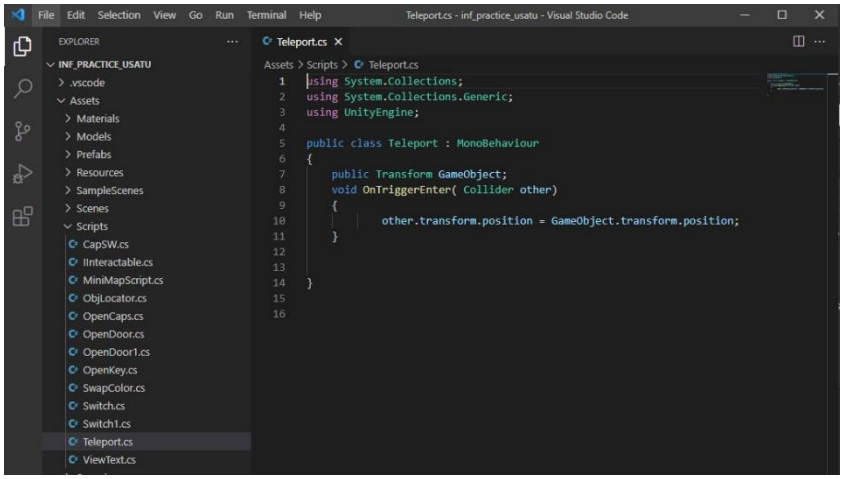


Рис. 2. Скрипт Teleport

Реализация точки спавна, которая представляет из себя пустой GameObject, представлена на рисунке 3. На рисунке 1б показано, что в окне инспектора, в скрипте, выбран ORUTeleportSpawn. Координаты этого объекта копирует скрипт.

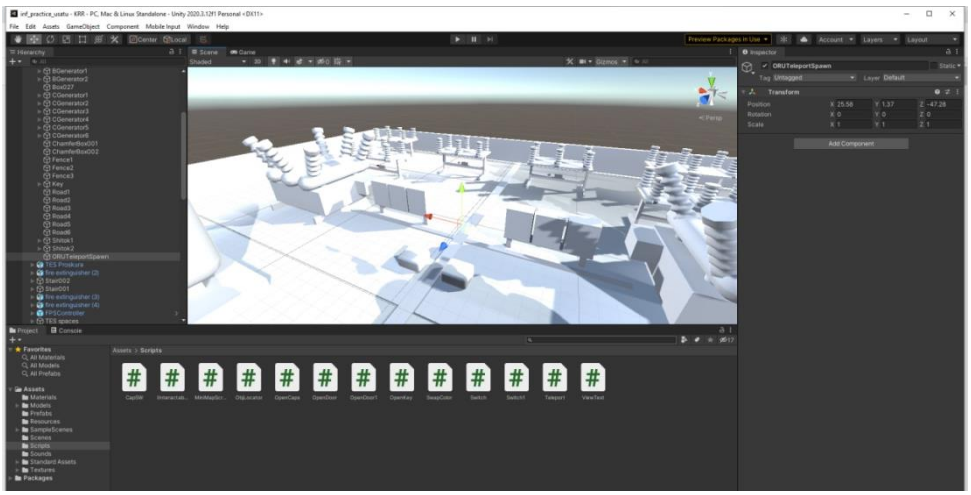


Рис. 3. Точка спавна

Выводы

В данном проекте была выполнена задача односторонней телепортации оператора в виртуальном тренажере, имитирующем модель реального производственного объекта. Метод решения задачи может быть использован для любого проекта, требующего телепортацию на одной сцене.

СПИСОК ЛИТЕРАТУРЫ

1.Каримов Р.Р., Кузьмина Е.А., Арсланов Т.Р., Макаев Р.А. Проектирование комплекса управления авиационно-космическими объектами на основе технологий смешанной реальности // Свободный полет-2018: сборник трудов всероссийской конференции. – Уфа-Жуковский, 2018. – С.73-75.
2.Руководство Unity URL: https://docs.unity3d.com/ru/530/Manual (дата обращения: 29.06.2021).

УДК 004.942

В. С. ИВАНОВА, Л. И. ШЕХТМАН
vika_ivanova290@mail.ru, lidia.shehtman@yandex.ru
Науч. руководд. – канд. физ.-мат. наук, доц. Л. И. ШЕХТМАН

Уфимский государственный авиационный технический университет

ИНФОРМАЦИОННО-АНАЛИТИЧЕСКАЯ ПОДДЕРЖКА ЦЕНООБРАЗОВАНИЯ ДЛЯ МАШИНОСТРОИТЕЛЬНОГО ПРЕДПРИЯТИЯ

Аннотация. Рассматривается проблема установления конкурентно способной цены на новое изделие с учетом цен на продукты-аналоге, имеющиеся на рынке. Для решения применяется метод анализа иерархий.
Ключевые слова: ценообразование; метод анализа иерархий.

Рассматривается предприятие, специализирующееся на разработке и производстве комплектующих изделий и агрегатов для авиации. Формированием цены на новое изделие занимается, в основном, планово-экономический отдел, но в этом процессе задействованы и другие отделы, предоставляющие информацию для расчета себестоимости изделия, и анализирующие рыночную ситуацию. Окончательное решение принимает руководитель предприятия. Данная статья посвящена разработке программной системы, способной оказать информационную поддержку руководителю при принятии решений по установлению цены на новое изделие. Целью является повышение качества процедуры принятия решений при выборе цены изделий за счет более полной и достоверной информационной поддержки на основе метода анализа иерархий.

Рисунок 1 демонстрирует факторы ценообразования факторы ценообразования, учитываемые при расчете нижней границы цены.

На рисунке 2 показана контекстная диаграмма информационной поддержки ценообразования на основе метода анализа иерархий. Исходными данными являются сведения о материалах, о технологиях, о продукта-аналогах, о производственном предприятии. В качестве результата выступает цена на новое изделие.

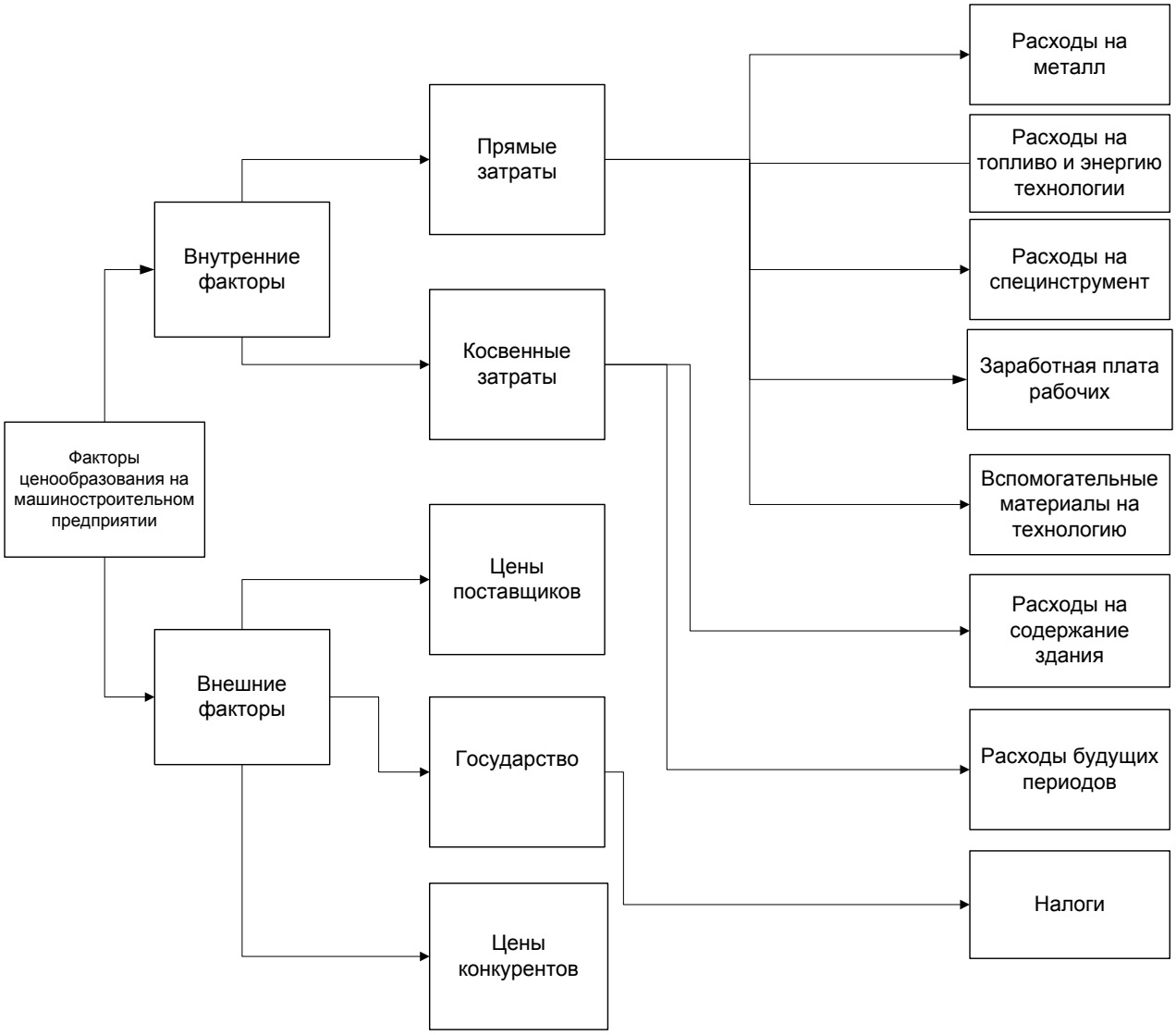


Рис. 1. Факторы ценоообразования

Цену на новое изделие устанавливает планово-экономический отдел, опираясь только на нижнюю границу цены: себестоимость + %надбавка. Предлагается рассчитывать верхнюю границу цены с помощью анализа качества и цен продуктов-аналогов, производимых конкурентами. В базе данных хранятся сведения о продуктах-аналогах, собранные менеджерами отдела снабжения. Расчет верхней границы цены планируется выполнять на основе метода анализа иерархии. Применение метода анализа иерархии позволяет рассчитать максимально возможную с учетом рыночной ситуации цену на новое изделие.

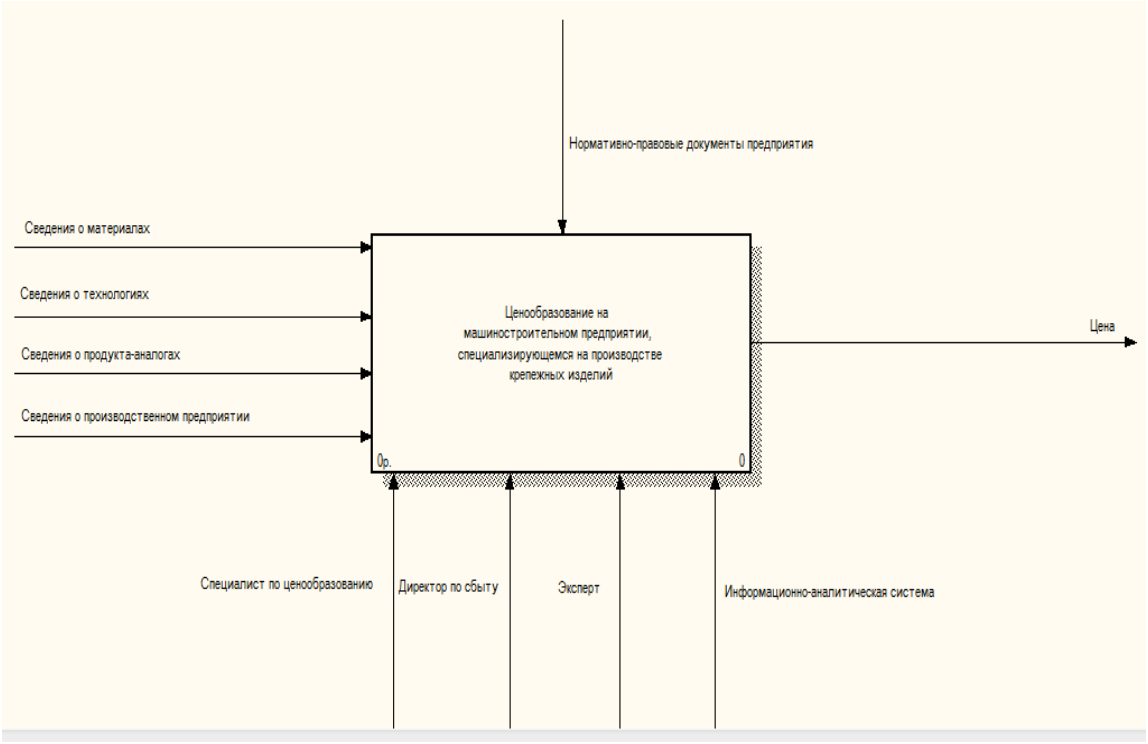


Рис. 2. Функциональная модель (0-й уровень)

Была построена математическая модель расчета цены на основе метода анализа иерархий.

m – число критериев; n – число альтернатив;

$F = \{f_i\}$ – множество критериев, $i = \overline{1,m}$;

$A = \{a_j\}$ – множество альтернатив, $j = \overline{1,n}$.

Матрица парных сравнений критериев: $Cf = \|Cf_{ij}\|$, где $i = \overline{1,m}$; $j = \overline{1,m}$.

Матрица парных сравнений альтернатив по критерию f_i:

$Ca^i = \|ca^i_{tk}\|$, где $t = \overline{1,n}$; $k = \overline{1,n}$; $i = \overline{1,m}$.

По каждой матрице парных сравнений вычисляются вектора $Y = (y_i)$, $i = \overline{1,l}$, где l – размерность матрицы парных сравнений.

Здесь $y_i = \sqrt[l]{\prod_{j=1}^{l} x_{ij}}$, где x_{ij} – элемент матрицы парных сравнений, $i, j = \overline{1,l}$.

Компоненты каждого вектора Y нормируются:

$S = \sum_{i=1}^{l} y_i$; $y_{n_i} = \frac{y_i}{S}$, $i = \overline{1,l}$.

Величины y_{n_i}, $i = \overline{1,l}$ принимаются в качестве коэффициентов важности (весов) элементов уровней иерархии. Обозначим коэффициенты важности критериев K_i, $i = \overline{1,m}$; а коэффициенты важности альтернатив по i-му критерию Ka^i_j, $j = \overline{1,n}$.

Для проверки согласованности суждений ЛПР по каждой матрице парных сравнений вычисляются:

$\mathrm{M}_j = \sum_{i=1}^{l} x_{ij}$, $j = \overline{1,l}$; $\lambda = \sum_{j=1}^{l} \mathrm{M}_j \cdot y_{m_j}$;

$I = \frac{\lambda - l}{l - 1}$ – индекс согласованности;

$\mathrm{T} = \frac{I}{R}$ – отношение согласованности, где R – значение индекса случайной согласованности.

Желательным считается уровень T<=0,1, иначе рекомендуется провести сравнения заново.

Результирующая оценка каждой альтернативы:

$$C_j = \sum_{i=1}^{m} \mathrm{K}_i Ka_j^i .$$

Альтернативы упорядочиваются по убыванию результирующих оценок.

Максимальная цена изделия рассчитывается по формуле:

$$\mathrm{Z}_1 = \frac{\sum_{j=2}^{n} C_j * \mathrm{Z}_j}{1 - C_1}.$$

Рисунок 3 демонстрирует схему алгоритма расчета максимально возможной цены изделия на основе метода анализа иерархий. Можно выделить следующие подзадачи:

– формирование списка оценивания продукции и списка альтернатив (оцениваемого продукта и продуктов-аналогов);

– попарные сравнения критериев и альтернатив;

– вычисление весов критериев и альтернатив;

– проверка согласованности суждений лица принимающего решения;

– вычисление результирующих оценок альтернатив;

– расчет цены оцениваемого продукта.

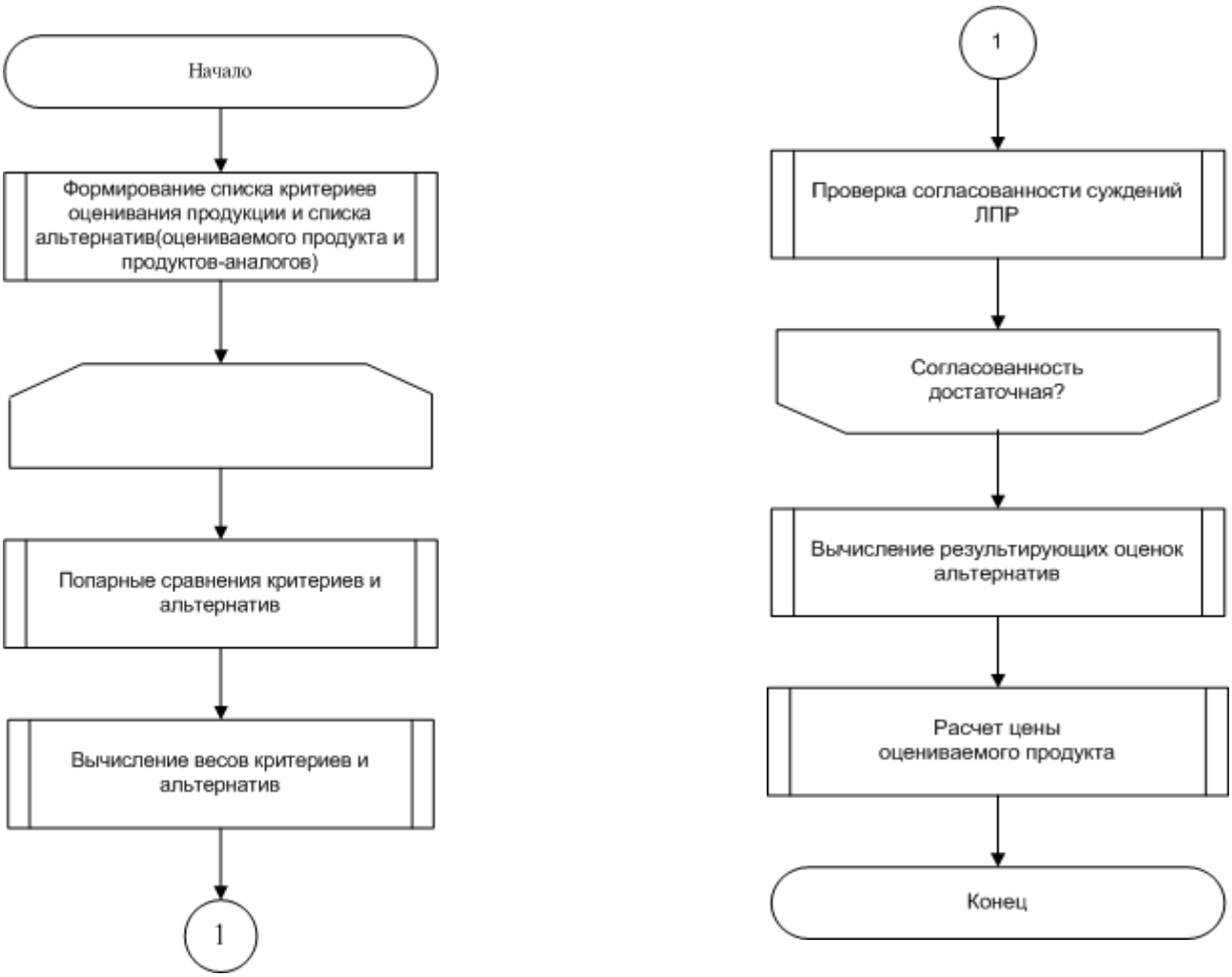


Рис. 3. Схема алгоритма расчета цены

Таким образом. ЛПР может при установлении цены опираться на две оценки: нижнюю (себестоимость + % надбавка) и верхнюю (рассчитанную с помощью метода анализа иерархий). Это способствует принятию более обоснованного решения.

СПИСОК ЛИТЕРАТУРЫ

1. Микони, С. В. Теория принятия управленческих решений : учебное пособие / С. В. Микони. — Санкт-Петербург : Лань, 2021. — 448 с. — ISBN 978-5-8114-1875-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/168845 (дата обращения: 02.09.2021). — Режим доступа: для авториз. пользователей.

УДК 681.518

В. С. ИВАНОВА, Р. Р. КАРИМОВ
vika_ivanova290@mail.ru, rikar@yandex.ru
Науч. руководов. – канд. техн. наук, доц. Р. Р. КАРИМОВ

Уфимский государственный авиационный технический университет

РАЗРАБОТКА БАЗЫ ДАННЫХ СЛОЖНОГО ИЗДЕЛИЯ С ПРИМЕНЕНИЕМ PDM-СИСТЕМЫ

Аннотация. Рассматривается процесс разработки базы данных сложного изделия на производственном предприятии с применением программного комплекса PDM STEP Suite.
Ключевые слова: информационная поддержка; база данных об изделии; PDM-система; изделие.

Введение

База данных об изделии (БДИ) создается на начальных стадиях жизненного цикла изделия и впоследствии широко используется на последующих стадиях жизненного цикла – проектирования, эксплуатации и утилизации изделия. БДИ является формой реализации электронного описания изделия [1] и составляет основу для построения автоматизированной системы управления данными об изделии, разработки электронного макета и структуры изделия, электронного дела (формуляра) изделия. БДИ применяется при решении разнообразных проектно-конструкторских, производственно-технологических и эксплуатационных задач.

БДИ создается с помощью системы управления данными об изделии – PDM-системы (Product data management). Примером PDM-системы является российский программный комплекс PDM STEP Suite (PSS).

Назначение PDM STEP Suite – собрать всю информацию об изделии в интегрированной базе данных (БД) и обеспечить совместное использование этой информации в процессах проектирования, производства и эксплуатации [2, 3].

В качестве примера сложного изделия рассматривается изделие ВСУ ТА-6А – вспомогательная силовая установка (базовая модификация), широкоис-

пользуемая на самолетах «ТУ», «ИЛ» и «АН». В качестве исходных данных использовано Руководство по технической эксплуатации [4].

Целью работы является повышение эффективности жизненного цикла изделия на основе информационной поддержки процесса разработки базы данных изделия в PDM-системе.

Рассматриваемая задача декомпозируется на следующие подзадачи:

1) создание базы данных, ввод организационной структуры предприятия и настройка словарей в БДИ;

2) создание электронной структуры изделия и описание его характеристик;

3) создание экземпляров изделия.

Решение поставленных задач

Задача 1. Создание базы данных, организационной структуры предприятия и настройка словарей в БДИ.

Прежде чем начать разработку БДИ в модуле PDM, необходимо произвести настройку, которая осуществляется с помощью различных модулей PSS. Настройка производится под специфику конкретного предприятия.

Шаг 1. Создаем БД в модуле Настройка локальных БД (Рисунок 1).

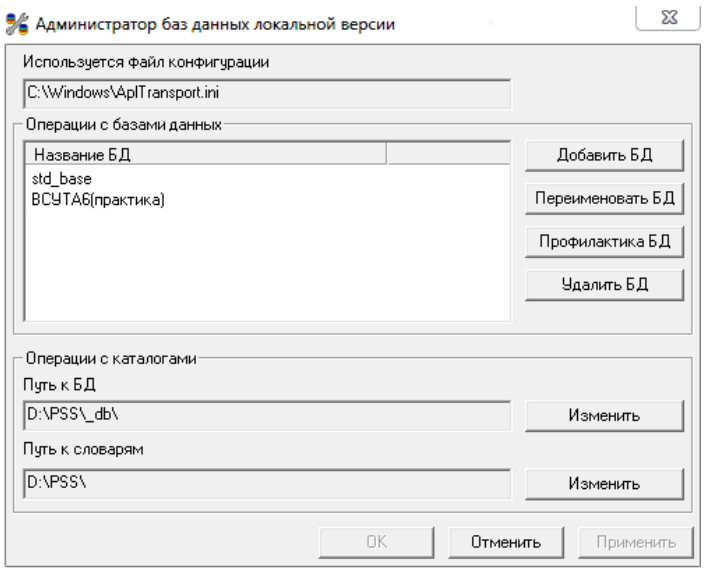


Рис. 1. Создание БД

Шаг 2. Вводим организационную структуру предприятия, настраиваем словари в новой БД.

К редко изменяющейся (статической) информации об изделии можно отнести:

– организационную структуру предприятия;

– характеристики/группы характеристик и единицы измерения;

– типы характеристик.

Всю информацию можно ввести в модуле Настройка словарей БД (Рисунок 2Рис. , Рисунок 3, Рисунок 4).

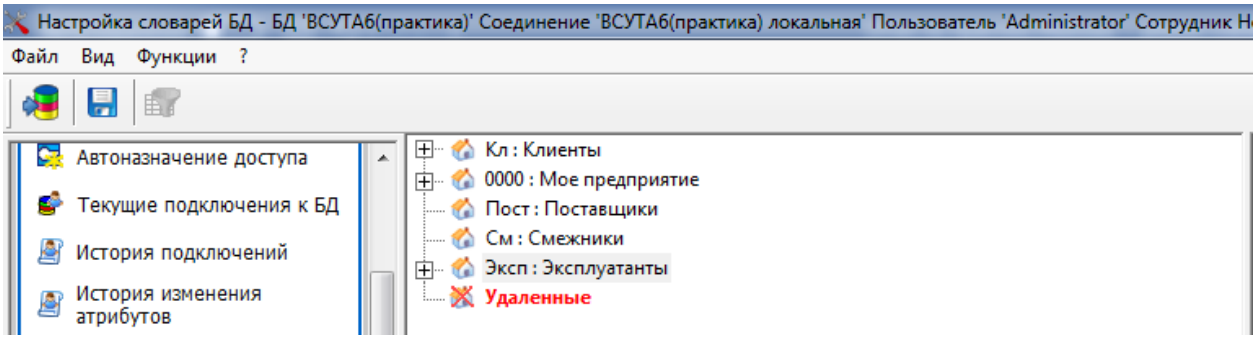


Рис. 2. Настройка организационной структуры

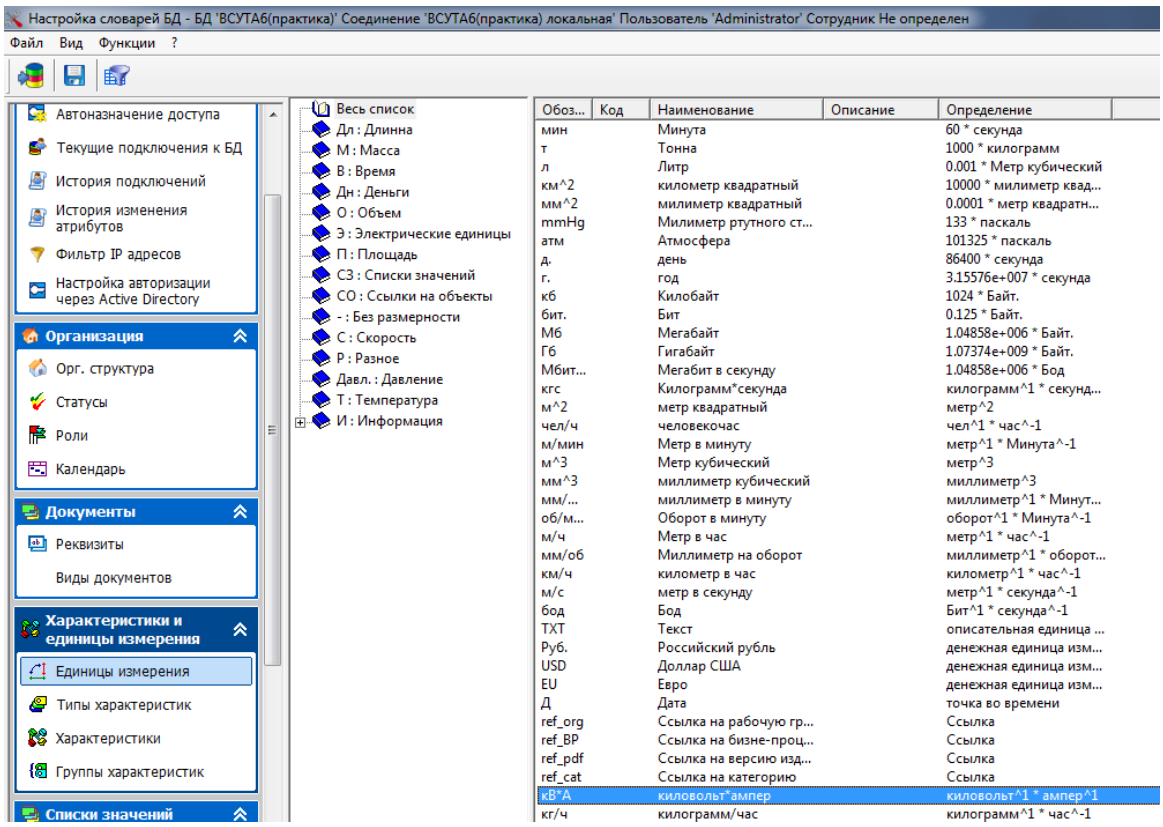


Рис. 3. Настройщик словарей БД в режиме редактирования единиц измерения

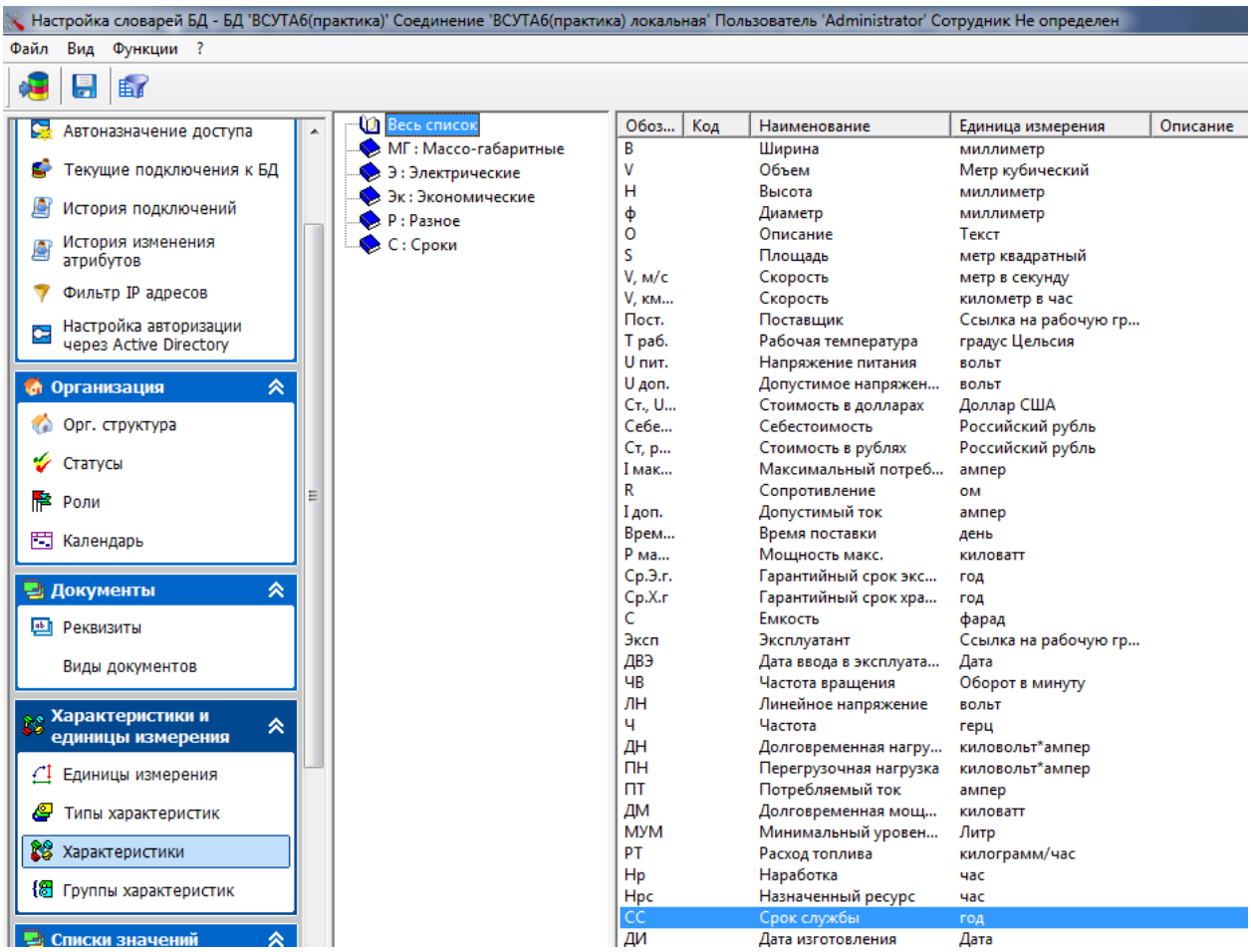


Рис. 4. Настройщик словарей БД в режиме редактирования характеристик

Для обеспечения доступа удаленных пользователей БДИ может быть размещена на Web-сервере, средства администрирования PSS позволяют обеспечить защиту и разграничение прав доступа пользователей к данным.

Задача 2. Описание структуры изделия и его характеристик.

В модуле PDM необходимо построить электронное описание структуры (состав) изделия. Структура изделия – перечень данных, описывающих то, из каких составных частей, узлов, деталей состоит изделие. К структуре изделия можно также отнести информацию о том, из каких материалов изготовлены детали и какие материалы входят в состав изделия, а также его различные характеристики [3] (Рисунок 5).

Рис. 5. Структура изделия и его характеристики

Одной из важных проектно-конструкторских задач является определение массы и стоимости всего изделия на основе соответствующих характеристик множества входящих в его состав узлов и деталей (Рисунок 6).

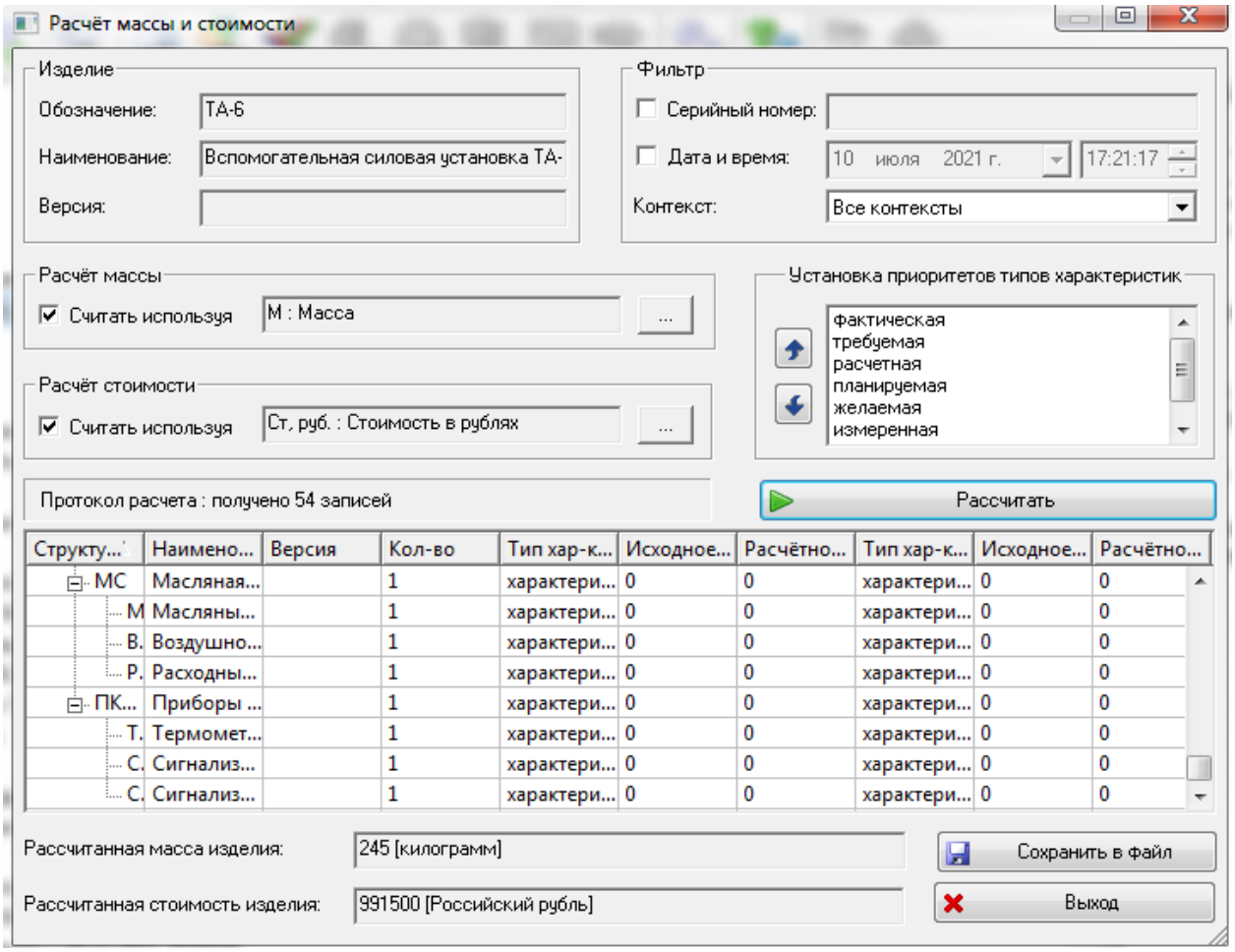


Рис. 6. Анализ массы и стоимости

Задача 3. Работа с экземплярами изделия.

При эксплуатации изделия для его описания используется такое понятие, как экземпляр изделия, у каждого из которых должен быть свой электронный формуляр (паспорт) изделия – с ним ассоциируется вся информация о параметрах и истории экземпляра изделия (Рисунок 7).

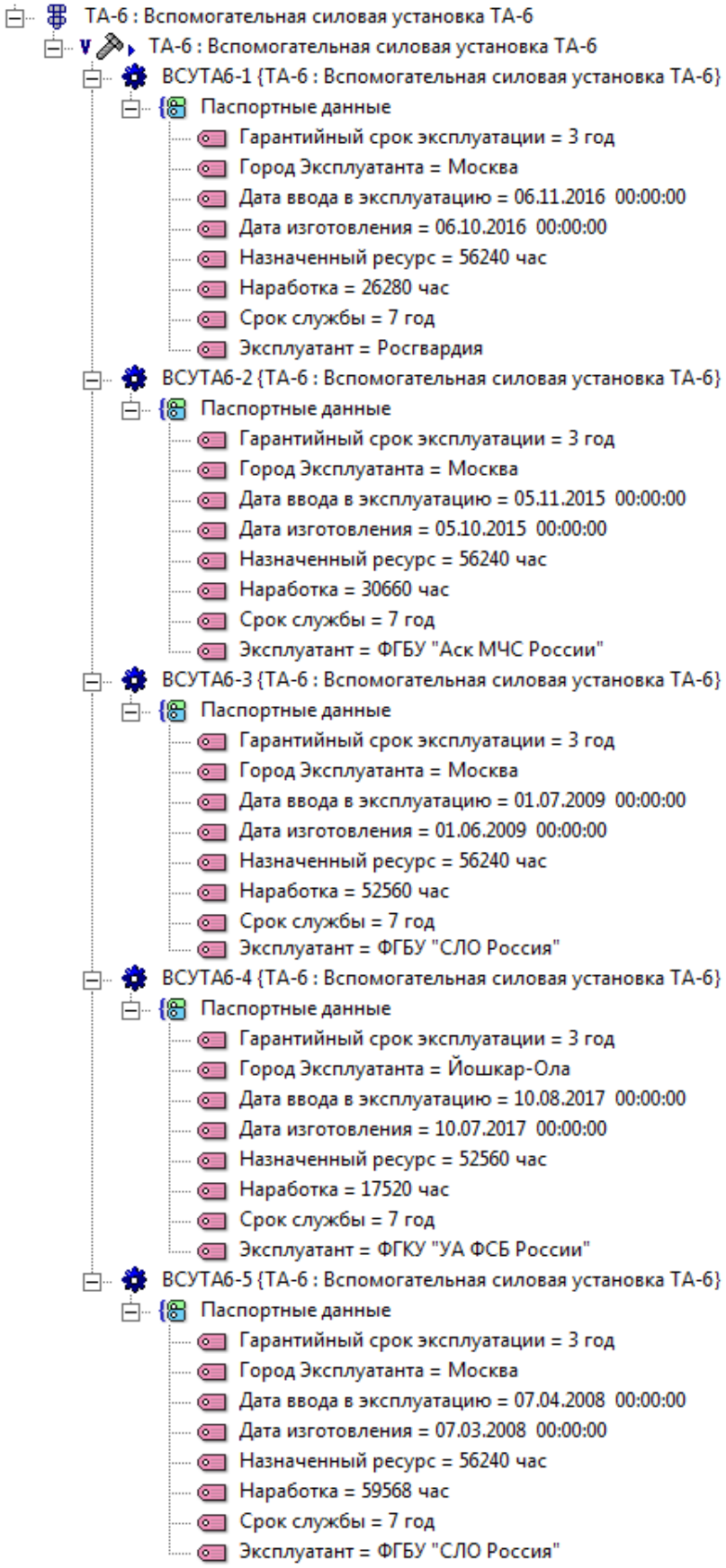


Рис. 7. Экземпляры изделия

Заключение

В ходе разработки БДИ рассмотрено решение следующих задач:

1) создание базы данных, ввод организационной структуры и настройка словарей в БДИ;

2) описание структуры изделия и его характеристик;

3) описание экземпляров изделия.

Разработанная БДИ может быть использована для решения разнообразных проектно-конструкторских, производственно-технологических и эксплуатационных задач, в т.ч. может быть обеспечена совместная работа различных служб в процессах проектирования, производства и эксплуатации изделия с целью оперативного получения информации об изделии. Система PDM STEP Suite позволяет повысить эффективность информационной поддержки ЖЦИ.

СПИСОК ЛИТЕРАТУРЫ

1. ГОСТ 2.053-2013. ЕСКД. ЭЛЕКТРОННОЕ ОПИСАНИЕ ИЗДЕЛИЯ.
2. Системы информационной поддержки жизненного цикла космических аппаратов: [учебное пособие] / Р. Р. Каримов, Н. В. Кондратьева ; ФГБОУ ВПО УГАТУ .— Уфа: УГАТУ, 2008 .— 154 с.
3. PDM Step Suite. [Электронный ресурс]. URL: http://cals.ru/products/pss (дата обращения: 15.08.2021).
4. Двигатель ТА6А.000.000 РЭ (049.00.00). Руководство по технической эксплуатации. – ООО «Авиа-Медиа», 2002-2007. — 396 с.

УДК 519.87

М. А. ИВАНОВ, Д. В. ШЛЁНКИН, В. А. ГЛУЩЕНКО, А. В. ШУНДЕЕВ
aa4052783@gmail.com, kot.dima2011@yandex.ru, val_g_2001@bk.ru, artem_shundeev@mail.ru.
Науч. руководитель – канд. техн. наук, проф. А. С. КОВТУНЕНКО.

Уфимский государственный авиационный технический университет

ИНФОРМАЦИОННАЯ ПОДДЕРЖКА ПРОЦЕССА ПОИСКА ЗАКАЗОВ НА БИРЖЕ ФРИЛАНСЕРОВ

Аннотация. Рассматривается информационная поддержка процесса поиска предложений на различных биржах фрилансеров путем создания многофункционального инструмента с набором настраиваемых фильтров.
***Ключевые слова*:** сбор данных; биржа фрилансеров; веб-программирование; фильтрация данных; база данных; разработка дизайна сайта.

Актуальность работы

Биржа фрилансеров – это сервисы, чаще всего в виде веб-приложений, которые предлагают услуги по размещению задач различных тематик и направлений, а также по поиску исполнителей для размещенных заказов (Рис.1).

Фрилансер – свободный работник, который, чаще всего, предлагает свои услуги на биржах фрилансеров.

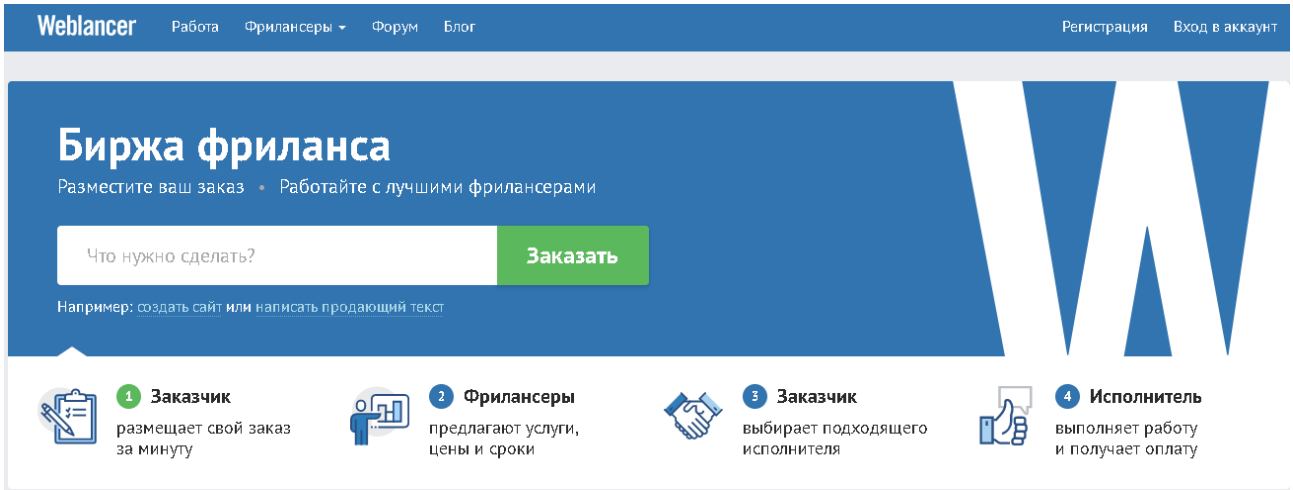


Рис. 1. Пример бирж фриналсеров

Основной проблемой фрилансеров, которые занимаются этой деятельностью на постоянной основе, является то, что для извлечения большей прибыли требуется осуществлять мониторинг заказов сразу на нескольких биржах, при

этом, вероятно, приходиться отслеживать различные категории и подкатегории заказов. Чтобы облегчить и оптимизировать данный процесс требуется создать удобный инструмент, который обеспечит фрилансера нужной для него информацией о заказах.

Конкурентные особенности

Изучая аналогичные варианты инструментов, удалось установить, что ключевой конкурентной особенностью проекта является набор фильтров, который способен удовлетворить запросы пользователей. Также плюсом разрабатываемого инструмента является система трендов заказов, которая будет располагать информацией о самых свежих задачах.

Этапы разработки инструмента

Было принято решение создать инструмент в виде веб-приложения.

Процесс разработки был разбит на следующие этапы:

1. Организация серверной части
2. Сбор данных о заказах
3. Организация и подключение базы данных
4. Создание дизайна
5. Создание фильтров

Стек технологий

Язык программирования Python – высокоуровневый язык программирования общего назначения с динамической строгой типизацией и автоматическим управлением памятью, ориентированный на повышение производительности разработчика, читаемости кода и его качества, а также на обеспечение переносимости написанных на нем программ.

Flask – фреймворк для создания веб-приложений на языке программирования Python.

PostgreSQL – свободная объектно-реляционная система управления базами данных.

Организация серверной части

С использованием фреймворка Flask реализована индексация страниц инструмента. При переходе по определенному адресу, приложение отрисовывает соответствующий html-шаблон (Рис. 2).

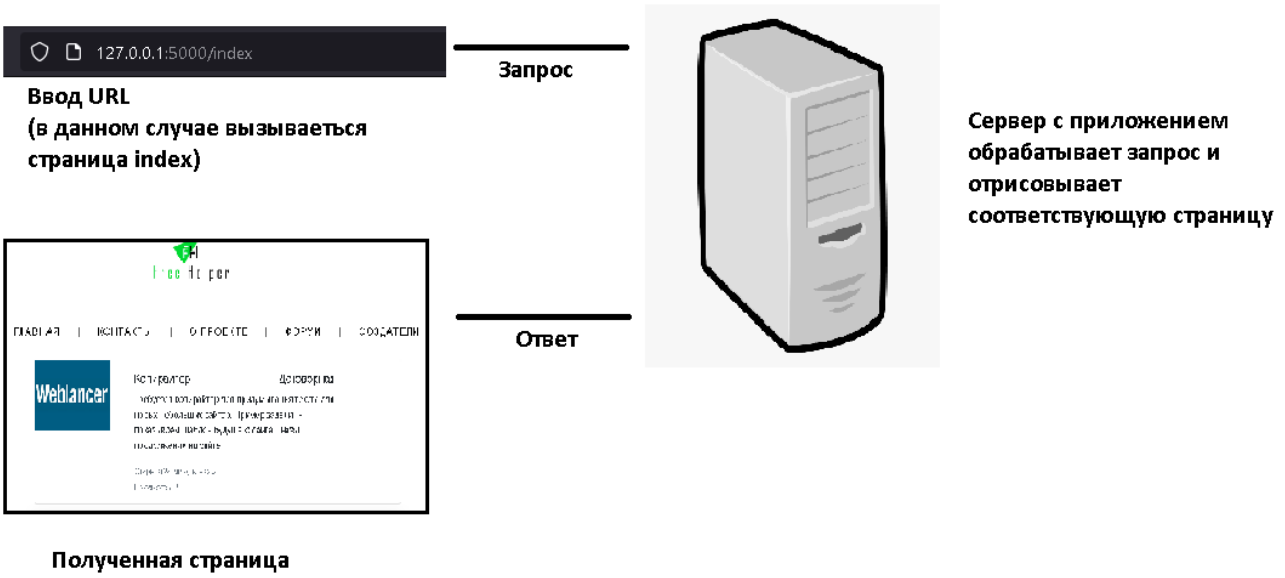


Рис. 2. Схема индексации страниц

Сбор данных о заказах

Парсинг — это процесс автоматического сбора данных и их структурирования. Парсинг обычно применяют, когда нужно быстро собрать большой объем данных. Его выполняют с помощью специальных сервисов — парсеров.

Для извлечения нужной информации, парсер скачивает html-код заданной страницы и преобразует ее в специальный объект, который называется «soup». В этом объекте определяются и считываться сегменты, в которых содержаться нужная информация. В данном случае парсер считывает цену, адрес, время и текст заказа.

Организация и подключение базы данных

В данном приложении база данных необходима для структурирования полученных данных, а также для их эффективного использования. Для удобства создания использовалось приложение pgAdmin 4. В данной базе данных содержится таблица с следующими столбцами:

1. Order_id – содержит уникальный идентификационный номер строки.

2. Order_name – содержит заголовок заказа.

3. Order_link – содержит адрес на страницу заказа.

4. Order_text – содержит краткое описание заказа.

5. Order_price – содержит вознаграждение за выполнение заказа.

6. Order_view – содержит количество просмотров на карточке заказа.

7. Order_status – содержит информацию о статусе заказа.

8. Order_time – содержит дату, когда был опубликован заказ.

Data Output | Explain | Messages | Notifications

	order_id integer	order_name character varying (200)	order_link character varying (400)	order_text character varying (3000)	order_price character varying (40)	order_view character varying (40)	order_status character varying (300)	order_time character varying (300)
1	52	Копирайтер	https://www.weblancer.net//v...	Требуется копирайтер для пр...	Договорная	2	Открыта 24 минуты назад	24 минуты назад
2	53	Добавление интеграций в м...	https://www.weblancer.net//pr...	Разрабатываем приложение ...	Договорная	0	Открыт 5 часов назад	5 часов назад
3	54	Озвучить видео на английск...	https://www.weblancer.net//pr...	Нужно весело и энергично оз...	$80	42	Открыт 4 дня назад	4 дня назад
4	55	Разработка админки на Yii2	https://www.weblancer.net//pr...	Требуется собрать веб-систе...	$1350	4	Открыт 5 дней назад	5 дней назад
5	56	Ищу профессионального ре...	https://www.weblancer.net//v...	Ищу профессионального ред...	Договорная	6	Открыта 6 дней назад	6 дней назад
6	57	Требуется парсер (на посто...	https://www.weblancer.net//v...	Подробности: ссылка... продо...	Договорная	7	Открыта 6 дней назад	6 дней назад
7	58	UI дизайн semi-casual игры.	https://www.weblancer.net//c...	Здравствуйте, друзья!	$400	16	Открыт 12 дней назад	12 дней назад
8	59	Сделать курсовую работу (...	https://www.weblancer.net//pr...	Курсовая работа по дисципл...	Договорная	8	Открыт 12 дней назад	12 дней назад
9	60	Telegram бот (работа с API +...	https://www.weblancer.net//pr...	Суть проекта:	Договорная	16	Открыт 12 дней назад	12 дней назад
10	61	Скрипт для тильды	https://www.weblancer.net//pr...	Нужен скрипт для тильды. За...	$10	4	Открыт 14 дней назад	14 дней назад
11	62	Ищу постоянного подрядчи...	https://www.weblancer.net//v...	В связи с перегрузом моей ко...	Договорная	8	Открыта 15 дней назад	15 дней назад
12	63	Разработка логотипа и фир...	https://www.weblancer.net//pr...	Здравствуйте, уважаемые ис...	$110	116	Открыт 16 дней назад	16 дней назад
13	64	Согласно алгоритму написа...	https://www.weblancer.net//pr...	Согласно алгоритму написат...	$25	7	Открыт 18 дней назад	18 дней назад
14	65	Художник-иллюстратор на к...	https://www.weblancer.net//v...	Требуется человек, который ...	$550	45	Открыта 20 дней назад	20 дней назад
15	66	Дописывать приложение дл...	https://www.weblancer.net//pr...	Помощь в написании новых ...	Договорная	8	Открыт 22 дня назад	22 дня назад
16	67	Дизассемблер прошивки s...	https://www.weblancer.net//pr...	Нужно помощь в внесении и...	Договорная	2	Открыт 22 дня назад	22 дня назад
17	68	C# Developer - Vote Bot / Auto...	https://www.weblancer.net//pr...	Привет,	Договорная	6	Открыт 23 дня назад	23 дня назад
18	69	Прием платежей через p2p	https://www.weblancer.net//pr...	Добрый день!	Договорная	8	Открыт 27 дней назад	27 дней назад
19	70	Дейтаграмные сокеты. Прог...	https://www.weblancer.net//pr...	На основе примеров програм...	Договорная	3	Открыт 28 дней назад	28 дней назад
20	71	Полное создание видео ,вме...	https://www.weblancer.net//pr...	Полное создание видео ,вмес...	Договорная	0	Открыт 8 минут назад	8 минут назад

Рис. 3. Визуальное представление таблицы из базы данных

Созданную базу данных требуется подключить как к основному приложению, для извлечения данных, так и к парсеру. Для этого используется библиотека psycopg2, которая организует подключение к базе данных и отправление команд.

Создание дизайна

Для создания шаблона используются HTML5 и CSS.

HTML – стандартизированный язык разметки документов для просмотра веб-страниц в браузере. Веб-браузеры получают HTML документ от сервера по протоколам HTTP/HTTPS или открывают с локального диска, далее интерпретируют код в интерфейс, который будет отображаться на экране монитора.

CSS – формальный язык описания внешнего вида документа (веб-страницы), написанного с использованием языка разметки.

Помимо стандартных тегов шаблон содержит элементы кода Python, который внедрен с помощью Jinja. Данное решение используется для того, чтобы автоматически заполнять название страницы, ее заголовок и элементы меню.

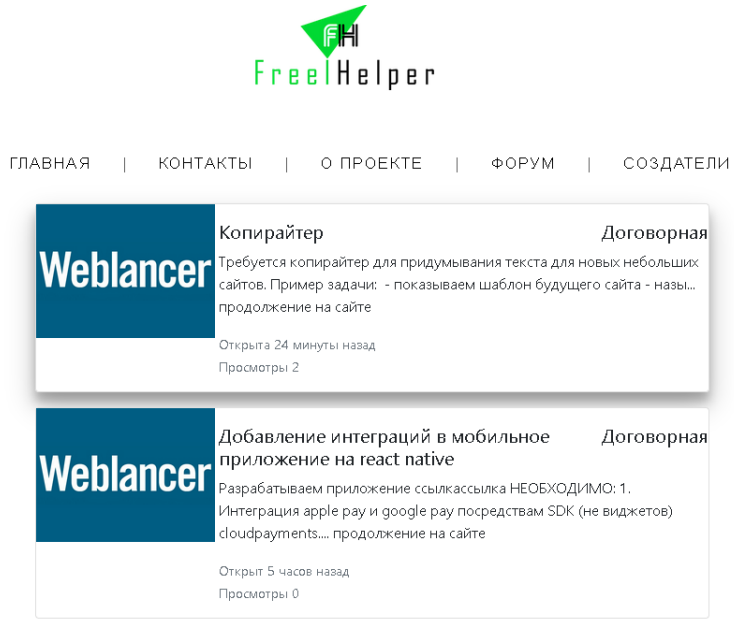


Рис. 4. Пример дизайна шаблона

Предоставлять информацию о заказах было запланировано в специальных картах. Карта заказа состоит информации, которую необходимо автоматически извлекать. Для этого используется шаблон разметки с внедренным кодом Python, в который циклические заполняются категории соответствующими данными.

Рис. 5. Пример дизайна карты заказа

Создание фильтров

Фильтр располагает следующими функциями:

1. Фильтрация по области заказа

2. Фильтрация по категории заказа

3. Фильтрация по стоимости заказа

4. Фильтрация по времени публикации заказа

5. Фильтрация по сервисам, на которых публиковался заказ

6. Фильтрация по количеству просмотров заказа

Данный набор фильтров основан на ранее собранной информации, он позволит исполнителю быстро находить желаемые заказы.

Анализ проделанной работы

Текущая версия проекта способна обеспечить удобный и оптимизированный мониторинг заказов с различных площадок, используя фильтры по категориям, времени и предлагаемой сумме оплаты труда. Веб-приложение способно сократить время поиска заказа и исключит неудобство мониторинга нескольких бирж.

СПИСОК ЛИТЕРАТУРЫ

1. Документация фреймвор Flask URL: https://flask.palletsprojects.com/en/2.0.x/
2. Ч. Муссиано, Б Кеннеди — HTML & XHTML. Подробное руководство.
3. Дронов.В.- HTML.5.CSS.3.и.Web 2.0.Разработка.современных.Web-сайтов.
4. Эрик Мэтиз. Изучаем Python. Программирование игр, визуализация данных, веб-приложения.
5. Italo Maia. Building Web Applications with Flask 2015.
6. Документация Jinja URL: https://jinja.palletsprojects.com/en/3.0.x/
7. Документация psycopg 2 URL: https://www.psycopg.org/docs/
8. Основы web-дизайна, Методика проектирования, Учебное пособие, Нагаева И.А., Фролов А.Б., Кузнецов И.А., 2021.
9. Ричард Лоусон Веб-парсинг на Python
10. Майкл Хидт «Поваренная книга» парсинга на Python

УДК 519.25

Г. И. МАСНАБИЕВА
guzel-04@mail.ru
Науч. руководов. – проф., д-р техн. наук С. С. ВАЛЕЕВ

Уфимский государственный авиационный технический университет

ИНФОРМАЦИОННО-АНАЛИТИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ПРОЦЕССА ПОДГОТОВКИ КОМПЛЕКСНОГО АНАЛИЗА РЕЗУЛЬТАТОВ ОБРАБОТКИ ДАННЫХ ЛЕТНЫХ ИСПЫТАНИЙ

Аннотация. Объектом исследования является система комплексного анализа динамических процессов с параметрами, являющаяся частью системы послеполетной обработки и анализа динамических процессов.
Ключевые слова: организационно-техническая система; летные испытания, внешние воздействующие факторы; система комплексного анализа данных; сценарий комплексного анализа.

Актуальность

На техническое состояние летательного аппарата в значительной мере оказывают влияние условия эксплуатации авиационной техники как на земле, так и в полете. Для исследования влияния внешних воздействующих факторов (ВВФ) проводят физический эксперимент в полете и изучают на основе полученных результатов эксперимента закономерности взаимодействия воздушного судна с окружающей ее средой, с различными полями Земли и (или) воздействия данной среды и этих полей на экипаж, а также на бортовое оборудование летательного аппарата.

При исследовании ВВФ необходимо проводить оценку реально действующих на аппаратуру и изделие уровней ВВФ с целью:

– обеспечения требуемой прочности и устойчивости аппаратуры и изделий к воздействию ВВФ;

– разработки новой и корректировки действующей нормативно-технической документации, устанавливающей требования и нормы при испытаниях аппаратуры и изделий на воздействие ВВФ.

В данной работе рассматриваются организационные принципы работы системы комплексного анализа, его функциональные возможности.

Система разработана для исследования влияния ВВФ, массовой обработки, анализа и обобщения больших объемов измерительной информации и обеспечивает эффективное решение задач по авиационной тематике: оценка уровней вибрации элементов конструкции летательного аппарата и его бортового оборудования; анализ виброхарактеристик авиационных двигателей; исследование смешанных вибропроцессов; оценка прочностных характери-стик летательного аппарата; исследование ударных и взрывных процессов (воздействие стрельбы на работу бортового оборудования и прочее); иссле-дование пульсаций давления, вибраций на беспилотном летательном аппара-те, угловых колебаний; оценка метрологических характеристик бортовой ап-паратуры; обобщение вибрационной и акустической информации по типам воздушных судов, по режимам полета, динамическим зонам летательного аппарата с целью прогнозирования и разработки нормативов.

Постановка задачи

Цель работы – повышение эффективности процесса обработки и комплексного анализа материалов летных испытаний на основе информационно-аналитического обеспечения подпроцесса подготовки сценария комплексного анализа.

Для достижения цели необходимо разработать системные модели, выполнить программную реализацию.

Системные модели процесса

Функциональная модель процесса обработки и комплексного анализа материалов летных испытаний, разработанная на основе технологии IDEF0 [1], представлена на рис. 1.

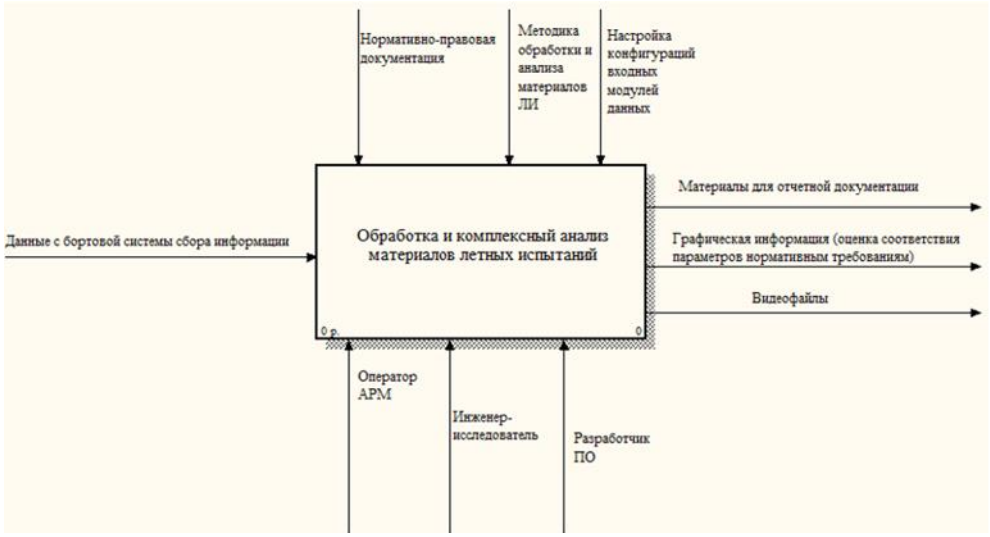


Рис. 1. Контекстная диаграмма процесса обработки и комплексного анализа материалов летных испытаний

При декомпозиции блока «Обработка и комплексный анализ материалов летных испытаний» функциональной модели можно представить в виде трех блоков: «Подготовка данных к экспорту в систему комплексного анали-за», «Подготовка сценария комплексного анализа» и «Комплексный анализ данных»(рис.2).

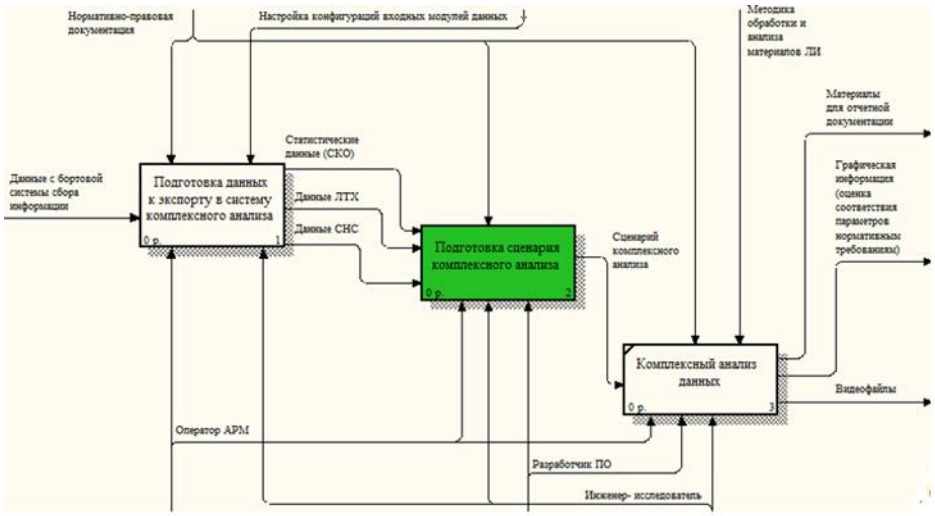


Рис. 2. Диаграмма декомпозиции процесса обработки и комплексного анализа материалов летных испытаний

Программная реализация процесса

Реализация процесса подготовки сценария комплексного анализа выполнена в виде программного обеспечения, разработанное на языке программирования Delphi в среде Embarcadero RAD Studio.

Embarcadero RAD (Rapid Application Development) Studio – среда быстрой разработки приложений фирмы Embarcadero Technologies, работающая под Windows. RAD позволяет создать различные виды программ: консольные приложения, оконные приложения, приложения для работы с Интернетом и базами данных [2].

Разработанное информационно-аналитическое обеспечение выполняет следующие функции: использование системных средств для задания путей доступа и имен файлов; проверка корректности вводимых имен папок и файлов; сохранение сформированного сценария комплексного анализа в текстовом формате; чтение ранее сформированного сценария комплексного анализа с целью корректировки и сохранения с изменениями; очистка всех элементов для последующего формирования нового сценария комплексного анализа.

Выполнены эксперименты в среде системы комплексного анализа (рис.3). В работе программы не было выявлено критических сбоев и неожиданных ошибок.

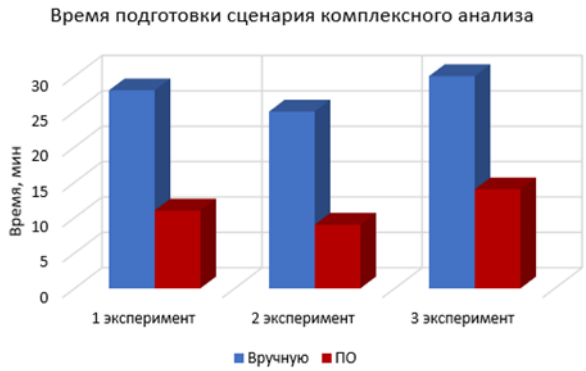


Рис. 3. Гистограмма времени подготовки сценария комплексного анализа

Таким образом, проведение экспериментов показало, что ПО, разработанное в рамках данной работы, уменьшает время подготовки сценария комплексного анализа в среднем на 58% и исключает появление ошибок.

СПИСОК ЛИТЕРАТУРЫ

1. Мартыненко, С.А. Управление потоками работ. Функциональное моделирование и основы управления проектами / С.А. Мартыненко. – СПб.: ГУАП, 2011. – 80 с.
2. [Электронный ресурс]. URL: www.embarcadero.com Дата обращения: (19.03.2021)

УДК 681.518 (075.8)

Д. А. МУХАМЕТГАЛИНА, Р. Р. КАРИМОВ
disha1904@yandex.ru, rikar@yandex.ru
Науч. руководов. – канд. техн. наук, доц. Р. Р. КАРИМОВ

Уфимский государственный авиационный технический университет

ИНФОРМАЦИОННАЯ ПОДДЕРЖКА КОНСТРУКТОРСКО-ТЕХНОЛОГИЧЕСКОГО ОБЕСПЕЧЕНИЯ ИЗДЕЛИЯ (УПРАВЛЕНИЕ ПОТОКАМИ РАБОТ НА ОСНОВЕ ТЕХНОЛОГИИ WORKFLOW)

Аннотация. Рассматриваются процессы управления жизненным циклом сложного изделия в PDM - системе на примере процесса конструкторско-технологического обеспечения изделия на производственном предприятии.
Ключевые слова: PDM STEP Suite; исполнители; шаблоны процессов; редактор шаблонов процессов; проектирование; подпроцесс; управление жизненным циклом; контроль сроков выполнения.

Введение

В процессе проектирования сложного изделия необходимо контролировать работы, связанные с конструкторско-технологическим обеспечением изделия. В настоящее время существенное внимание уделяется автоматизации конструкторско-технологических работ. Для решения подобного рода задач широко применяются не только CAD/CAM/CAE-системы, но системы управления данными об изделии, т.н. PDM-системы (Product data management). Примером PDM-системы является российский программный комплекс PDM STEP Suite (PSS).

PDM STEP Suite – это компьютерная система, предназначенная для управления данными о машиностроительном изделии на всех стадиях жизненного цикла изделия (ЖЦИ). Назначение PDM STEP Suite – собирать информацию об изделии в интегрированной базе данных (БД) и обеспечивать совместное использование этой информации в процессах проектирования, производства и эксплуатации.

В состав программного комплекса PSS помимо основного модуля PDM также входят «Редактор шаблонов процессов» и подсистема «PSS WorkFlow»,

которые позволяют разрабатывать модели процессов на различных стадиях жизненного цикла изделия, а также запускать и контролировать выполнение процессов.

На многих предприятиях с высоким уровнем автоматизации проектно-конструкторских и технологических работ схема взаимодействия отделов предприятия может быть описана следующим образом (рис.1).

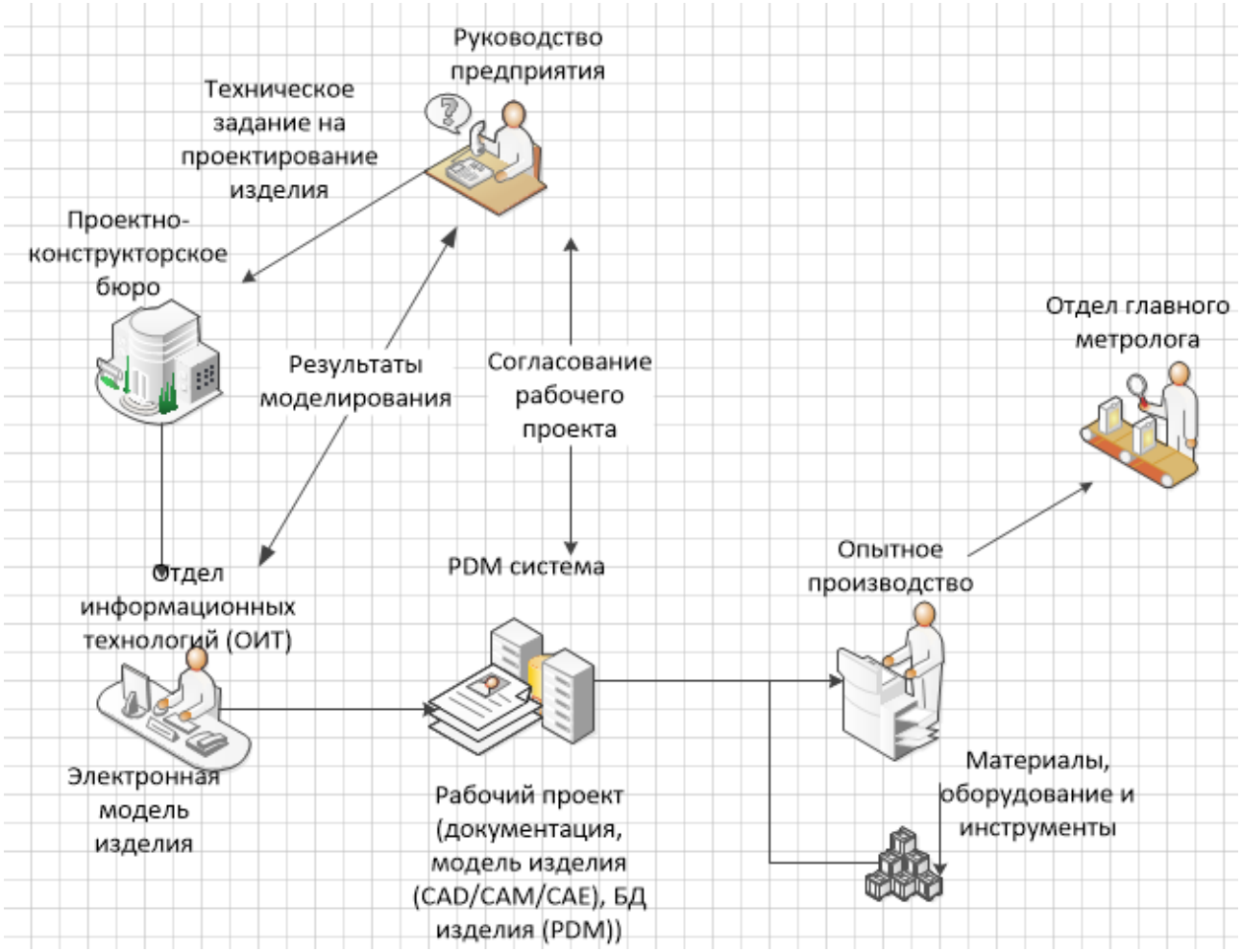


Рис. 1. Схема взаимодействия отделов предприятия в процессе конструкторско-технологического обеспечения производства

На предприятие поступает заказ на изготовление изделия. Руководство передает техническое задание на изготовление изделия в проектно-конструкторское бюро, которое формирует технический проект и передает его в отдел информационных технологий для моделирования изделия. При этом отдел информационных технологий предоставляет результаты моделирования руководству.

После отработки электронной модели создается рабочий проект, который согласовывается с руководством предприятия и заказчиком. После согласования с заказчиком рабочий проект предается в опытное производство. Далее изготовленное изделие передается в отдел главного метролога, в котором производятся контрольные измерения.

Постановка задачи

Целью работы является повышение эффективности проектирования изделия на основе информационной поддержки конструкторско-технологического обеспечения, включающего управление потоками проектно-конструкторских и технологических работ.

Для достижения цели необходимо разработать модели процессов управления жизненным циклом изделия и провести эксперимент по запуску процесса конструкторско-технологического обеспечения изделия.

Системные модели процесса

Функциональная модель процесса управления единым конструкторско-технологическим обеспечением изделия, разработанная на основе технологии IDEF0, представлена на рис. 2.

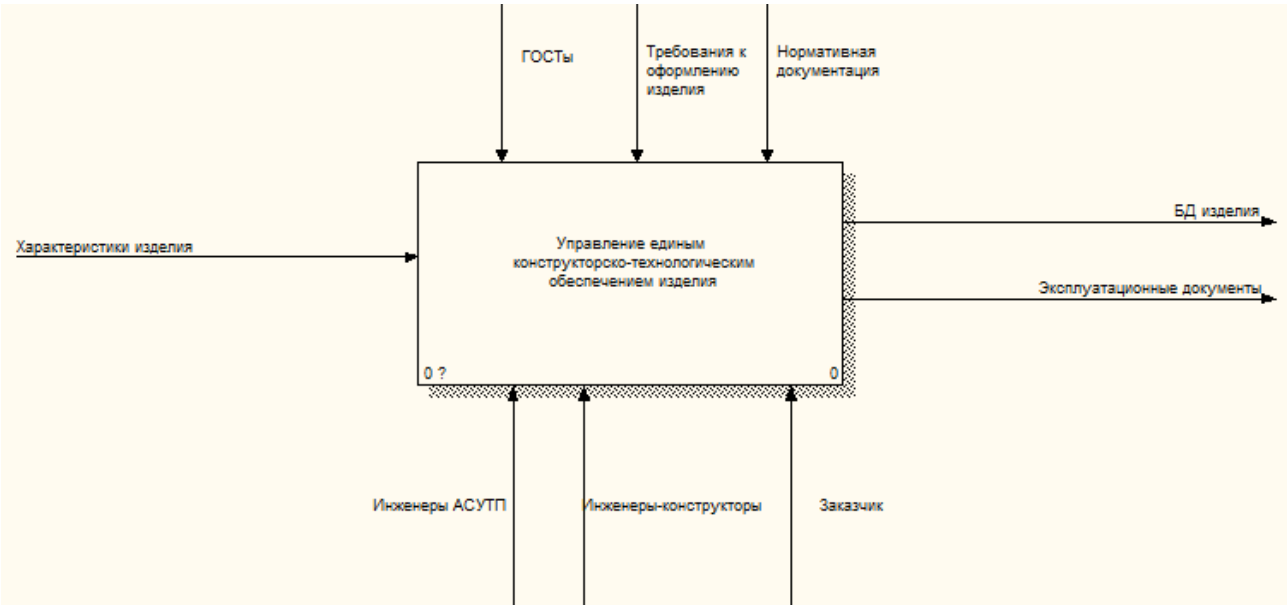


Рис. 2. Контекстная диаграмма процесса управления единым конструкторско-технологическим обеспечением изделия

Диаграмма декомпозиции первого уровня включает в себя следующие подпроцессы (рис.3):

– выбор облика;

– проектирование;

– изготовление и доводка опытного образца.

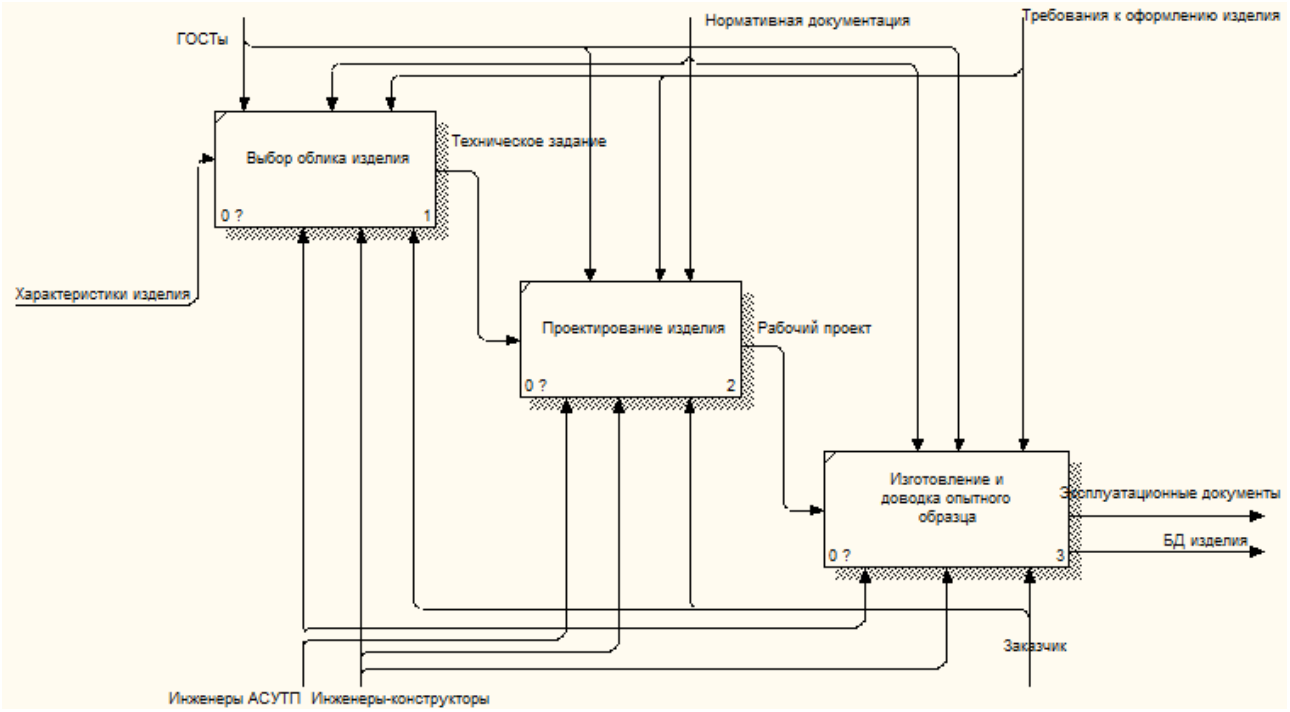


Рис. 3. Диаграмма декомпозиции первого уровня процесса управления единым конструкторско-технологическим обеспечением изделия

Программная реализация процесса

Программная реализация процесса конструкторско-технологического обеспечения выполнена на базе следующих модулей системы PDM STEP Suite:

– Модуль PDM;

– Настройка словарей БД;

– Редактор шаблонов процессов.

Модуль «Настройка словарей БД» позволяет создавать учетные записи пользователей, добавлять сотрудников и их ролей.

Графический модуль «Редактор шаблонов процессов» позволяет создавать и редактировать шаблоны процессов.

Модуль PDM – основной модуль PSS, в котором выполняются основные работы с данными об изделии. Содержит подсистему PSS-WorkFlow.

Реализация процесса «Проектирование изделия» представляет собой совокупность действий и подпроцессов, приведенных на рис. 4 – 7.

Основным является процесс «Проектирование изделия», его владельцем является пользователь, относящийся в организационной структуре предприятия к высшему руководству. Владелец процесса запускает экземпляр процесса, назначает исполнителей подпроцессов и контролирует весь комплекс проектно-конструкторских и технологических работ.

Назначенные исполнители подпроцессов, в свою очередь, назначают исполнителей работ, контролируют сроки и качество выполняемых работ.

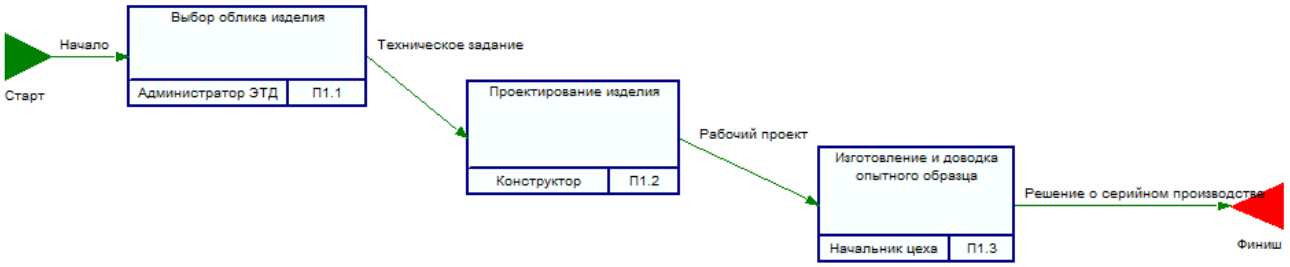


Рис. 4. Шаблон процесса «Проектирование изделия»

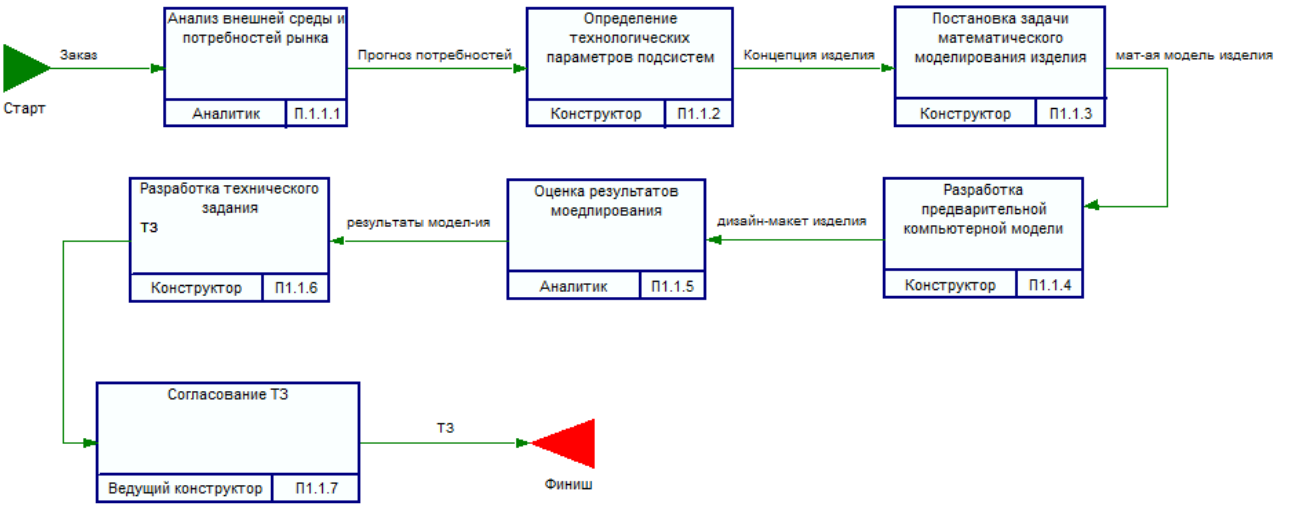


Рис. 5. Шаблон подпроцесса «Выбор облика изделия»

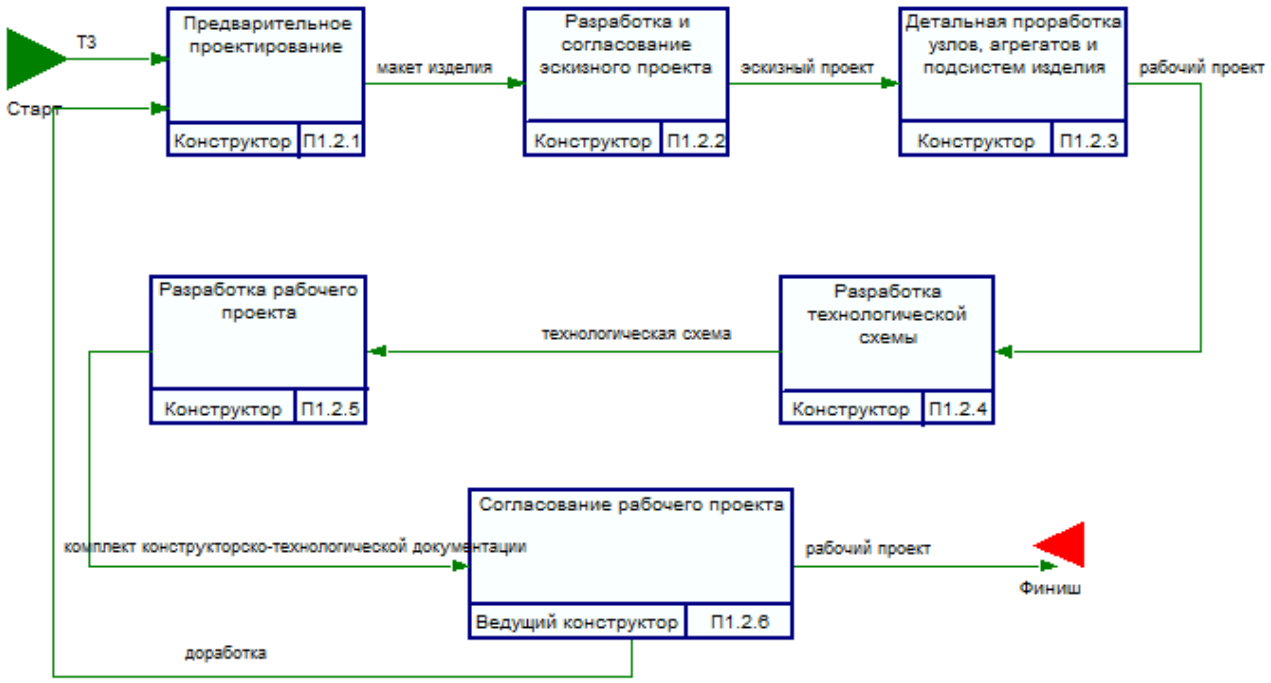


Рис. 6. Шаблон подпроцесса «Проектирование изделия»

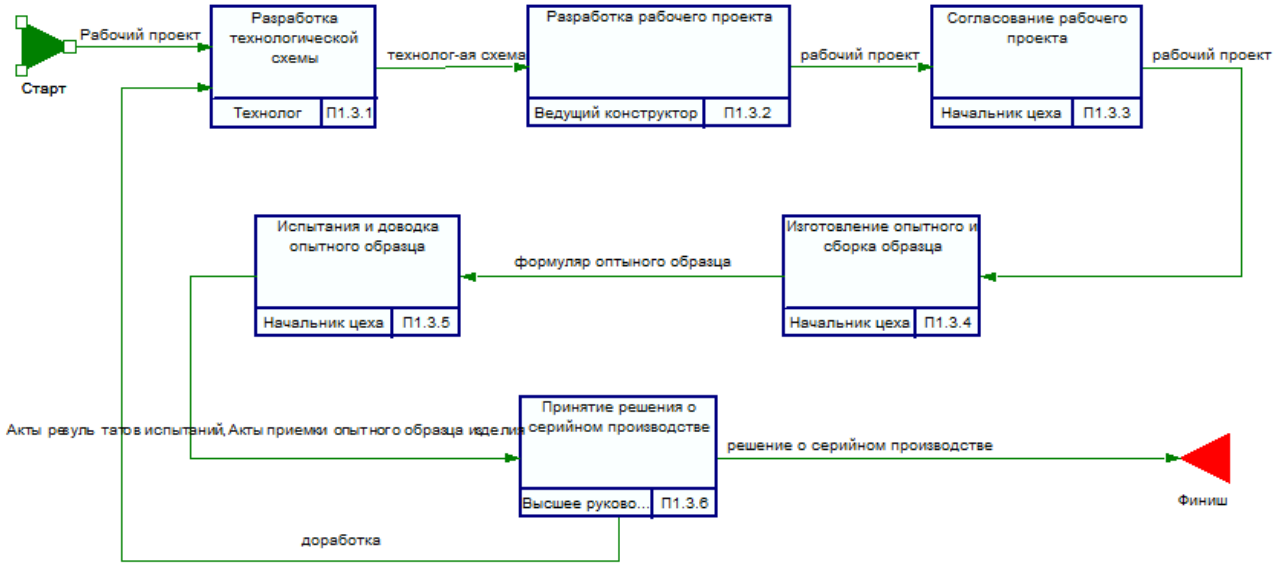


Рис. 7. Шаблон подпроцесса «Изготовление и доводка опытного образца»

Все результаты работ, проектно-конструкторская и технологическая документация заносится в интегрированную базу данных изделия.

Для того чтобы запустить процессы, создается проект пользователем из высшего руководства. При создании проекта назначаются исполнители и координаторы процессов.

Кроме того, у каждого из подпроцессов свой владелец, контролирующий выполнение задач и назначение исполнителей.

Все задачи формируются и автоматически передаются следующему исполнителю. Как только все задачи подпроцесса выполнены, владелец выдает решение о доработке или принимает задачу, выполняя ее.

Результат проведенного эксперимента по управлению потоками проектно-конструкторских и технологических работ представлен на рис.8.

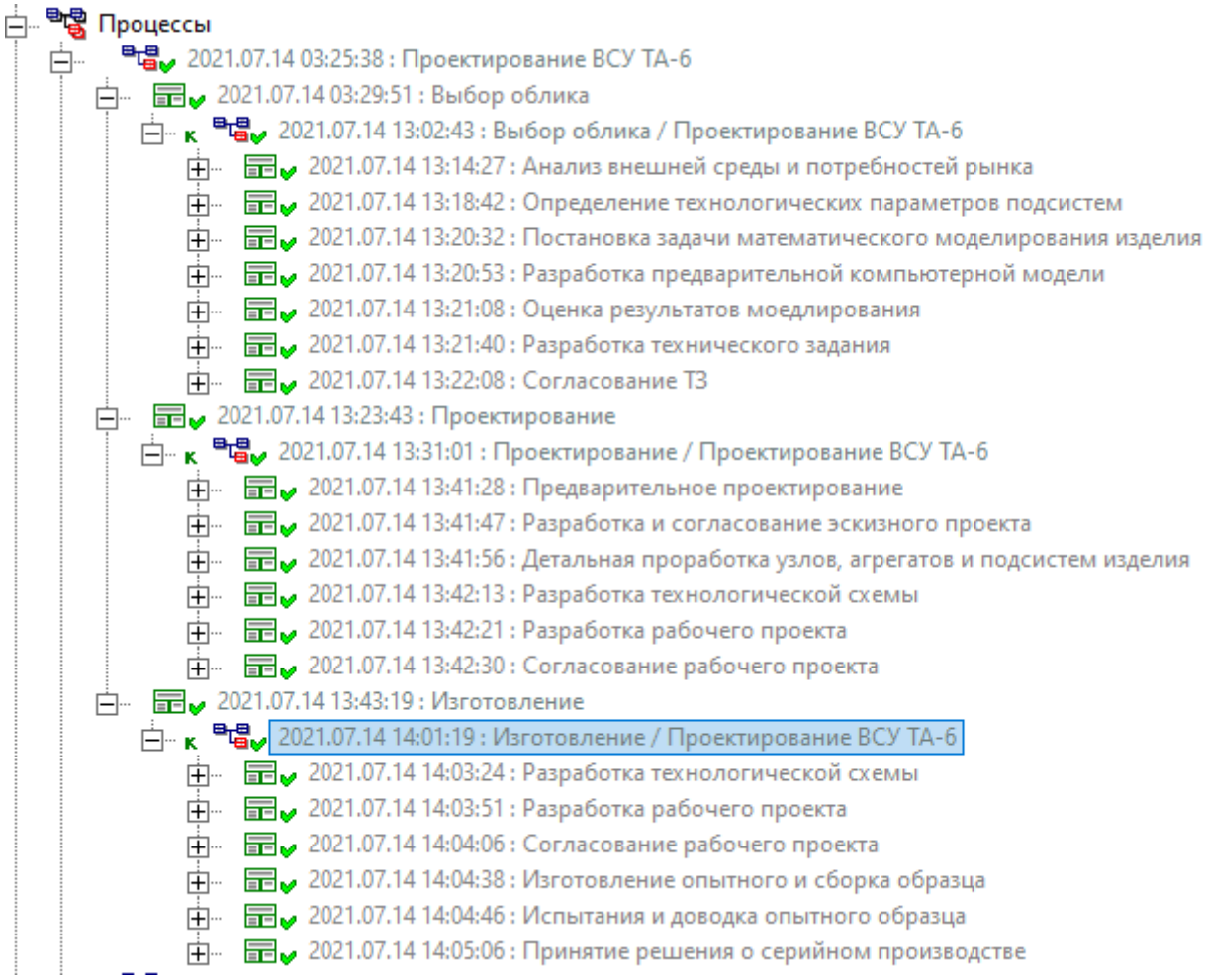


Рис. 8. Комплекс выполненных работ

Таким образом, с помощью разработанных моделей процессов управления жизненным циклом изделия проведен эксперимент по запуску процесса конструкторско-технологического обеспечения изделия. В процессе эксперимента по управлению потоками работ получены следующие результаты применения технологии управления данными об изделии: PDM-систем позволяет контролировать доставку и получение задания исполнителем, получать актуальную информацию о текущем состоянии процессов, контролировать сроки выполнения

заданий и процессов, а также отслеживать историю выполнения заданий и процессов.

СПИСОК ЛИТЕРАТУРЫ

1. [Электронный ресурс]. http://pss.cals.ru/ (Дата обращения: 16.08.2021).
2. Системы информационной поддержки жизненного цикла космических аппаратов: [учебное пособие] / Р. Р. Каримов, Н. В. Кондратьева; ФГБОУ ВПО УГАТУ .— Уфа : УГАТУ, 2008 .— 154 с. (Дата обращения:16.08.2021).

УДК 681.518 (075.8)

В. А. НЕМКОВА, Д. У. СЫТДЫКОВА, Е. А. КУЗЬМИНА
nemkovav@bk.ru, dilarasytdykova@mail.ru, kuzminaea@mail.ru
Науч. руководит. – канд. техн. наук, доц. Е. А. КУЗЬМИНА

Уфимский государственный авиационный технический университет

ИНФОРМАЦИОННО-АНАЛИТИЧЕСКАЯ ПОДДЕРЖКА ПРОЦЕССА ОБУЧЕНИЯ В АО «УФАНЕТ»

Аннотация. Рассматривается процесс обучения сотрудников с использованием обучающей системы Moodle, позволяющей организовать более продуктивный процесс мониторинга квалификационного уровня сотрудников, а также оперативного формирования методических материалов.
Ключевые слова: СДО Moodle; обучение сотрудников; набор тестовых заданий; оценивание и анализ результатов обучения; методический контент; среда обучения; мониторинг процесса обучения; кластерный анализ.

Введение

В процессе обучения сотрудников любого производства, фирмы, компании необходимо контролировать процесс обучения. В наше время увеличение информационных потоков и повышение сложности организационного управления приводят к необходимости использования автоматизированных информационных систем. А в условиях современных стандартов образования сотрудников растет количество информации и ее необходимо обрабатывать, тем самым становится необходимо внедрение информационной системы поддержки процесса обучения.

Для решения подобного рода задач множество подобных систем, как отечественного, так и зарубежного производства такие как ATutor, ILIAS, SAKAI, OLAT, OpenACS, Автоматизированная система Прометей, Moodle, LAMS, iSpring, Dokeeos. Мы рассмотрим СДО Moodle.

Moodle – это среда дистанционного обучения, предназначенная для создания качественных дистанционных курсов. Этот программный продукт используется более чем в 100 странах мира университетами, школами, компаниями и независимыми преподавателями. По своим возможностям Moodle выдерживает сравнение с известными коммерческими системами управления учеб-

ным процессом, в то же время выгодно отличается от них тем, что распространяется в открытых исходных кодах – это дает возможность "заточить" ее под особенности каждого образовательного проекта, дополнить новыми сервисами.

В системе Moodle существует 3 типа форматов курсов: форум, структура (учебные модули без привязки к календарю), календарь (учебные модули с привязкой к календарю). Курс может содержать произвольное количество ресурсов (веб-страницы, книги, ссылки на файлы, каталоги) и произвольное количество интерактивных элементов курса. Практически во всех ресурсах и элементах курса в качестве полей ввода используется удобный и интуитивно понятный WYSIWYG HTML редактор, кроме того, существует возможность ввода формул в формате TeX или Algebra.

Для всех элементов курса возможно оценивание, в том числе по произвольным, созданным преподавателем, шкалам. Все оценки могут быть просмотрены на странице оценок курса, которая имеет множество настроек по виду отображения и группировки оценок. Web-сайт Moodle бесплатно оказывает пользователям платформы качественную поддержку.

Постановка задачи

Одной из весомых задач, стоящих перед предприятием, является повышение квалификации сотрудников за счет постоянного обучения (как новых, так и старых сотрудников), следовательно, становится необходимо улучшение работы тренингового центра с внедрением информационных технологий.

Поэтому актуальным является повышение эффективности обучения сотрудников на основе информационно-аналитической поддержки процесса формирования банка тестовых заданий и алгоритмов аналитической обработки результатов обучения.

Для достижения цели необходимо разработать комплекс системных моделей процесса организации обучения сотрудников, выполнить программную реализацию ИАП с использованием необходимого программного и алгоритмического обеспечения.

Схема процесса обучения сотрудников многих предприятий может быть описана следующим образом (рис.1).

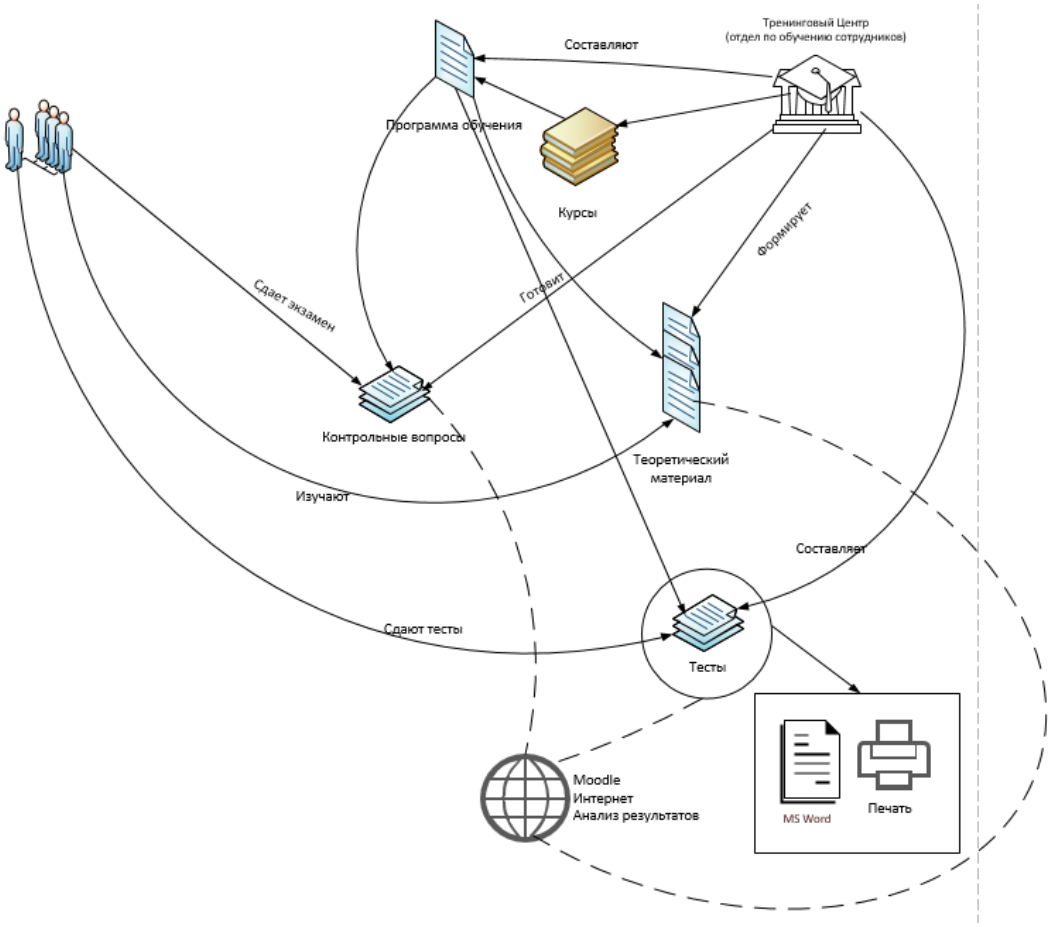


Рис. 1. Схема процесса обучения сотрудников

Отдел по обучению сотрудников составляет тесты, курсы и программу обучения, благодаря которой формируется теоретический материал. Сотрудники в свою очередь изучают этот материал и впоследствии сдают тесты и экзамен. Анализ результатов отсутствует, а подведение результатов производится тренером (преподавателем) вручную и занимает в лучшем случае около двух-трех минут на один тест. Это очень много, поэтому этот процесс нужно автоматизировать для оптимизации используемых ресурсов. Также может отсутствовать объективная оценка освоения материала с точки зрения тренера (преподавателя).

Предлагаемое решение улучшения эффективности процесса обучения

На (рис.2) показана мнемосхема работы информационно-аналитической поддержки процесса обучения с использованием Moodle.

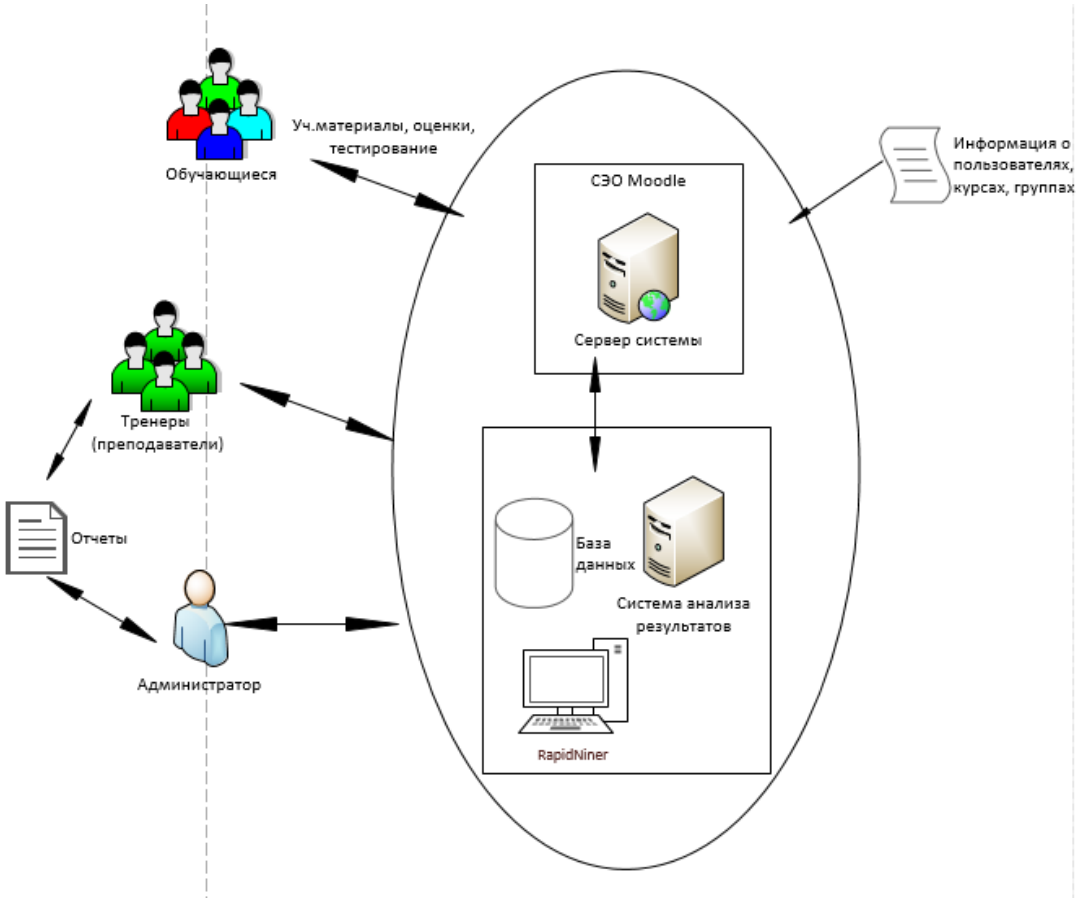


Рис. 2. Мнемосхема процесса

Преподаватели составляют рабочие материалы, тесты и контрольные вопросы, которые вводят в сервер системы Moodle. Все вопросы хранятся в базе данных и могут быть впоследствии использованы снова в этом же курсе (или в других).

Обучающиеся же дистанционно обучаются, усваивают теоретический и практический материалы, а также в этой системе проходят тестирование и сдают экзамены. Анализ результатов присутствует, вследствие чего ученики наглядно видят свои ошибки.

Также система хранит и обновляет информацию о сотрудниках, курсах и группах.

Программная реализация процесса

Программная реализация включает в себя осуществление нескольких блоков, необходимых для более подробного анализа данных, полученных в результате прохождения процедуры тестирования на базе Moodle.

Первый блок включает в себя процедуру импорта результатов проведения тестирования. Первоначально информация представляет собой таблицу, содержащую баллы каждого обучающегося по конкретному пройденному тесту. Стоит отметить, что не все оценочные мероприятия могут быть пройдены конкретным человеком, а, следовательно, не все ячейки таблицы могут содержать баллы.

После сбора всей необходимой информации нужно произвести процедуру классификации данных. Данная процедура поможет совершить более подробный анализ результатов, так как с помощью нее возможно сгруппировать баллы по нескольким показателям (например, < 70% правильности, <30% правильности и так далее). Также классификация подготавливает данные для дальнейшего еще более подробного анализа с использованием технологий кластеризации.

Далее после всех вышеописанных процедур информация должна быть сохранена для дальнейшей передачи в процедуру кластеризации. Информация в удобном и понятном для пользователя формате записывается в виде таблицы в файл Excel.

Архитектура программной реализации включает в себя класс Form1.cs с тремя методами. Каждый метод отвечает за один из вышеупомянутых разобранных блоков. Однако стоит отметить, что для ускорения процедуры анализа было принято решение объединить исполнение первого и второго блока в реализации первого метода.

Метод Form1_Load является приватным и событийным, то есть его исполнение запускается сразу при загрузке экранной формы программы. Суть его работы заключается в следующей последовательности действий:

– разметка таблицы из класса dataGridView на экранном окне;

– открытие необходимого табличного файла Excel, содержащего первоначальные баллы обучающихся;

– подсчет количества обучающихся, чьи баллы удовлетворяют каким-либо из утвержденных показателей классификации;

– вывод таблицы с показателями классификации в подготовленный объект класса dataGridView.

Метод button2_Click является приватным и событийным, вызывается при нажатии на кнопку «Сохранить». Суть метода состоит в реализации блока записи полученных классифицированных данных в таблицу Excel. Информация носит формат удобных для чтения данных для дальнейшего анализа при помощи алгоритма кластеризации.

Третий метод класса Form1.cs называется button1_Click, он является приватным и событийным. После завершения процедуры работы с оконным приложением пользователь может совершить выход из программы при помощи нажатия на соответствующий объект button1, имеющий подпись «Закрыть».

Таким образом, для повышения эффективности модели процесса обучения разработана информационная система. В процессе эксперимента использования системы получены следующие результаты применения технологии:

– предложен метод кластеризации k-средних для обработки результатов тестирования, также разработан алгоритм оценки результатов на основе кластерного анализа;

– выполнена программная реализация ИАП с использованием системы дистанционного обучения Moodle, среды разработки Visual Studio на языке программирования C#, также для проведения кластерного анализа был использован пакет Rapid Miner;

– проведена оценка эффективности, после которой было выявлено, что время на составление тестовых заданий снижается в 10 раз, а время проверки тестовых заданий в 50 раз.

СПИСОК ЛИТЕРАТУРЫ

1. Moodle // Moodle URL: https://moodle.com/ (дата обращения: 25.09.2021).
2. Учимся C# // Хабр URL: https://habr.com/ru/post/49404/ (дата обращения: 28.09.2021).
3. Кластеризация: алгоритмы k-means и c-means // Хабр URL: https://habr.com/ru/post/67078/ (дата обращения: 28.09.2021).
4. Оценка эффективности систем защиты информации с использованием функционально-стоимостного анализа: лабораторный практикум по дисциплине «Экономика защиты информации» / Уфимск. гос. авиац. техн. ун-т; сост.: В. А. Чанышева, Т. А. Иванова. Уфа : РИК УГАТУ, 2020. 29 с.

УДК 004.942

А. А. ПЕРЕВЕРЗИНА
inf.ugatu@mail.ru
Науч. руковод. – канд. физ.-мат. наук, доц. Л. И. ШЕХТМАН

Уфимский государственный авиационный технический университет

ПРОГРАММИРОВАНИЕ МИКРОКОНТРОЛЛЕРОВ ДЛЯ СИСТЕМ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ

Аннотация. Рассматривается задача программирования контроллеров, используемых в составе систем контроля и управления доступом. Созданы программы в системах AtmelStudio и CODESYS.
Ключевые слова: программирование контроллеров; система контроля и управления доступом.

Рассматривается деятельность инжиниринговой компании, занимающейся разработкой и установкой систем безопасности, автоматизации и обеспечения комфортной жизнедеятельности, а также сервисным обслуживанием и модернизацией любых инженерных систем.

Практически каждая автоматизированная система имеет в своем составе программируемые логические контроллеры. Программируемый логический контроллер (ПЛК) – это программно управляемый дискретный автомат, имеющий некоторое множество входов, подключенных посредством датчиков к объекту управления, и множество выходов, подключенных к исполнительным устройствам. Он контролирует состояние входов и вырабатывает определенные последовательности программно заданных действий, отражающихся в изменении выходов.

В рассматриваемой инжиниринговой компании для программирования микроконтроллеров применяется AtmelStudio (ранее AVR Studio) [1] – основанная на Visual Studio бесплатная интегрированная среда разработки (IDE) для разработки приложений для 8- и 32-битных микроконтроллеров семейства AVR и 32–битных микроконтроллеров семейства ARM от компании Atmel, работающая в операционных системах Windows NT/2000/XP/Vista/7/8/10.

На предприятии используется микроконтроллер ATMEGA8 (рисунок 1), необходимо написать код на языке С. На данном микроконтроллере имеется кнопка, гасящий резистор на 200 Ом, имеется светодиод, а также источник питания 5В. Необходимо составить принципиальную схему, где программно, последовательным нажатием на кнопку нужно включать или выключать светодиод. При установке единичного состояния на входе 0 порта PB программа возвращается в начало, при сбросе входа 0 порта PB, программа инвертирует значение выхода 7 порта PB. На основе поставленной задачи был составлен алгоритм будущей программы.

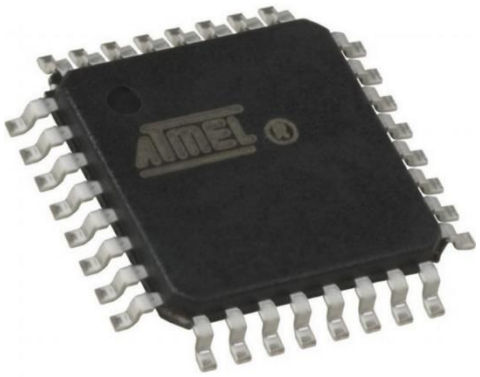


Рис. 1. Микроконтроллер ATMEGA8

Алгоритм был программно реализован в AtmelStudio. В программе инициализировались порты микроконтроллера. Инициализация нужна для того, чтобы подготовить к работе необходимые разъемы микроконтроллера или активировать встроенные устройства. Разъем порта PB0 включается на вход и к нему подсоединяется подтягивающий резистор, который подключен к плюсу источника питания контроллера, а разъем PB7 включается на выход.

Для того, чтобы можно было управлять работой микроконтроллера, включать определенные устройства, устанавливать их режим работы существует специальная область памяти, где есть множество ячеек, представляющих из себя единичные биты, т. е. в каждую ячейку можно прописать 0 или 1. Каждая ячейка определяет конкретную функцию, которую выполнит контроллер. Чем сложнее микроконтроллер, тем больше управляющих ячеек, и тем сложнее их

запомнить. В таблице Excel прописаны регистры портами управления микроконтроллера для наглядности (рисунок 2).

	A	B	C	D	E	F	G	H	I
1		7	6	5	4	3	2	1	0
2	F.sreg	I	T	H	S	V	N	Z	C
3	E.								
4	D.								
5	C.								
6	B.DdrB	DdrB7	DdrB6	DdrB5	DdrB4	DdrB3	DdrB2	DdrB1	DdrB0
7	A.PinB	PinB7	PinB6	PinB5	PinB4	PinB3	PinB2	PinB1	PinB0
8	9.Port B	Port B7	Port B6	Port B5	Port B4	Port B3	Port B2	Port B1	Port B0
9	8.								
10	7.								
11	6.								
12	5.								
13	4.								
14	3.								
15	2.								
16	1.								
17	0.								
18									

Рис. 2. Таблица регистров в Excel

Создается три регистра: DdrB, PinB, PortB, с помощью которых будем управлять портами микроконтроллера. Регистр DdrB (DdrB0...DdrB7) будет переключать соответствующий порт в два режима: ввод и вывод. В режиме ввода можно будет считывать состояние на разъемах контроллера и сохранять значения портов в регистр PinB (PinB0...PinB7), а в режиме вывода выдавать в порт данные из регистров PortB (PortB0...PortB7).

Кроме AtmelStudio на предприятии используется программно-инструментальный комплекс CODESYS [2], основанный на стандарте IEC 61131-3 и предназначенный для программирования промышленных контроллеров и компьютеров. Интегрированный комплекс CODESYS (аббревиатура от Controller Development System) состоит из двух частей: среды программирования и системы исполнения. Система исполнения CODESYS встраивается в контроллер в ходе его изготовления и необходима для программирования устройства в рассматриваемой среде. С помощью специального инструмента систему исполнения CODESYS можно адаптировать к различным аппаратным платформам. Среда программирования – основа всего комплекса, позволяющая разрабатывать прикладные программы для логических контроллеров в пяти специ-

ализированных редакторах, использующих разные, определяемые стандартом IEC 61131-3 языки:

– ассемблер-подобный список инструкций IL;

– pascal-подобный структурированный текст ST;

– язык функциональных блоковых диаграмм FBD (а в дополнение к нему и CFC с возможностью свободного размещения элементов и обратными связями);

– язык релейно-контактных схем LD;

– язык последовательных функциональных схем SFC.

Данные редакторы содержат огромное число вспомогательных функций, ускоряющих написание программ. Среди них: автоматическое объявление переменных, ассистенты ввода, интеллектуальная коррекция ввода, синтаксический контроль и цветовое выделение при вводе, масштабирование, автоматическое соединение и размещение графических элементов, поддержка объектно-ориентированного программирования.

Встроенные оптимизирующие компиляторы CODESYS создают машинный код, который загружается в память контроллера. Поддерживаются 16-ти и 32-х разрядные микропроцессоры 80x86, Infineon C166, архитектура ARM, TriCore, Analog Devices Blackfin, PowerPC, архитектура MIPS, SH, TI C2000/28x и некоторые другие.

Режим эмуляции комплекса позволяет отладить программное обеспечение без контроллера. После подключения к устройству среда программирования CODESYS способна провести отладку программ и оборудования, используя функции мониторинга, изменения и фиксации значений переменных, контроля потока выполнения, расстановки точек останова, обновления кода, графической трассировки в реальном времени. При непрерывных технологических процессах CODESYS может исправлять уже работающую программу на лету. Измененные части компилируются и попадают в контроллер, а система исполнения подключает новый код.

В программе существует менеджер задач и библиотек, встроенная поддержка различных сетей. Последние версии CODESYS позволяют пользователям самостоятельно развивать систему путем подключения плагинов, а встроенный в программу инструмент визуализации приближается по своей функциональности к коммерческим SCADA-системам. На предприятии данная программа служит для программирования линейных контроллеров.

Были рассмотрены вопросы, связанные с построением систем контроля и управления доступом, изучены основы программирования контроллеров в системах AtmelStudio и CODESYS. Были выполнены задания по программированию контроллера ATMEGA8.

СПИСОК ЛИТЕРАТУРЫ

1. AtmelStudio URL: http://wiki.amperka.ru/atmel-studio:start Дата обращения 03.07.2021).
2. CODESYS V2.3 – CODESYS V3. [Электронной ресурс] – URL: https://www.codesys.com (Дата обращения 16.07.2021).

УДК 004.42

А. А. ПЕРЕВЕРЗИНА, М. И. ГИЛЯЗОВА, Ю. Ф. АХМАДУЛЛИНА
angelina.pereverzina@mail.ru, gilyazova2001@bk.ru, julia13112000@mail.ru
Науч. руководит. – А. С. КОВТУНЕНКО

Уфимский государственный авиационный технический университет

СОЗДАНИЕ ПРОТОТИПА СЕРВИСА ПЕРСОНАЛИЗАЦИИ ЗОЖ-ПРИВЫЧЕК И ТРЕНИРОВОК НА ОСНОВЕ КОМПЛЕКСА ДАННЫХ ОБ ОРГАНИЗМЕ КЛИЕНТА

Аннотация. Рассматривается разработка мобильного приложения, с помощью которого пользователь сможет отслеживать результаты диагностики своего организма и получать индивидуальные рекомендации по питанию, тренировкам и процедурам.
***Ключевые слова*:** мобильное приложение; фитнес; здоровье.

Актуальность работы

С каждым днем все труднее представить современного человека без смартфона. За его экранами человек проводит большую часть жизни. Мобильные приложения становятся незаменимыми помощниками как по работе и учебе, так и по уходу за здоровьем. Мобильные приложения очень помогают человеку в работе, в учебе, в спорте и во многом другом. Существует множество различных фитнесс-приложений, но не во всех приложениях есть достаточно функций. Поэтому было разработано мобильное фитнесс-приложение, которое кардинально отличается от всех остальных

Об оборудовании

SCANME — это аппаратно-программный комплекс диагностики для автоматизированного определения индивидуальных программ коррекции и увеличения резервов здоровья человека.

Рис. 1.

Оборудование включает в себя следующие диагностические устройства:

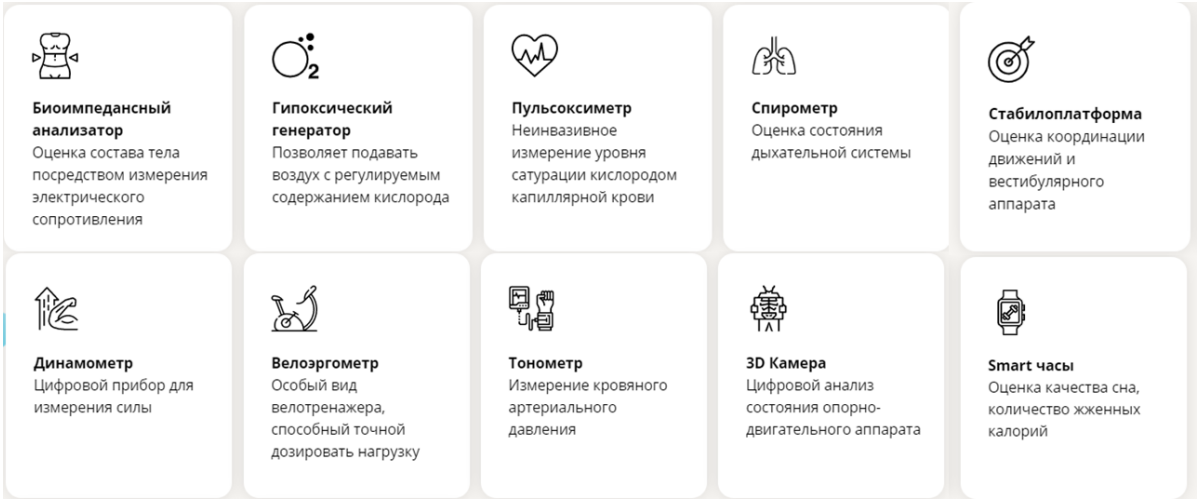


Рис. 2.

Используя разработанные алгоритмы, система осуществляет перекрестный анализ измеряемых показателей с последующей автоматизированной генерацией заключения и рекомендаций, как общих, так и каждому из анализируемых показателей.

Проблема

В дальнейшем через свою платформу компания, которая владеет оборудованием, хочет передавать данные партнерам, чтобы те использовали эту информацию для предоставления персонализированных услуг клиенту. В качестве потенциальных партнеров рассматриваются сервисы подбора плана питания, фитнес-клуба, страховые …

Решение проблемы

Разрабатывается мобильное приложение, которое является прототипом сервиса персонализации ЗОЖ-привычек и тренировок на основе комплекса данных об организме клиента и фармацевтические компании.

Мобильное приложение разрабатывается в интегрированной среде разработки Android Studio на языке Java.

Интерфейс приложения

Разработан интерфейс приложения. При запуске приложения появляются кнопки «ВОЙТИ» и «ЗАРЕГИСТРИРОВАТЬСЯ».

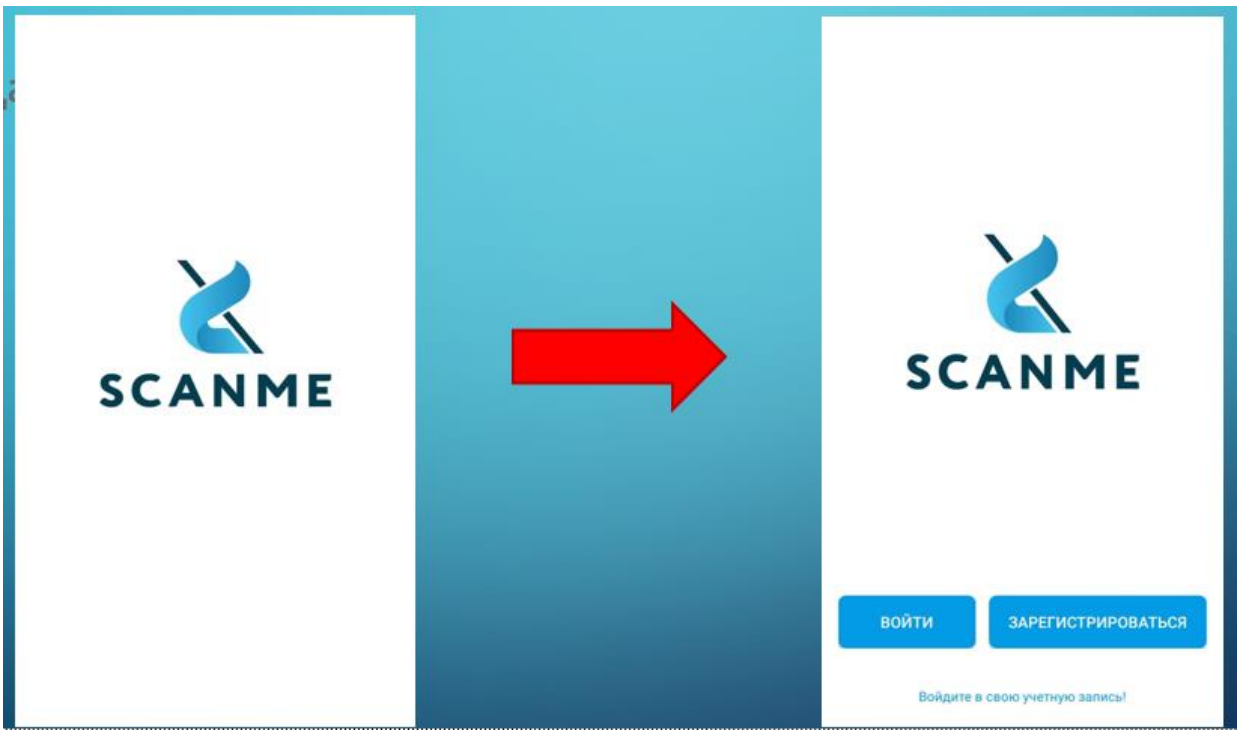


Рис. 3.

При их нажатии открываются соответствующие окна для входа в профиль или регистрации.

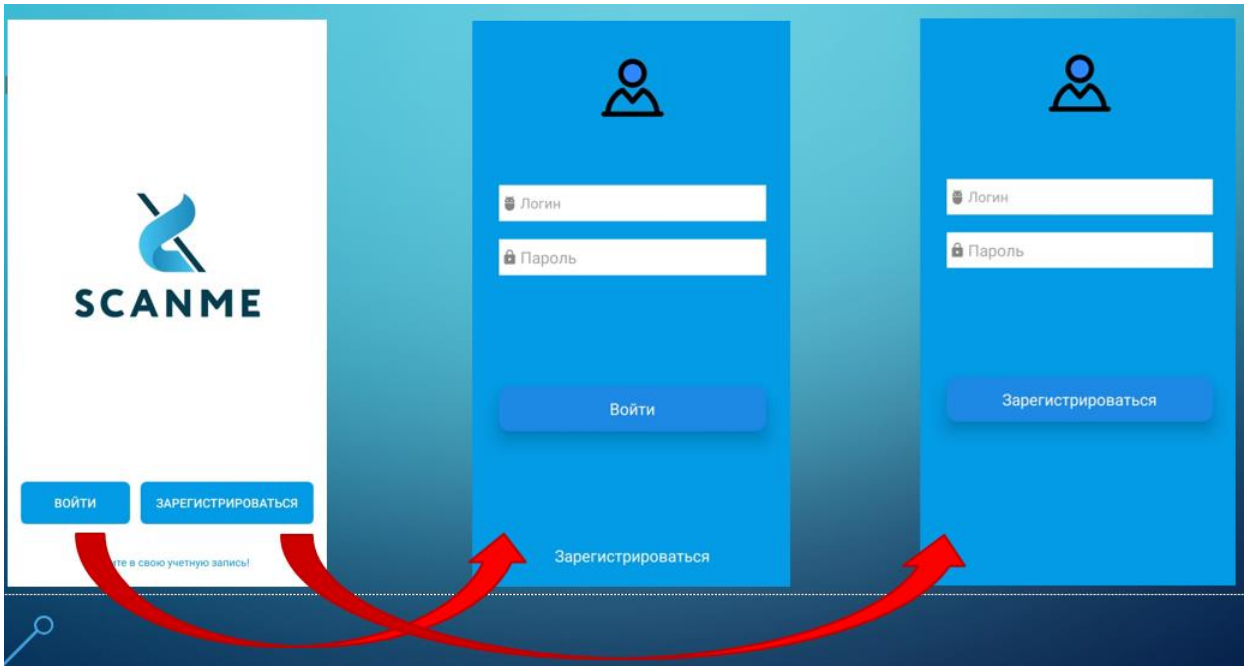


Рис. 4.

Снизу расположена нижняя панель навигации, которая включает в себя такие пункты как: главное, рекомендации, WELLNESS-программа и профиль.

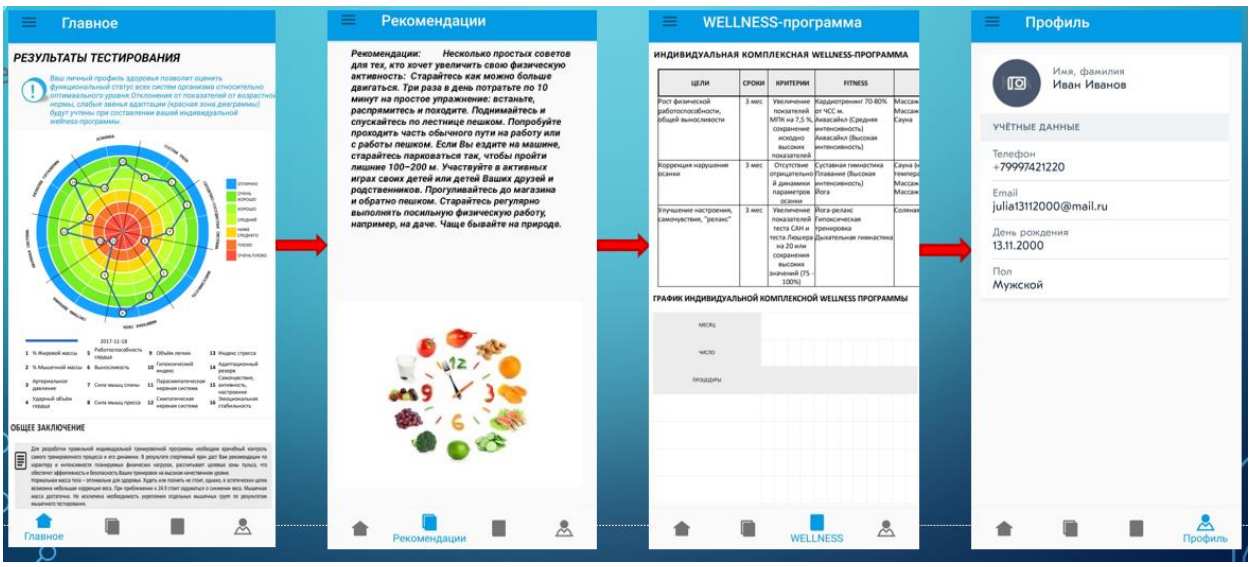


Рис. 5.

Сбоку слева расположено выдвигающееся боковое меню, включающее в себя результаты диагностики по различным параметрам организма.

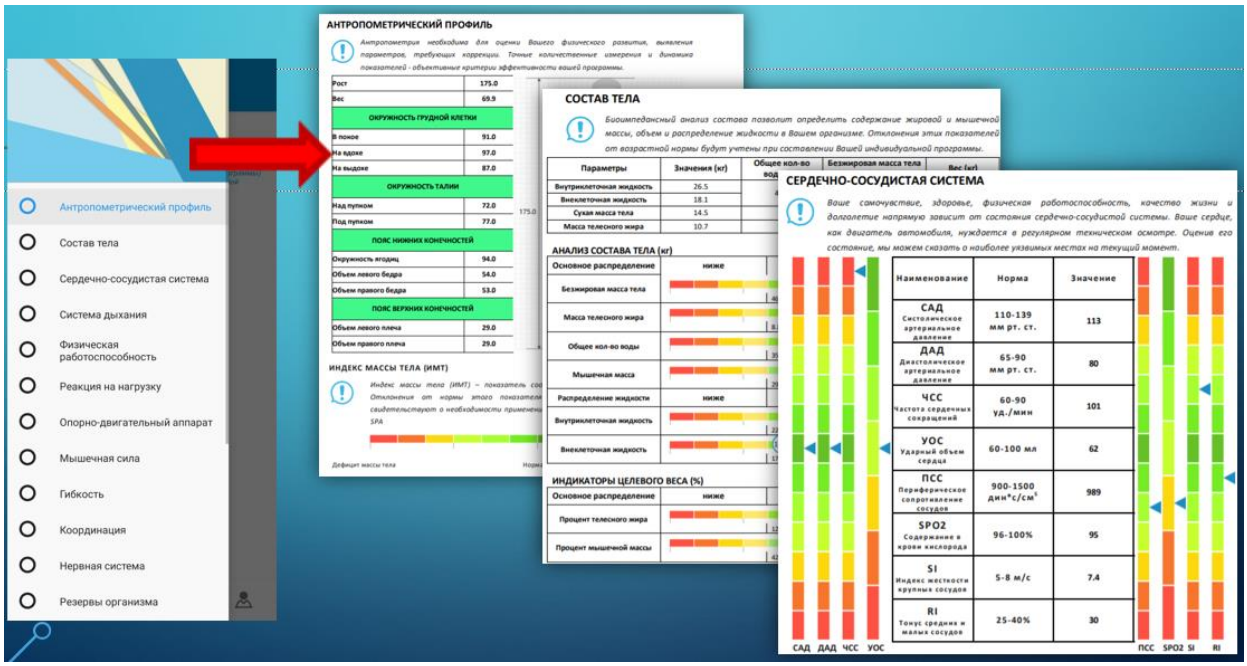


Рис. 6.

СПИСОК ЛИТЕРАТУРЫ

1. Полезные инструменты в Android Studio [Электронный ресурс] Хабр – 2021. – URL: https://habr.com/ru/post/239199/ (Дата обращения: 28.09.2021).
4. Разработка приложения на Android [Электронный ресурс] // Хабр – 2021. – URL: https://habr.com/ru/all/ (Дата обращения: 28.09.2021).
5. Разработка мобильных приложений: [Электронный ресурс] // Хабр – 2021. – URL: https://habr.com/ru/company/mailru/blog/179113/ (Дата обращения: 28.09.2021).

УДК 004.946

В. Д. ПРОФАТИЛОВ, Д. Е. ФАЛЬШУНОВА
profatilov2000@mail.ru, dfalshunova@mail.ru
Науч. руководов. – канд. техн. наук, доц. А. С. КОВТУНЕНКО

Уфимский государственный авиационный технический университет

ПРИМЕНЕНИЕ МЕТОДА WAVELET-ПРЕОБРАЗОВАНИЯ ДЛЯ ЦИФРОВОЙ ОБРАБОТКИ АУДИОДАННЫХ

***Аннотация*.** Рассматривается эффективность применения прямого и обратного Wavelet-преобразования в компьютерной программе для сжатия и восстановления аудиофайлов (аудиокодек).
***Ключевые слова*:** Wavelet; компрессия; вейвлет; сжатие аудио.

Актуальность работы

Технологии сжатия аудиоданных все чаще получают развитие в сферах сетевой коммуникации и цифровой обработки звука. Основная задача аудиокодека – уменьшить размер входного аудиофайла и, желательно, без потерь в качестве. Уменьшенный размер сжатого файла обеспечивает прирост скорости его передачи по сети относительно входного, а также, более рациональное хранение на цифровых накопителях.

На сегодняшний день актуально изучать старые и новые методы сжатия звуковых файлов для нахождения оптимального решения в разработке аудиокодека – максимального сжатия и минимальных потерь в качестве.

Понятие аудиокодека

Аудиокодек на программном уровне является специализированной компьютерной программой, кодеком, который сжимает (производит компрессию) или разжимает (производит декомпрессию) цифровые звуковые данные в соответствии с файловым звуковым форматом или потоковым звуковым форматом.

Понятие wavelet-преобразования

Wavelet-преобразование – это способ преобразования сигнала в форму, которая делает некоторые величины исходного сигнала более поддающимися изучению или позволяет сжать исходный набор данных.

Вейвлет-анализ разработан для решения задач, оказавшихся слишком сложными для традиционного анализа Фурье.

Основной недостаток преобразования Фурье заключается в том, что частотные компоненты не могут быть локализованы во времени, обуславливая его применимость только к анализу стационарных сигналов, в то время как многие сигналы имеют сложные частотно-временные характеристики. Как правило, такие сигналы состоят из близких по времени, короткоживущих высокочастотных компонентов и долговременных, близких по частоте низкочастотных компонентов.

Собственно, вейвлеты появились при анализе нестационарных процессов и сигналов. Фурье-анализ таких сигналов дает лишь перечисление его характерных частот (масштабов), но не содержит никакой информации о локальных координатах, при которых эти частоты себя проявляют.

Достоинства wavelet-преобразования:

1. Данное преобразование работает быстрее, чем преобразование Фурье;

2. Программная реализация несравненно проще, чем реализация преобразования Фурье.

Эффективность вейвлет-анализа в сравнении с преобразованием Фурье объясняется большей информативностью, предоставляющего исследователям дополнительную степень свободы для анализа в виде возможности видеть разложение сигналов по компактным базисным функциям не только при различных масштабах (частотах), но и при различных сдвигах по времени, что позволяет локализовать временные особенности сигнала [].

СПИСОК ЛИТЕРАТУРЫ

1. Аудиокодек [интернет ресурс] // URL: https://wiki2.info/Аудиокодек%20 (дата обращения: 28.09.2021).
2. Сжатие аудиоданных с применением wavelet-преобразований [интернет ресурс] // URL: https://bstudy.net/858151/tehnika/szhatie_audiodannyh_primeneniem_veyvlet_preobrazovaniy (дата обращения: 28.09.2021).

УДК 001.891.57: 004.657

Г. Р. ФАИЗОВА, Р. Р.КАРИМОВ
ffaiz2020@mail.ru,rikar@yandex.ru
Науч. руководь. – канд. техн. наук, доц. Р. Р. КАРИМОВ

Уфимский государственный авиационный технический университет

ИНФОРМАЦИОННАЯ ПОДДЕРЖКА ПРОЦЕССА ПРОГНОЗИРОВАНИЯ ПАРАМЕТРОВ СТАТИЧЕСКОГО НАГРУЖЕНИЯ ПРИ ОБРАБОТКЕ РЕЗУЛЬТАТОВ ЛЕТНО-ПРОЧНОСТНЫХ ИСПЫТАНИЙ ЛЕТАТЕЛЬНОГО АППАРАТА

Аннотация. Рассматривается задача разработки компьютерной нейросетевой модели параметров статического нагружения на основе результатов летно-прочностных испытаний летательного аппарата.
Ключевые слова: нейронная сеть; летно-прочностные испытания; регрессия; статическое нагружение.

Актуальность

Летные прочностные испытания (ЛПИ) проводятся с целью подтверждения безопасности по условиям прочности полетов на режимах, разрешенных для эксплуатации самолета данного типа.

Указанная цель достигается путем:

– исследования закономерностей и особенностей нагружения конструкции самолета и его отдельных частей в ожидаемых условиях эксплуатации, сравнения их с принятыми при расчетах и лабораторных испытаниях и, в случае необходимости, корректировки последних на основе материалов летных исследований;

– внесения изменений (при необходимости) в руководство по эксплуатации с тем, чтобы исключить режимы полета, представляющие опасность по условиям прочности;

– выполнения полетов с достижением предельных режимов полета для непосредственной демонстрации наличия необходимых запасов по прочности при наиболее неблагоприятных сочетаниях параметров полета.

Летные испытания проводятся по программам, составленным для каждого типа самолета. Режимы испытаний назначаются таким образом, чтобы ограниче-

ния, накладываемые по условиям аэродинамики, устойчивости, работы силовых установок, а также конструктивные особенности самолета не препятствовали их достижению.

Программа летных испытаний должна включать в себя:

– исследования закономерностей нагружения самолета в ожидаемых условиях эксплуатации;

– выполнение полетов на предельных режимах.

Постановка задачи

Цель работы – повышение эффективности обработки результатов ЛПИ на основе информационной поддержки процесса прогнозирования параметров статического нагружения.

Для достижения поставленной цели необходимо решить следующие задачи:

1) Провести анализ входных и выходных данных летно-прочностных испытаний;

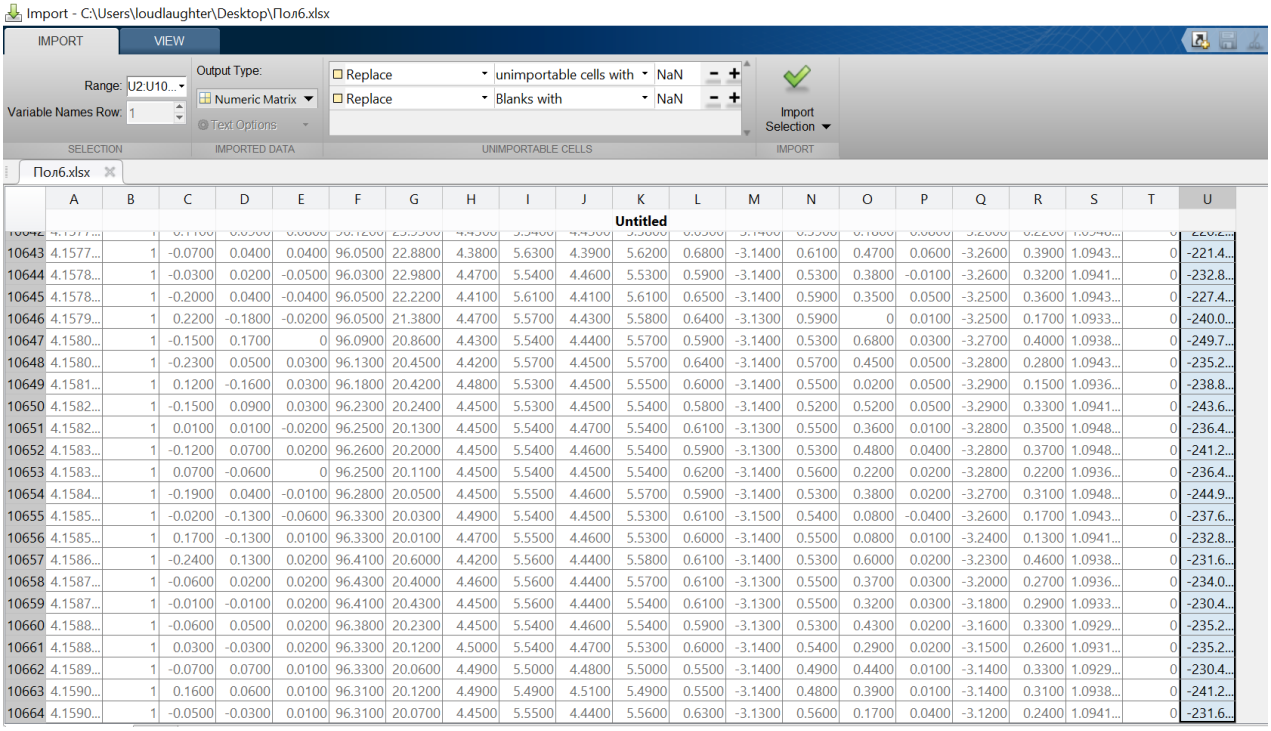
2) Построить компьютерную модель на основе нейросети для обработки входных и выходных данных статического нагружения.

В ходе проведения летно-прочностных испытаний были получены выходные данные изгибающего момента в одном сечении левой консоли крыла. Входные данные представляют собой вектор из 20 параметров. Для получения предполагаемого значения изгибающего момента в определенном режиме полета, не проводя летные испытания в выбранном режиме, необходимо создать нейросеть для прогнозирования выходного значения изгибающего момента в зависимости от входных данных.

Решение задачи

В качестве инструментальной среды для разработки компьютерной модели выбран пакет математического и инженерного моделирования Mathworks MatLab и входящий в его состав Neural Network Toolbox.

Процесс создания нейросети начинается с подготовки обучающей выборки. На основе результатов ЛПИ подготовлена матрица размером 10663×21, в которой последний столбец – это выходные данные статического нагружения (рисунок 1).



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
10643	4.1577...	1	-0.0700	0.0400	0.0400	96.0500	22.8800	4.3800	5.6300	4.3900	5.6200	0.6800	-3.1400	0.6100	0.4700	0.0600	-3.2600	0.3900	1.0943...	0	-221.4...
10644	4.1578...	1	-0.0300	0.0200	-0.0500	96.0300	22.9800	4.4700	5.5400	4.4600	5.5300	0.5900	-3.1400	0.5300	0.3800	-0.0100	-3.2600	0.3200	1.0941...	0	-232.8...
10645	4.1578...	1	-0.2000	0.0400	-0.0400	96.0500	22.2200	4.4100	5.6100	4.4100	5.6100	0.6500	-3.1400	0.5900	0.3500	0.0500	-3.2500	0.3600	1.0943...	0	-227.4...
10646	4.1579...	1	0.2200	-0.1800	-0.0200	96.0500	21.3800	4.4700	5.5700	4.4300	5.5800	0.6400	-3.1300	0.5900	0	0.0100	-3.2500	0.1700	1.0933...	0	-240.0...
10647	4.1580...	1	-0.1500	0.1700	0	96.0900	20.8600	4.4300	5.5400	4.4400	5.5700	0.5900	-3.1400	0.5300	0.6800	0.0300	-3.2700	0.4000	1.0938...	0	-249.7...
10648	4.1580...	1	-0.2300	0.0500	0.0300	96.1300	20.4500	4.4200	5.5700	4.4500	5.5700	0.6400	-3.1400	0.5700	0.4500	0.0500	-3.2800	0.2800	1.0943...	0	-235.2...
10649	4.1581...	1	0.1200	-0.1600	0.0300	96.1800	20.4200	4.4800	5.5300	4.4500	5.5500	0.6000	-3.1400	0.5500	0.0200	0.0500	-3.2900	0.1500	1.0936...	0	-238.8...
10650	4.1582...	1	-0.1500	0.0900	0.0300	96.2300	20.2400	4.4500	5.5300	4.4500	5.5400	0.5800	-3.1400	0.5200	0.5200	0.0500	-3.2900	0.3300	1.0941...	0	-243.6...
10651	4.1582...	1	0.0100	0.0100	-0.0200	96.2500	20.1300	4.4500	5.5400	4.4700	5.5400	0.6100	-3.1300	0.5500	0.3600	0.0100	-3.2800	0.3500	1.0948...	0	-236.4...
10652	4.1583...	1	-0.1200	0.0700	0.0200	96.2600	20.2000	4.4500	5.5400	4.4600	5.5400	0.5900	-3.1300	0.5300	0.4800	0.0400	-3.2800	0.3700	1.0948...	0	-241.2...
10653	4.1583...	1	0.0700	-0.0600	0	96.2500	20.1100	4.4500	5.5400	4.4500	5.5400	0.6200	-3.1400	0.5600	0.2200	0.0200	-3.2800	0.2200	1.0936...	0	-236.4...
10654	4.1584...	1	-0.1900	0.0400	-0.0100	96.2800	20.0500	4.4500	5.5500	4.4600	5.5700	0.5900	-3.1400	0.5300	0.3800	0.0200	-3.2700	0.3100	1.0948...	0	-244.9...
10655	4.1585...	1	-0.0200	-0.1300	-0.0600	96.3300	20.0300	4.4900	5.5400	4.4500	5.5300	0.6100	-3.1500	0.5400	0.0800	-0.0400	-3.2600	0.1700	1.0943...	0	-237.6...
10656	4.1585...	1	0.1700	-0.1300	0.0100	96.3300	20.0100	4.4700	5.5500	4.4600	5.5300	0.6000	-3.1400	0.5500	0.0800	0.0100	-3.2400	0.1300	1.0941...	0	-232.8...
10657	4.1586...	1	-0.2400	0.1300	0.0200	96.4100	20.6000	4.4200	5.5600	4.4400	5.5800	0.6100	-3.1400	0.5300	0.6000	0.0200	-3.2300	0.4600	1.0938...	0	-231.6...
10658	4.1587...	1	-0.0600	0.0200	0.0200	96.4300	20.4000	4.4600	5.5600	4.4400	5.5700	0.6100	-3.1300	0.5500	0.3700	0.0300	-3.2000	0.2700	1.0936...	0	-234.0...
10659	4.1587...	1	-0.0100	-0.0100	0.0200	96.4100	20.4300	4.4500	5.5600	4.4400	5.5400	0.6100	-3.1300	0.5500	0.3200	0.0300	-3.1800	0.2900	1.0933...	0	-230.4...
10660	4.1588...	1	-0.0600	0.0500	0.0200	96.3800	20.2300	4.4500	5.5400	4.4600	5.5400	0.5900	-3.1300	0.5300	0.4300	0.0200	-3.1600	0.3300	1.0929...	0	-235.2...
10661	4.1588...	1	0.0300	-0.0300	0.0200	96.3300	20.1200	4.5000	5.5400	4.4700	5.5300	0.6000	-3.1400	0.5400	0.2900	0.0200	-3.1500	0.2600	1.0931...	0	-235.2...
10662	4.1589...	1	-0.0700	0.0700	0.0100	96.3300	20.0600	4.4900	5.5000	4.4800	5.5000	0.5500	-3.1400	0.4900	0.4400	0.0100	-3.1400	0.3300	1.0929...	0	-230.4...
10663	4.1590...	1	0.1600	0.0600	0.0100	96.3100	20.1200	4.4900	5.4900	4.5100	5.4900	0.5500	-3.1400	0.4800	0.3900	0.0100	-3.1400	0.3100	1.0938...	0	-241.2...
10664	4.1590...	1	-0.0500	-0.0300	0.0100	96.3100	20.0700	4.4500	5.5500	4.4400	5.5600	0.6300	-3.1300	0.5600	0.1700	0.0400	-3.1200	0.2400	1.0941...	0	-231.6...

Рис. 1. Файл входных данных

В соответствии с заданной структурой обучающей выборки создается разметка для импорта входных и выходных данных.

В процессе создания нейросети подобрано опытным путем количество нейронов в скрытом слое (Number of Hidden neurons), при заданной структуре обучающей выборки количество нейронов в скрытом слое должно быть не менее 30 (рисунок 2).

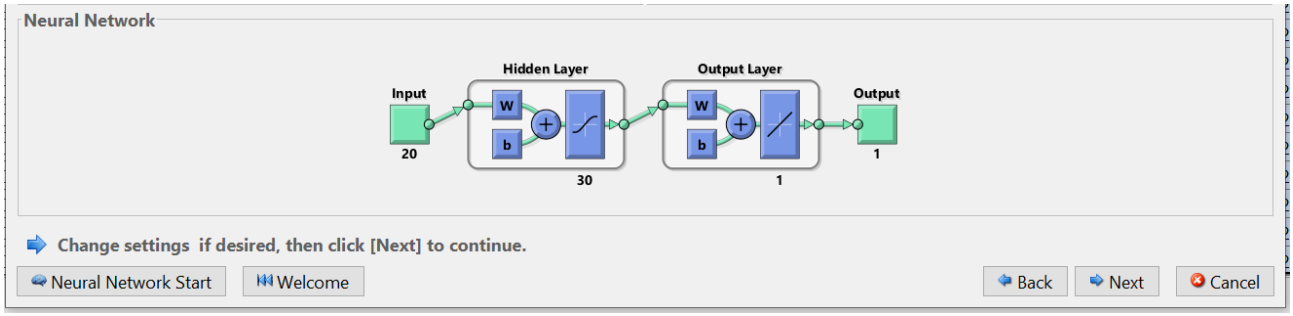


Рис. 2. Структура нейронной сети

Процесс обучения нейросети и его результаты представлены на рисунке 3.

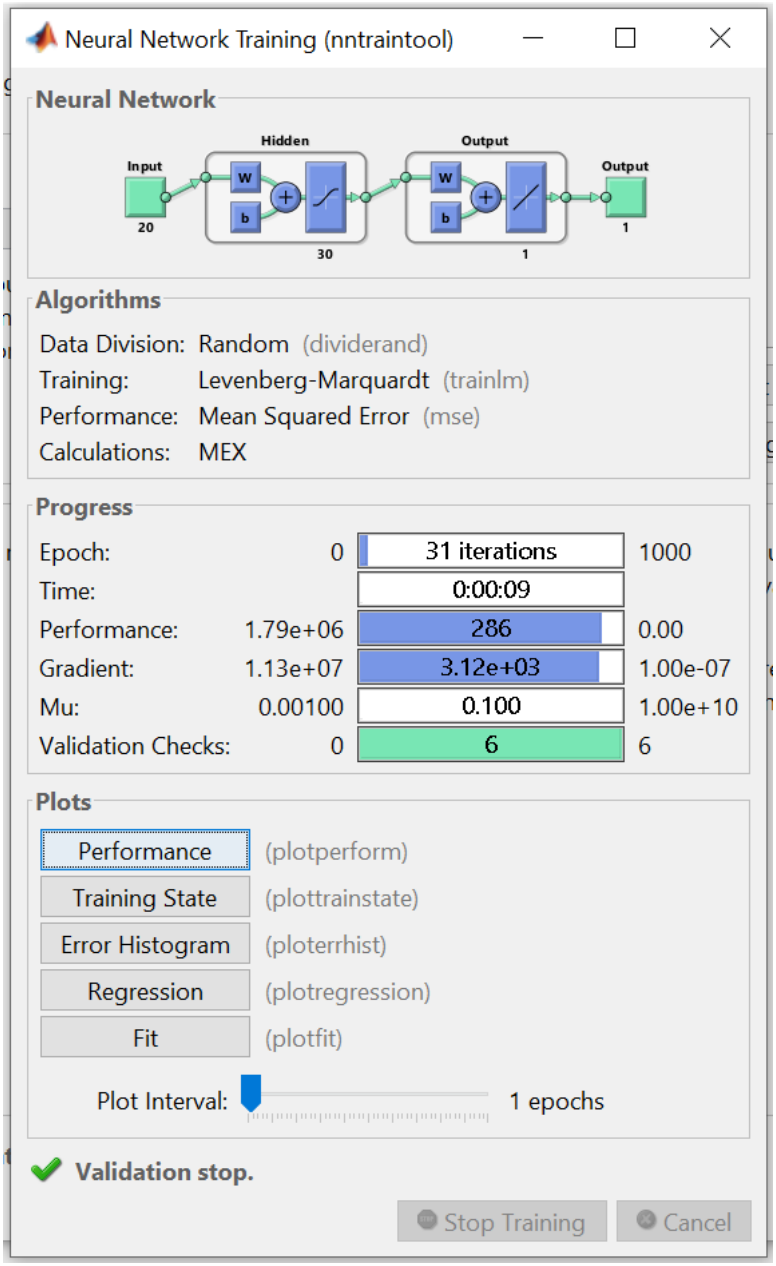


Рис. 3. Обучение нейросети

Регрессионный анализ результатов обучения показал высокую сходимость как на обучающей выборке, так и на тестовой (рисунок 4).

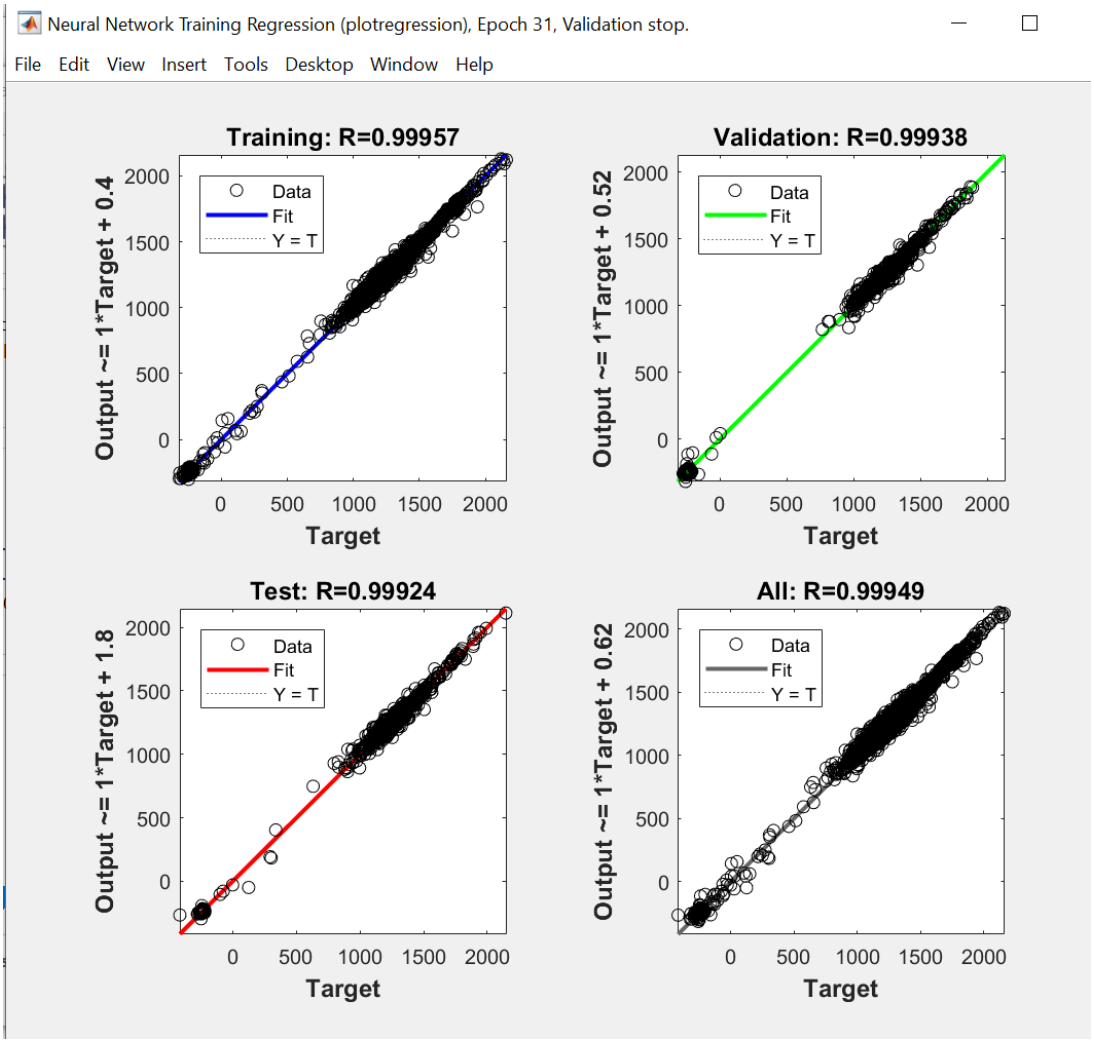


Рис. 4. Результаты регрессионного анализа процесса обучения

Точность экстраполяции при единичных тестовых проверках также показывает удовлетворительные результаты. При заданных входных параметрах реальное выходное значение изгибающего момента было -231, а прогноз нейросети показал -227.5220.

```
>> sim(net,[41590.31;1;-0.05;-0.03;0.01;96.31;20.07;4.45;5.55;4.44;5.56;0.63;-3.13;0.56;0.17;0.04;-3.12;0.24;1094.06;0])

ans =

  -227.5220

fx >>
```

Рис. 5. Результат работы нейросети

СПИСОК ЛИТЕРАТУРЫ

1.[Электронный ресурс]. URL: https://digiratory.ru/508 (Дата обращения: 12.08.2021)
2.[Электронный ресурс]. URL: https://habr.com/ru/company/etmc_exponenta/blog/530792/ (Дата обращения:12.08.2021)

УДК 004.946

Д. Е. ФАЛЬШУНОВА, В. Д. ПРОФАТИЛОВ
dfalshunova@mail.ru, profatilov2000@mail.ru
Науч. руководв. – канд. техн. наук, доц. А. С. КОВТУНЕНКО

Уфимский государственный авиационный технический университет

ПРИМЕНЕНИЕ МЕТОДА БЫСТРОГО ПРЕОБРАЗОВАНИЯ ФУРЬЕ ДЛЯ ЦИФРОВОЙ ОБРАБОТКИ АУДИОСИГНАЛОВ

Аннотация. Рассматривается эффективность применения алгоритма ускоренного вычисления дискретного преобразования Фурье с целью создания компьютерной программы, предназначенной для кодирования (сжатия) и декодирования (восстановления) аудиоданных.
***Ключевые слова*:** обработка аудиосигналов; частота дискретизации; преобразование Фурье; компрессия/декомпрессия аудиоданных; аудиокодек.

Актуальность работы

Развитие цифровой техники привело к изменению способов хранения сигналов. Если раньше сигнал мог записываться на магнитофон и храниться на ленте в аналоговом виде, то сейчас аудиосигналы оцифровываются и хранятся в файлах в памяти компьютера в виде набора чисел. Данный массив целых чисел представляет собой несжатый аудиопоток, представляющий собой дискретный набор значений-амплитуд аналогового сигнала, взятых через равные промежутки времени (с определенной частотой дискретизации).

При записи данного массива в файл, даже короткий временной интервал получается весьма объемным, так как в таком потоковом сигнале содержится много избыточных данных.

В связи с этим, возникает необходимость применения специальных технологий и методов для создания программных средств, главной задачей которых является уменьшения объема пространства, требуемого для хранения аудиоданных, а также предоставления возможности снизить полосу пропускания канала, по которому передаются аудиоданные.

Метод быстрого преобразования фурье для обработки аудиосигналов

Метод быстрого преобразования Фурье (*БПФ, FFT*) позволяет увидеть в исследуемом сигнале вклад каждой гармонической составляющей, характеризу-

емой определенной частотой. Данный метод позволяет разложить функцию по частотам.

Эффективность применения

Основным преимуществом метода является его быстродействие и удобство применения в цифровой обработке аудиосигналов.

Анализ Фурье – область математического анализа, отвечающая на вопрос, как можно представить математическую функцию в виде комбинации простых тригонометрических функций.

Основной алгоритм

Алгоритм ускоренного вычисления дискретного преобразования Фурье, позволяет получить результат за время, меньшее чем $O(N^2)$ (требуемого для прямого, поформульного вычисления).

При применении основного алгоритма дискретное преобразование Фурье может быть выполнено за $O(N(p_1+...+p_n)$ действий при $N = p_1 p_2 ... p_n$, в частности, при $N = 2^n$ понадобится $O(N\log(N))$ действий.

Дискретное преобразование Фурье преобразует набор чисел $a_0,...,a_{n-1}$ в набор чисел $b_0,...,b_{n-1}$, такой, что

$$b_i = \sum_{j=0}^{n-1} a_j \varepsilon^{ij} ,$$

где ε – первообразный корень из единицы, то есть $\varepsilon^n = 1$ и $\varepsilon^k \neq 1$ при $0 < k < n$. Основной шаг алгоритма состоит в сведении задачи для N чисел к задаче с меньшим числом. Для $N = pq$, $p > 1$, $q > 1$, над полем комплексных чисел вводятся: $\varepsilon_\nu = e^{2\pi i/\nu}$, $\varepsilon_\nu = 1$, где ν – любое число.

Дискретное преобразование Фурье может быть представлено в виде:

$$b_i = \sum_{k=0}^{p-1} \sum_{j=0}^{q-1} a_{kq+j} \varepsilon_N^{(kq+j)i} .$$

Данные выражения могут быть легко получены, если исходную сумму разбить на меньшее число сумм с меньшим числом слагаемых, а после полученные

суммы привести к одинаковому виду путем сдвига индексов и их последующего переобозначения.

Таким образом:

$$b_i = \sum_{k=0}^{p-1}\sum_{j=0}^{q-1} a_{kq+j}\varepsilon_N^{(kq+j)i} = \sum_{j=0}^{q-1}\varepsilon_N^{ij}\left(\sum_{k=0}^{p-1} a_{kq+j}\varepsilon_N^{(kiq)}\right).$$

С учетом того, что $\varepsilon_N^{kiq} = \varepsilon_{N/q}^{ki}$ и $N/q = p$,окончательная запись:

$$b_i = \sum_{j=0}^{q-1}\varepsilon_N^{ij}\left(\sum_{k=0}^{p-1} a_{kq+j}\varepsilon_p^{ki}\right).$$

Далее вычисляется каждое b_i , где $i = \overline{0, p-1}$, здесь по-прежнему требуется совершить $O(N)$ действий, то есть на этом этапе производится $p \cdot O(N) = O(Np)$ операций.

Далее считается b_{i+mp} , где $i = \overline{0, p-1},\ m = \overline{1, q-1}$. При замене $i \to i + mp$ в последней формуле, выражения, стоящие в скобках, остались неизменными, а так как они уже были посчитаны на предыдущем шаге, то на вычисление каждого из них потребуется только $O(q)$ действий. Всего $p(q-1) = N - p$ чисел. Следовательно, операций на этом шаге $(N-p)\cdot O(q) = O((N-1)q \cong O(Nq)$. Последнее с хорошей точностью верно при любых *N*.

Алгоритм быстрого преобразования Фурье логично применять для $N \gg 1$, потому как при малом числе отсчетов он дает небольшой выигрыш в скорости по отношению к прямому расчету дискретного преобразования Фурье. Таким образом, для того чтобы полностью перейти к набору чисел $b_0,...,b_{n-1}$, необходимо $O(Np)+O(Nq)$ действий. Следовательно, нет разницы, на какие два числа разбивать *N* – ответ от этого сильно не будет меняться. Уменьшено же число операций может быть только дальнейшим разбиением *N*.

Для *обратного преобразования Фурье* можно применять алгоритм прямого преобразования Фурье – нужно лишь использовать ε^{-1} вместо ε (или применить операцию комплексного сопряжения вначале к входным данным, а затем к результату, полученному после прямого преобразования Фурье), и окончательный результат поделить на N.

Применение метода прямого и обратного БПФ для создания аудиокодека

Аудиокодек на программном уровне является специализированной компьютерной программой, которая сжимает (производит компрессию) или восстанавливает (производит декомпрессию) цифровые звуковые данные в соответствии с потоковым звуковым форматом.

Задача аудиокодека как компрессора заключается в предоставлении аудиосигнала с заданным качеством/точностью и минимально возможным размером.

Следовательно, процесс создания аудиокодека с применением быстрого преобразования Фурье заключается в следующем:

1. Разбиение сигнала на амплитудно-временные кадры;

2. Использование прямого БПФ для получения амплитудно-частотных кадров;

3. Запись полученных данных в файл;

4. Считывание закодированных данных;

5. Восстановление амплитудно-частотных кадров;

6. Применение обратного БПФ для получения амплитудно-временных кадров;

7. Восстановление сигнала из амплитудно-временных кадров.

СПИСОК ЛИТЕРАТУРЫ

1. Аудиокодек | URL: Аудиокодек — Википедия (wikipedia.org) (Дата обращения: 21.06.2021).
2. Сжатие аудиоданных | URL: Сжатие аудиоданных — Википедия (wikipedia.org) (Дата обращения: 24.06.2021).

3. Классификация методов преобразования Фурье | URL: О классификации методов преобразования Фурье на примерах их программной реализации средствами Python / Хабр (habr.com) (Дата обращения: 25.06.2021).
4. Быстрое преобразование Фурье | URL: Быстрое преобразование Фурье — Википедия (wikipedia.org) (Дата обращения: 25.06.2021).

УДК 004.942

Н. К. ХАННАНОВ, А. А. ПЕРЕВЕРЗИНА
inf.ugatu@mail.ru
Науч. руковод. – канд. физ.-мат. наук, доц. Л. И. ШЕХТМАН

Уфимский государственный авиационный технический университет

ИНФОРМАЦИОННАЯ ПОДДЕРЖКА ПРОЦЕССА РАСПРЕДЕЛЕНИЯ ЗАДАНИЙ МЕЖДУ ИСПОЛНИТЕЛЯМИ НА ОСНОВЕ ЭКСПЕРТНОЙ КЛАССИФИКАЦИИ

Аннотация. Рассматривается задача распределения заданий между сотрудниками организационно-технической системы. Создана программа на C#, реализующая метод экспертной классификации заданий по нескольким уровням сложности. Применение экспертного метода обеспечивает информационную поддержку принятия решений по распределению заданий между исполнителями.
Ключевые слова: распределение заданий между исполнителями; программа на C#; экспертная классификация.

Задачу распределения заданий между исполнителями приходится решать при управлении любой организационно-технической системой. Частота возникновения задачи зависит от специфики работы и может варьироваться от нескольких часов до нескольких лет. Рассмотрим в качестве примера деятельность контакт-центра банка, а именно группы по обработке web-обращений клиентов [1]. Контакт-центр является важным структурным подразделением любой компании, имеющей активный контакт с людьми. В условиях конкуренции побеждает тот, кто имеет лучшую обратную связь с клиентами, причем как действующими, так и потенциальными. Сейчас многие клиенты выбирают в качестве способа обращения в банк именно web-обращения из-за таких преимуществ, как

– отсутствие необходимости посещения офиса и ожидания в очереди;

– отсутствие затрат времени на ожидание и разговор с оператором, при обращении по телефону.

Web-обращения различаются по объему рабочего времени сотрудников, требуемого на их обработку, а также составу действий, которые нужно выпол

нить в процессе обработки. Можно выделить следующие категории web-обращений клиентов с точки зрения сложности:

1) простые – обращения, примеры ответов на которые есть в электронном пособии для сотрудников; занимают от 5 до 7 минут для составления и отправления ответа;

2) средние – обращения, касающиеся проблемы, для решения которой требуется работа в специальном прикладном программном обеспечении и составление ответов, требующих больше рабочего времени;

3) сложные – требующие еще больше рабочего времени сотрудников, больше работы с программным обеспечением, регистрации заявки в технической поддержке, взаимодействия с другими сотрудникам из сторонних департаментов банка.

Если распределение заданий между сотрудниками выполняется без учета класса сложности, то это приводит к неравномерной загруженности исполнителей.

Для описания проекта была построена функциональная модель (рис. 1). В качестве входной информации используются web-обращения клиентов банка.

Управляющими воздействиями являются:

– трудовой кодекс;

– должностные инструкции;

– экспертные методы.

В качестве механизмов реализации выступают:

– руководство контакт-центра;

– сотрудники контакт-центра;

– информационно-аналитическая система (ИАС).

Выходными данными являются отчеты по проделанной работе и решения по управлению группой сотрудников.

Рисунок 2 отображает диаграмму декомпозиции первого уровня для рассматриваемой задачи.

Очередность выполнения функций для решения рассматриваемой задачи следующая:

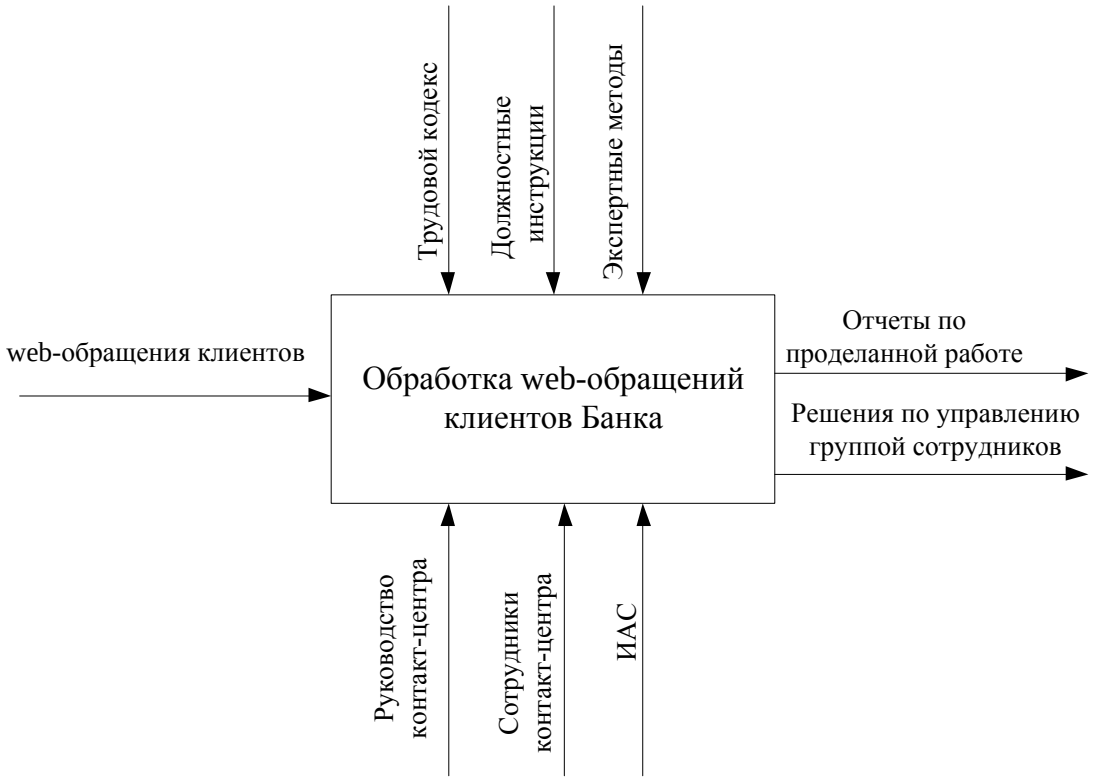


Рис. 1. Контекстная диаграмма системы обработки web-обращений клиентов банка

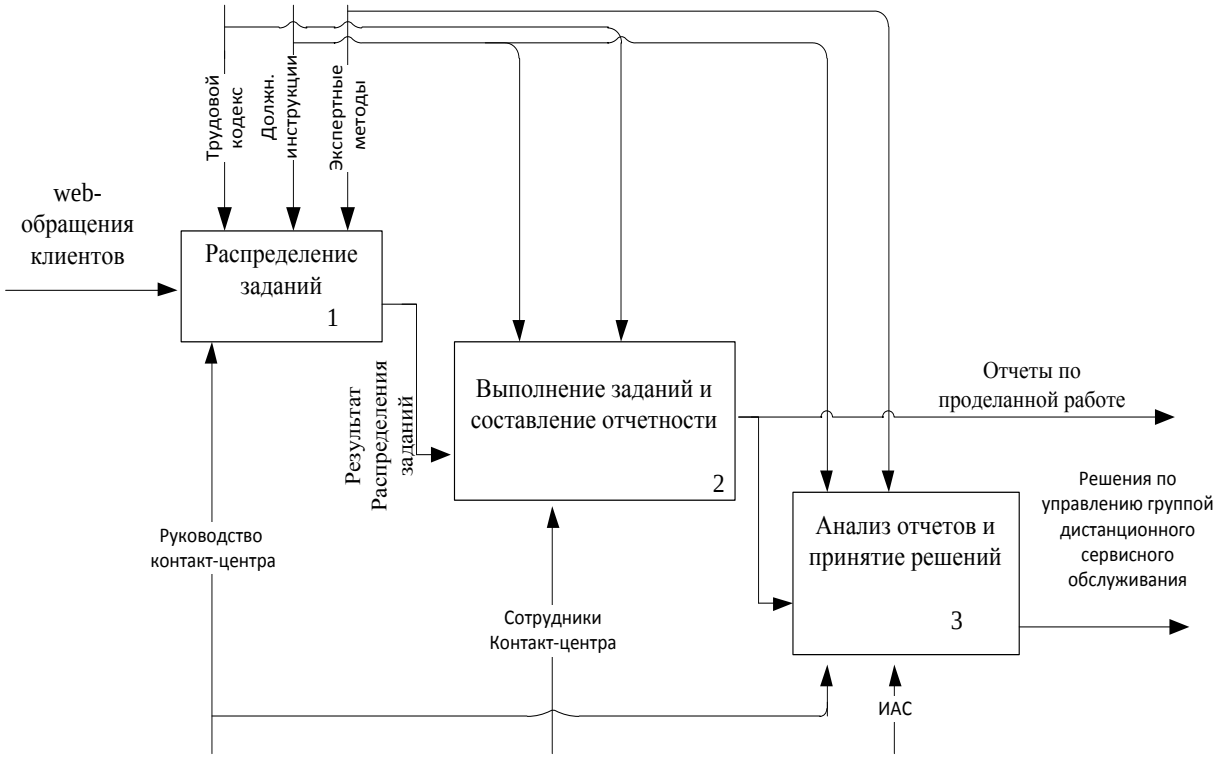


Рис. 2. Диаграмма декомпозиции первого уровня

– распределение заданий, выполняемое руководством контакт-центра с помощью экспертных методов, реализованных в ИАС с учетом требований трудового кодекса и должностных инструкций;

– выбор заданий и составление отчетов;

– анализ отчетов и принятие решений.

Рисунок 3 представляет информационную модель обработки web-обращений клиентов банка.

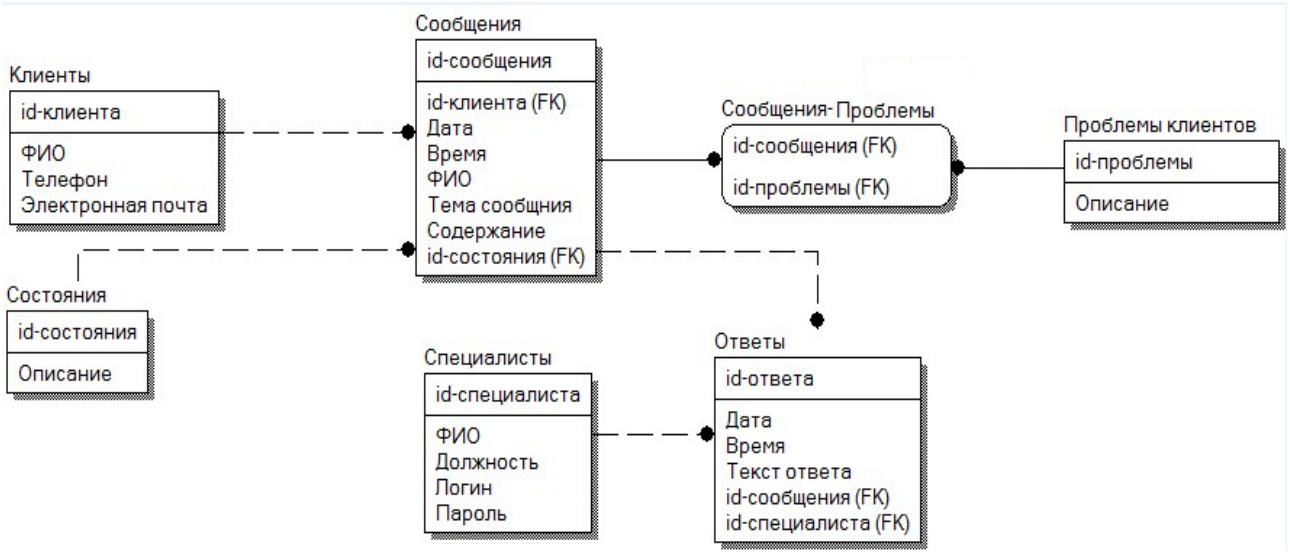


Рис. 3. Информационная модель обработки web-обращений клиентов банка

Предлагается до начала распределения заданий между сотрудниками выполнить экспертную классификацию [2] web-обращений по сложности обработки. В качестве эксперта выступает руководитель контакт-центра банка. Эксперту предъявляется все множество web-обращений, которые требуется обработать в течение рабочего дня. Эксперт выполняет предварительный анализ каждого web-обращения, оценивая требуемые затраты времени, количество и сложность выполняемых операций, в том числе по применению программного обеспечения, необходимости привлечения специалистов других отделов. Эксперт может учитывать количество подзадач, которые можно выделить в проблеме клиента, а также связи между ними. По итогам выполненного анализа эксперт относит каждое web-обращение к одному из классов сложности.

После того как все обращения проанализированы и оценены, эксперт может еще раз посмотреть на всю получившуюся классификацию (т.е. распределение обращений по классам) в целом и решить не требуется ли выполнить корректировку. Возможно, окажется, что некоторые близкие по сложности обращения клиентов оказались в разных классах, или, наоборот, значительно отличающиеся – в одном. При необходимости выполняется перенос обращений между классами.

Для выполнения экспертной классификации была разработана программа на языке C#, которая обеспечивает выполнение следующих функций:

– загрузка списка альтернатив из текстового файла, выбираемого пользователем;

– выбор пользователем количества уровней сложности;

– присвоение каждой альтернативе уровня сложности;

– отображение результатов классификации на экране;

– корректировка классификации;

– сохранение результата классификации в текстовый файл;

– загрузка результата классификации из текстового файла.

После разбиения множества заданий на непересекающиеся подмножества (классы) задания каждого класса сложности распределяются между сотрудниками. В результате у каждого сотрудника будет приблизительно одинаковое соотношение между количествами заданий различной сложности. Это позволит повысить качество процедуры принятия решений при управлении группой дистанционного сервисного обслуживания банковского учреждения.

СПИСОК ЛИТЕРАТУРЫ

1. Шехтман Л. И., Каримов Р. Р., Шаяхметова Д. И. Информационная поддержка управления группой дистанционного сервисного обслуживания банковского учреждения. Сборник материалов VII Международной научной конференции, посвященной памяти С.С. Ефимова, «Математическое и компьютерное моделирование». Омск, 2020. С. 136-138.
2. Литвак Б.Г. Экспертные технологии в управлении. М.: Дело, 2004. 400 с.

УДК 519.87

Д. В. ШЛЁНКИН, В. А. ГЛУЩЕНКО, А. В. ШУНДЕЕВ, М. А. ИВАНОВ
kot.dima2011@yandex.ru, val_g_2001@bk.ru, artem_shundeev@mail.ru, aa4052783@gmail.com
Науч. руководит. – канд. техн. наук, проф. А. С. КОВТУНЕНКО

Уфимский государственный авиационный технический университет

РАЗРАБОТКА ПРИЛОЖЕНИЯ ДЛЯ АНАЛИЗА ЗАВИСИМОСТИ ТЕКУЧЕСТИ КАДРОВОГО СОСТАВА ОТ СТАЖА РАБОТЫ НА ПРЕДПРИЯТИИ

Аннотация. Рассматривается информационная поддержка процесса формирования отчетов о текучести кадрового состава предприятия путем анализа исходных данных за прошлые года.
***Ключевые слова*:** анализ; кадровый состав; текучесть кадрового состава, разработка, внедрение, обработка данных.

Актуальность работы

Текучесть – это процентное выражение, частное от деления численности увольняющихся сотрудников, которые приняли это решение самостоятельно («по собственному желанию») к общей численности уволенных сотрудников за тот же период (месяц, квартал, год). Основная проблема большинства предприятий – невозможность анализировать изменения кадрового состава и выявить влияние стажа работы на его изменение. Несмотря на то, что на текучесть кадрового состава влияют различные параметры, одним из важных является стаж работы.

Кадровый состав [1] – это совокупность всех работников, занятых на предприятии и входящих в его штатный состав, вне зависимости от их профессионально-квалификационных групп.

Кадры включают в себя специалистов, рабочих, технических сотрудников и руководителей (вместе - группа служащих), а также работников охраны, учеников и младший обслуживающий персонал.

Специалисты - это сотрудники, которые подготавливают производство, осуществляют инженерное его сопровождение и продажу продукции.

Рабочие кадры - это лица, занятые непосредственно созданием продукции. Делится данная категория на две группы: основные и вспомогательные. Основные рабочие непосредственно своими руками и посредством орудий труда создают из материалов конечный продукт. Вспомогательные обеспечивают материалами, сырьем, энергией, топливом, транспортом и т. д.

Ключевая задача разработки проекта состоит в том, чтобы определить как влияет параметр стажа работы на текучесть кадрового состава на предприятии.

В качестве параметров рассматривались данные, опубликованные компанией РОСАТОМ на сайте «Цифровой прорыв».(1. Данные для анализаРисунок 1).

период	01.01.2020					31.01.2020						
							Отсутствия в отчетном периоде					
ID	Должность	Дата рождения	Пол	Семейное положение	Дата приема	Дата увольнения (если была в отчетном периоде)	Наименование отсутствия	Календарные дни отсутствия	Оклад/тариф на конец отчетного периода	Город в адресе регистрации на конец отчетного периода	Количество детей
23854332	Ведущий инженер	9/16/1956	женский	Разв.	8/19/1982				38,600.00	Москва	1
23854336	машинист	8/30/1959	мужской	Жен/ЗМ	10/2/2001				25,200.00	Москва	2
23854339	инженер	11/11/1979	мужской	Жен/ЗМ	9/27/2001				42,300.00	Москва	1
23854353	начальник смены	5/6/1979	мужской	Жен/ЗМ	10/9/2001		Прочие отсутствия	1	65,000.00	Москва	1
23854358	Ведущий инженер	10/3/1962	мужской	Жен/ЗМ	4/2/1993				52,500.00	Москва	1
23854360	заведующий хозяйством	8/8/1956	женский	Жен/ЗМ	6/29/1982		Лист нетрудоспособности	5	29,500.00	Москва	1
23854379	заместитель начальника отдела	3/19/1963	мужской	Жен/ЗМ	10/31/2001				84,000.00	Москва	3
23854408	инженер	3/28/1965	мужской	Жен/ЗМ	4/9/1993				42,300.00	Москва	2
23854414	электрослесарь	6/3/1972	мужской	Жен/ЗМ	4/22/1993		Лист нетрудоспособности	4	37,200.00	Москва	1
23854414	электрослесарь	6/3/1972	мужской	Жен/ЗМ	4/22/1993		Прочие отсутствия	1	37,200.00	Москва	1
23854418	машинист	5/13/1961	женский	Жен/ЗМ	9/6/1994				25,200.00	Москва	2
23854420	эксперт	3/9/1952	женский	Вдов.	12/13/1983				65,000.00	Москва	2
23854425	начальник смены	8/30/1959	мужской	Жен/ЗМ	3/24/1993				58,500.00	Москва	1

Рис. 1. Данные для анализа

Чтобы анализировать данные, необходимо разобраться в алгоритме расчета стажа работы.

Трудовой стаж [2] — в законодательстве Российской Федерации время (продолжительность) трудовой или другой общественно полезной деятельности работника. Является основанием для возникновения права на пенсионное обеспечение, отпуск, получение пособия по временной нетрудоспособности, а также в ряде ситуаций — заработной платы.

Данные (рисунок 1) представлены в табличном виде. Пользователь не может наблюдать динамческое изменение кадров, тем самым невозможно анализировать такой тип данных.

Приложение имеет способность обрабатывать (фильтровать) данные по различным критериям (размер заработной платы, тип образования, наличие детей и т.д.).

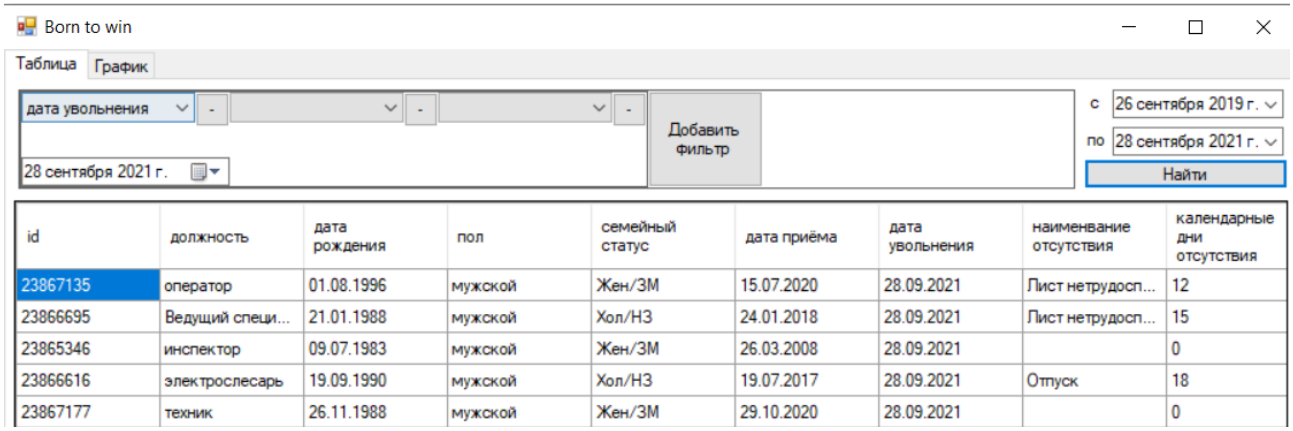


Рис. 2. Работа с данными

Чтобы построить график зависимости числа уволенных от стажа работы, необходимо обработать данные следующим образом:

– Подсчитать количество человек, уволевшихся с предприятия;

– Рассчитать стаж работы в организации.

Стаж работы в организации – это время, которое субъект проработал в организации. Тем самым можно сказать, что это разность даты окончания работы и даты приема на работу.

Чтобы подсчитать количество человек, уволившихся именно за какое-либо время, необходимо привести разность дат к единому формату (даты из формата ЧЧ.ММ.ГГГГ преобразованы в формат <M> – число месяцев).

Далее необходимо произвести подсчет одинакового стажа работы. Для этого нужно сложить одинаковый стаж работы и посчитать по количеству. (Рисунок 3).

Данный график отображает зависимость числа ухода работников от стажа их работы в организации РОСАТОМ.

Анализ результатов

Анализируя данные, показанные на рисунке 3 – можно сделать вывод о том, что текучесть кадрового состава организации резко возрастает сразу после приема на работу, это значит что субьект, устроившийся на работу в первые 6 месяцев увольняется. «Пик» ухода сотрудников возникает на 5-6 месяце после приема на работу. В это время большой показатель текучести кадров. Далее

необходимо заметить, что с течением времени текучесть кадров постепенно уменьшается.

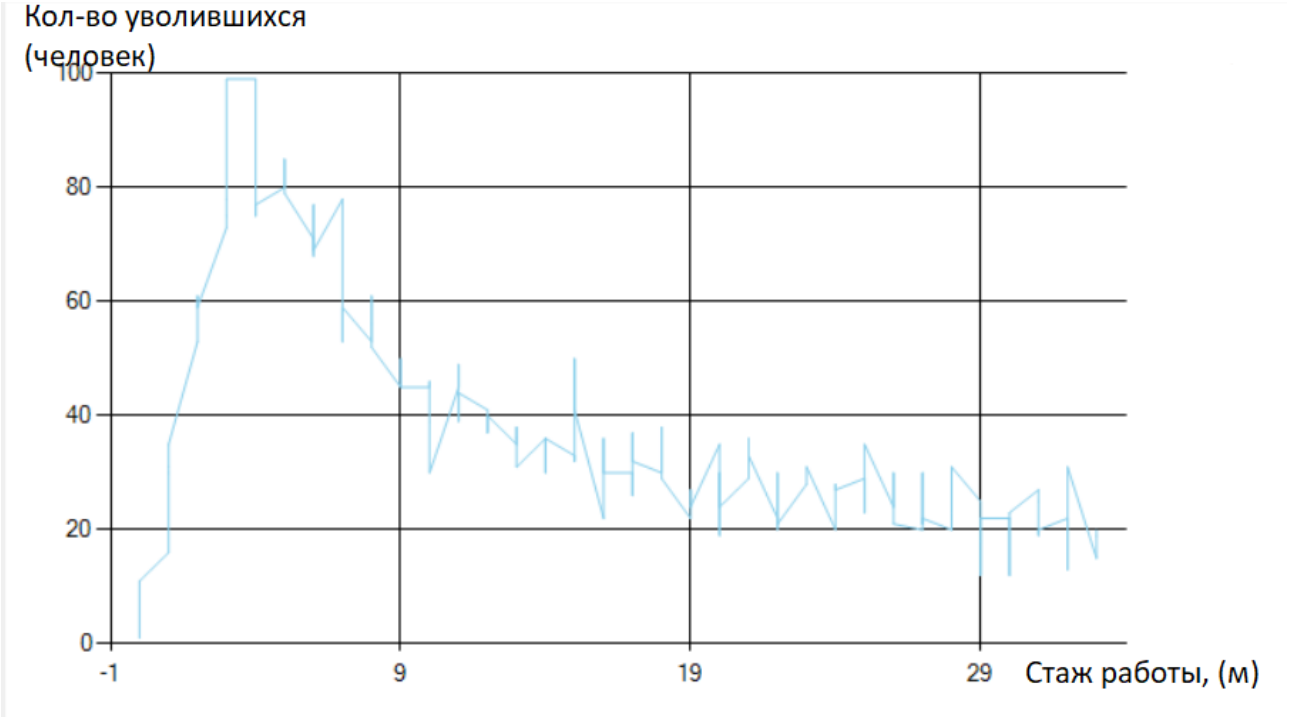


Рис. 3. График зависимости

Таким образом, можно производить глубокий анализ текучести, и менять условия работы, чтобы повлиять на столь высокую текучесть в первый год работы в компании.

СПИСОК ЛИТЕРАТУРЫ

1.Интернет-ресурс «Гугл»
URL: https://www.google.com/search?q=что+такое+стаж+работы+определение&client=opera-gx&sxsrf=AOaemvJKqMd-EUNNFECgLf1m6_S2TWUkLw%3A1632835588832&ei=BBhTYbCXMor0rgTjkKXQBg&oq=что+такое+стаж+работы+определение&gs_lcp=Cgdnd3Mtd2l6EAMyCAghEBYQHRAeMggIIRAWEB0QHjoHCAAQRxCwAzoFCAAQgAQ6BggAEBYQHjoFCCEQoAFKBAhBGABQnrYEWPPDBGDZxgRoAXACeACAAZwBiAH9C5IBBDAuMTKYAQCgAQHIAQjAAQE&sclient=gws-wiz&ved=0ahUKEwiwqf7J4qHzAhUKuosKHWNICWoQ4dUDCA0&uact=5. (Дата посещения 28.09.21)
2.Интернет-ресурс «Кадровый состав»
https://unisto-petrostal.ru/kadrovyi-sostav-primer-trudovye-resursy-personal-i-kadry-organizacii.html(Дата посещения 28.09.21)

УДК 004.946

А. В. ШУНДЕЕВ, В. А. ГЛУЩЕНКО, Д. В. ШЛЕНКИН, М. А. ИВАНОВ
artem_shundeev@mail.ru, val_g_2001@bk.ru, kot.dima2011@yandex.ru, aa4052783@gmail.com
Науч. руководит. – канд. техн. наук, доц. А. С. КОВТУНЕНКО

Уфимский государственный авиационный технический университет

ПРИМЕНЕНИЕ МАШИННОГО ЗРЕНИЯ В ПРОИЗВОДСТВЕ ДЛЯ ПОИСКА ДЕФЕКТОВ В СОЕДИНЕНИЯХ ЗВЕНЬЕВ ТКАННОЙ ПРЕФОРМЫ ИЗ УГЛЕВОЛОКНА

Аннотация. Рассматривается упрощение процесса визуального контроля по поиску дефектов деталей, для уменьшения трудоемкости процесса и исключения ошибок, связанных с человеческим фактором, с использованием нейронных сетей и распределенной системы контроля версий.
***Ключевые слова*:** нейронная сеть; интерактивная графическая среда; групповая разработка; распределенная система контроля версий; репозиторий.

Актуальность работы

Технологии нейронных сетей все чаще получают развитие в сфере автоматизации какого-либо процесса в различных отраслях экономики и производства. Одним из основных вариантов применения нейронных сетей является разработка автоматизированных технологических процессов производства. Особенно актуально применение искусственных нейронных сетей при обучении машинного зрения, которое позволяет отслеживать изменения объектов на сцене видеофайла, а также поиска дефектов детали.

Применении технологии машинного зрения позволяет уменьшить высокую трудоемкость и вероятность возникновения ошибок ввиду высокой плотности плетения и его рисунка. Также использование данных технологий позволяет снизить расходы и адаптировать программное обеспечение под изменяющиеся требования и технологии. Таким образом, применение технологии машинного зрения обеспечивает быстроту и эффективность, экономию ресурсов, гибкость.

Ключевая задача разработки проекта состоит в том, чтобы найти дефектные детали, улучшить и модернизировать контроль качества.

Данные были представлены ОДК-РГАТУ (Рисунок 1).

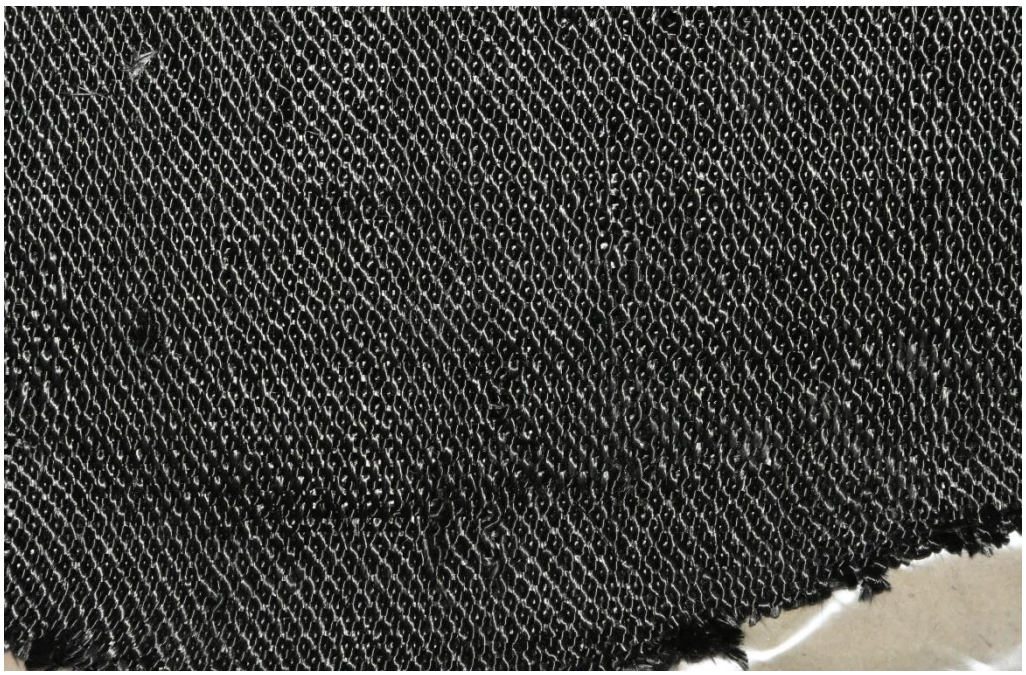


Рис. 1. Data set

Чтобы нейронная сеть с наибольшей вероятность нашла дефект детали, необходимо первоначально обработать фотографию (Рисунок 2).

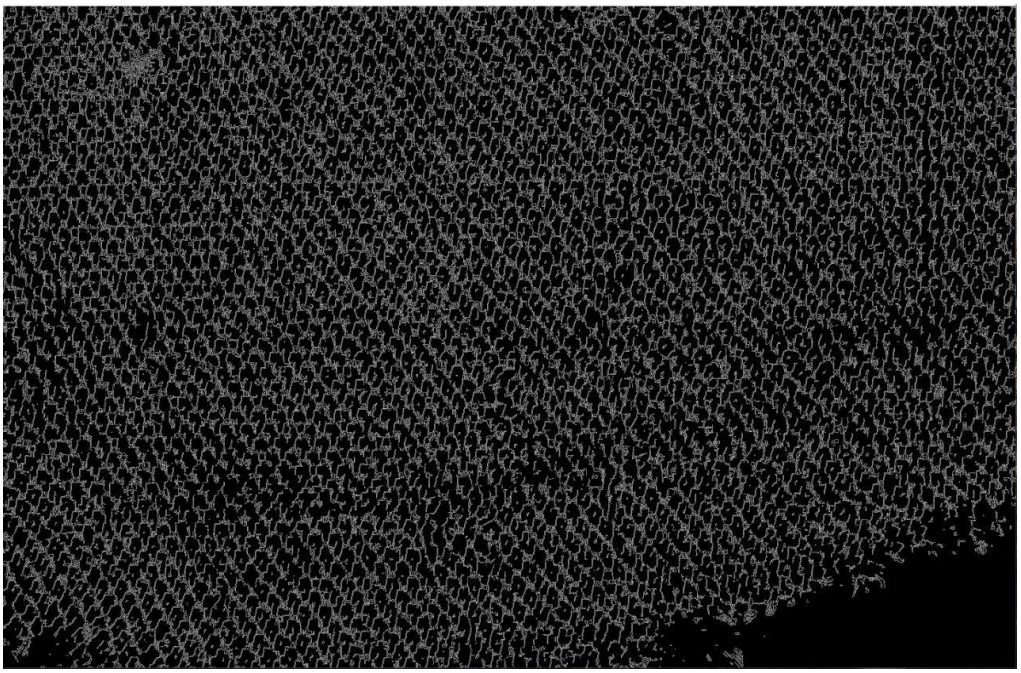


Рис. 2. Изображение после предобработки

После получения готового изображения, происходит кодирование изображения в матрицу. С этими данными продолжает работать нейронная сеть, которая была ранее обучена методом «учитель ученик» на предоставленном нам Data set.

По завершении работы искусственной нейронной сети, данные об обработке записываются в таблицу, и на фотографии выделяется область с дефектом (Рисунок 3).

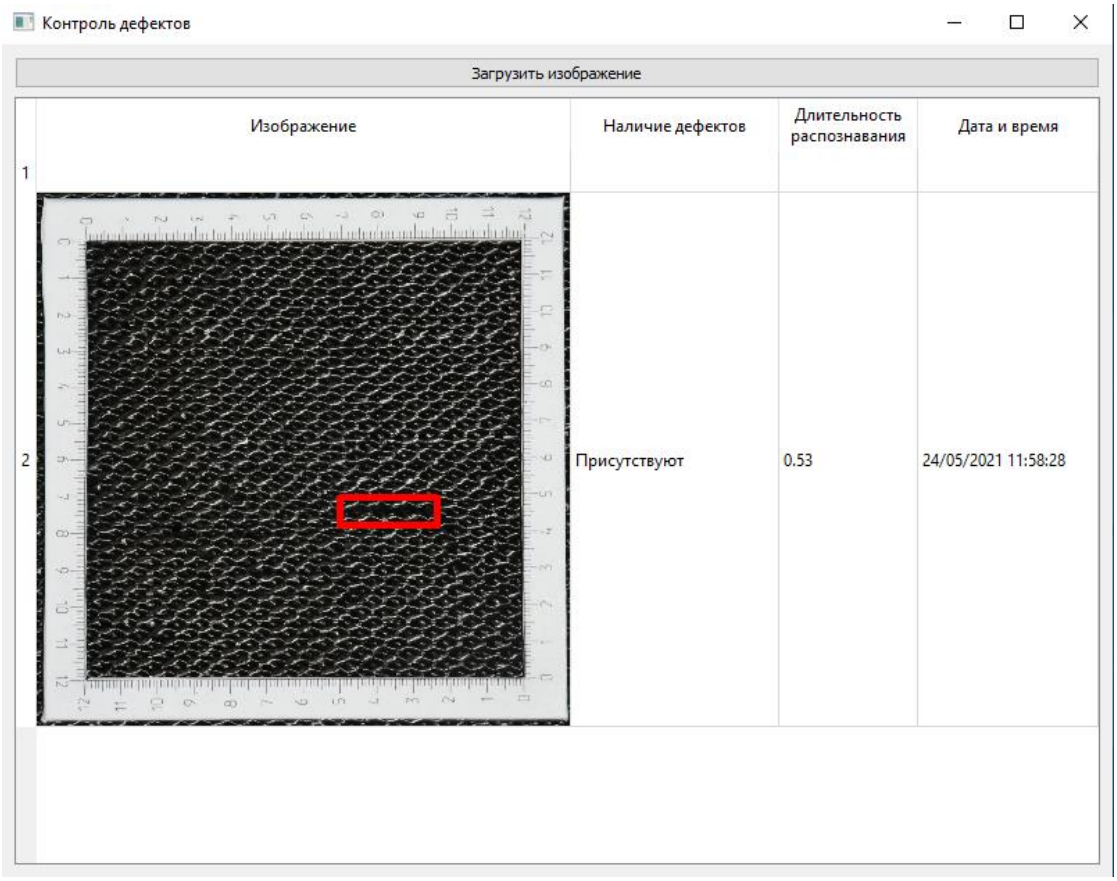


Рис. 3. Результат функционирования программы

Анализ результатов

Анализируя данные, показанные на рисунке 3– можно сделать вывод о том, что машинное зрение уменьшает трудоемкость процесса, тем самым увеличивая скорость обработки данных, и исключает ошибки, связанные с человеческим фактором.

Таким образом, можно автоматизировать и ускорить процесс поиска дефектов в соединениях звеньев тканной преформы из углеволокна. Тем самым, дать возможность, наращивать обороты производства тканной преформы из углеволокна.

СЕКЦИЯ 5.11
ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ

УДК 336

А. А. АБДРАХМАНОВА, В. А. ДОЛЖЕНКО
honey.adelka@list.ru, lera-k-pop@mail.ru
Науч. руководит. – канд. экон. наук, доц. А. В. СТАРЦЕВА

Уфимский государственный авиационный технический университет

ВЛИЯНИЕ ОФШОРНЫХ ЗОН НА ЭКОНОМИЧЕСКУЮ БЕЗОПАСНОСТЬ СТРАНЫ

Аннотация. При неблагоприятных экономических условиях для бизнеса многие предприятия переносят свою деятельность в так называемые «налоговые гавани» – офшорные зоны. Одна из самых существенных угроз экономической безопасности Российской Федерации – это уход от налогообложения, вывоз капитала, а также переводы активов в оффшорные компании. Перевод активов в оффшорные юрисдикции, а также перевод управления российскими организациями в оффшорные компании создает одну из самых значительных угроз экономической безопасности. В работе рассмотрены основные характеристики таких зон, схемы и методы их использования и исходящие от них угрозы для экономики России.

***Ключевые слова*:** оффшор; офшорные зоны; экономика; экономическая безопасность; методы борьбы; офшорные схемы; вывод капитала; противоправная деятельность; отмывание денег; деофшоризация; налоги; капитал; инвестиции.

Офшорной зоной называют страну или территорию, предоставляющую иностранным компаниям особые условия для ведения бизнеса. Очень низкие или даже нулевые налоги (налог на прибыль из внешних источников либо взимается по низкой ставке, либо не берется вообще; налог на имущество берется по очень низким ставкам; налоги с доходов физических лиц существенно ниже средних значений ставок по этим налогам в развитых странах и т.д.), простые правила отчетности и управления компаний, возможность скрыть настоящих владельцев бизнеса. Офшорных зон в мире насчитывается около полусотни. Владельцы компаний и просто богатые люди тратят меньше денег на налоги или не тратят вовсе и имеют возможность скрыть свою деятельность от государственных органов.

В условиях, когда интересы государства требуют принятия жестких мер по увеличению налоговых поступлений в бюджет и пресечению незаконного

вывоза зарубеж российского национального богатства, проблемы, связанные с оффшорными зонами и в целом с оффшорным бизнесом в России являются одними из самых актуальных. От их успешного решения во многом зависит экономическая безопасность страны.

Оффшорные зоны играют опасную роль для национальных экономик, в первую очередь в процессе «отмывания денег». Это одна из основных угроз, исходящих от оффшорных зон.

Если бы эти активы были вложены в отечественную экономику, они могли бы увеличить объемы производства и доходы бюджета от налогов, которые можно было бы потратить на развитие инфраструктуры и социальные программы страны, но вместо этого их большая часть пошла на приобретение зарубежных активов.

В России также незаконный вывоз капитала и доходов в оффшорные зоны приобрел большие масштабы и является острой проблемой. Внастоящеевремяточнонеизвестенразмер выведенногокапитала из России, но за 25 лет по подсчетам аналитиков Bloomberg Economics общая сумма составляет как минимум 750 млрд долл., и это почти 50% годового ВВП страны, другими словами, около трех годовых бюджетов РФ, это серьезный ущерб для страны.

Наблюдается также сокращение государственного бюджета за счет снижения налоговых поступлений, внутренних инвестиций, усиление государственной зависимости от иностранных займов, нарушение устойчивости финансового рынка страны, структурные деформации в экономике (бесконтрольный оффшорный бизнес ведет не только к уменьшению доходной части государственного бюджета, но и к изменению структуры национальной экономики за счет угнетения отечественных производителей товаров для внутреннего рынка и увеличения крена в сторону преимущественного развития экспортноориентированных и зависящих от импортных поставок отраслей экономики). Все это негативно сказывается на конкурентоспособности страны на мировом

рынке и в совокупности приводит к дальнейшему ослаблению экономики России.

Несовершенство таможенного, валютного, банковского и иммиграционного законодательства, «прозрачность» границ привлекают в Россию зарубежные оффшорные компании. Многие сделки и контракты совместно осуществляются оффшорными компаниями российского и иностранного происхождения.

Также существует множество и других исходящих угроз от оффшорных зон, которые в своей совокупности могут нанести значительный урон для экономики России, а именно:

– совершение и сокрытие налоговых преступлений. По мнению многих экспертов, банковская система Каймановых островов существует исключительно в целях уклонения от уплаты налогов;

– сокрытие настоящих организаторов и исполнителей финансовых преступлений путем создания оффшорных банков с представительским офисом. Оффшорный банк, как правило, не имеет в стране регистрации действующего офиса. Любая корреспонденция, которая прибывает, затем пересылается согласно инструкциям, местным агентством в страну нахождения истинного владельца: Канаду, Германию, США и т.д. В случае вопросов со стороны органов власти директора офисов утверждают, что они – просто советники и не занимаются банковскими операциями;

– финансовое мошенничество под прикрытием банковской деятельности. Криминальные оффшорные банки часто предлагают различные банковские услуги, например, депозитные сертификаты с необычно высокими процентными ставками. Через некоторое время данные банки ликвидируются, не рассчитавшись по своим обязательствам;

– все более широкое распространение получает практика использования оффшорных компаний в качестве элемента процесса легализации криминальных фондов денежных средств. Например, владелец финансовых фондов пре-

ступного происхождения учреждает холдинговую оффшорную компанию, затем приобретает от ее имени объект недвижимости за рубежом и в дальнейшем распоряжается этой недвижимостью на им же самим оговоренных условиях. Под залог этой недвижимости может быть получен кредит в иностранном банке на хороших условиях, а средства вновь использованы в легальном или нелегальном бизнесе. В результате возможности установить источник происхождения капитала еще более сокращаются.

Использование хозяйствующих субъектов, которые ведут свою деятельность на территории Российской Федерации, а центр накопления прибыли размещают за ее пределами, приводит, с одной стороны, к сокращению налоговых поступлений в российский бюджет, а с другой – к несанкционированной утечке капитала за рубеж. Таким образом, Россия финансирует целый ряд и без того благополучных стран, испытывая при этом острую потребность в инвестициях для модернизации собственной экономики.

Не менее опасны и политические последствия бегства оффшорного капитала, которые заключаются в недоверии российских капиталовладельцев к своему государству, к тому, что оно может реально гарантировать сохранность их капиталов.

Аналитики отмечают, что в последние годы отток замедлился. Неясно, стало ли это следствием более жесткого контроля или же денежные потоки лишь стало сложнее отслеживать, а также могли сыграть роль проводимая ЦБ расчистка банковского сектора, борьба с теневой экономикой и антироссийские санкции, вынудившие российских олигархов начать возврат денег в Россию, а также объявленная властями амнистия капиталов.

Современные оффшорные зоны можно подразделить на 5 групп.

К первой группе можно отнести Карибский бассейн. Основные удобства этой зоны: можно осуществлять некоторые простые сделки, отсутствие контроля со стороны проверяющих органов, нет отчетности и налогообложения. Все проводимые здесь сделки отличаются полной секретностью и конфиденци-

альностью, предоставление сведений о владельце-собственнике компаний не требуется.

Ко второй группе можно отнести некоторые острова, такие как Гернси, Джерси и Мэн. Предпринимательскую деятельность здесь можно осуществлять аналогично, без предоставления отчетности и уплаты налогов. При регистрации фирмы определенные данные о владельцах предоставлять необходимо.

К третьей группе можно отнести Гибралтар и Кипр, где установлены определенные незначительные налоговые уплаты. Деятельность компаний на этих территориях подлежит обязательным аудиторским проверкам. Хотя для открытия бизнеса в этой зоне необходимо значительное количество средств, эти зоны считаются престижными и пользуются популярностью у бизнесменов.

К четвертой группе можно отнести Люксембург и Швейцарию. Здесь также установлены некоторые налоговые нагрузки, которые при выполнении некоторых условий можно использовать льготы. Эта оффшорная зона также пользуется определенной популярностью у отечественных предпринимателей.

Пятая группа включает в себя некоторые страны Азии: Сингапур, Малайзию и Гонконг. В этой зоне также обязательны регистрация и предоставление данных о владельце компании. Предпринимательская деятельность фирм подлежит обязательному аудиту. В Малайзии предусмотрен налог в размере 3 %, а для Гонконга и Сингапура налоговых обязательств нет.

Существуют международные организации (ОЭСР, FATF и другие), которые выпускают рекомендации для государств о том, как строить политику и законодательство в области офшоров.

Некоторые страны, в том числе и Россия, создают законы, пытаются применять какие-то меры, направленные на закрытие границ для «вывоза» капитала. Однако против законных способов государство ничего не сможет сделать. По прогнозам некоторых специалистов, движение денег через оффшорные зоны будет обязательно расти.

Наиболее известным способом борьбы с оффшорными организациями является установление так называемых правил контролируемых иностранных компаний. Данные правила предусматривают налогообложение граждан или юридических лиц – резидентов своих стран – в случае, если контролируемые ими иностранные компании (как правило, зарегистрированные в оффшорных зонах), получают какой-либо доход. Иными словами, неважно, распределены ли дивиденды в пользу таких контролирующих лиц или нет, они в любом случае должны уплатить налог с дохода, который получила подконтрольная им иностранная компания. «НК РФ (часть первая) от 31.07.1998 N 146-ФЗ (ред. от 17.02.2021)».

Другой способ борьбы с безналоговыми компаниями, который используется во многих государствах, связан со статусом так называемого «налогового резидентства» юридического лица. Данная концепция предполагает налогообложение доходов компании, зарегистрированной в одном государстве, на территории другого. В случае если ключевые решения, относящиеся к деятельности иностранной компании, принимаются резидентами, находящимися на территории этого другого государства, весь доход оффшорной компании подлежит налогообложению в государстве, где принимаются соответствующие решения. Федеральный закон от 24 ноября 2014 г. N 376-ФЗ «О внесении изменений в части первую и вторую Налогового кодекса Российской Федерации (в части налогообложения прибыли контролируемых иностранных компаний и доходов иностранных организаций)».

В некоторых других случаях методы борьбы могут быть связаны с применением повышенных налоговых ставок для компаний, которые каким-либо образом ведут бизнес с офшорами, ограничением банковских операций с такими компаниями, внесением оффшорных зон в «черные» списки, что влечет за собой специальный контроль и дополнительную отчетность для оффшорных компаний.

Таким образом, можно с уверенностью говорить о том, что офшорный бизнес является планетарным явлением, имеющим огромное влияние на экономико-политическую ситуацию во всем мире. Офшорные финансовые центры представляют собой потенциальную угрозу стабильности не только российской экономики, но и всей мировой финансовой системы. Это наносит существенный урон экономической безопасности Российской Федерации.

По-настоящему бороться с офшорами можно только создав у себя в стране благоприятные условия для бизнеса, и на законодательном и на правоприменительном уровне. В условиях отсутствия возможности защитить свой бизнес и свою собственность интерес бизнесменов к офшорам неискореним. А бороться с коррумпированными чиновниками и главами госкорпораций нужно не формально, а законодательно закрепив эффективные механизмы их ответственности. И оценивать признаки аффилированности нужно не по формальным и узким критериям, которые легко обойти, а всесторонне исследовав истинные связи чиновников с офшорными компаниями и подставными российскими юрлицами.

СПИСОК ЛИТЕРАТУРЫ

1. Налоговый Кодекс РФ (часть первая) от 31.07.1998 N 146-ФЗ (ред. от 17.02.2021)
2. Федеральный закон от 24.11.2014 г. N 376-ФЗ «О внесении изменений в части первую и вторую Налогового кодекса Российской Федерации (в части налогообложения прибыли контролируемых иностранных компаний и доходов иностранных организаций)».
3. Федеральный закон "О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма" от 07.08.2001 N 115-ФЗ.
4. Басова С.А. Офшоризация как закономерность глобализации и ее воздействие на экономику России // Автореферат дис. канд. экон. наук. – Кемерово, 2006. – С. 19.
5. Воронина А.М. Эволюция офшорного бизнеса // Финансы и кредит. – 2006. – №13. – С. 44–47.

УДК 336

А. Р. АБДУЛХАКОВА, Д. Р. ТИМЕРГАЛИНА
darina.timergalina@mail.ru
Науч. руководитель – ст. преп. О. П. МЕНДЕЛЬ

Уфимский государственный авиационный технический университет

ВАРИАНТЫ И СПОСОБЫ РЕАЛИЗАЦИИ ПРЕДНАМЕРЕННОГО БАНКРОТСТВА В РОССИИ

Аннотация. В период нестабильности экономики, все больше предприятий прибегают к осуществлению преднамеренного банкротства как к способу уклонению от исполнения обязательств перед различного рода контрагентами, сотрудниками, налоговыми органами. В связи с этим, выявление признаков преднамеренного банкротства на предприятии и формирование механизмов подобной диагностики является частью обеспечения экономической безопасности.
Ключевые слова: преднамеренное банкротство; признаки преднамеренного банкротства.

Рыночная экономика по сравнению с иными экономическими моделями предлагает почти каждому человеку возможность, шанс стать участником свободного рынка и получить не ограниченный ничем доход или норму прибыли. Но свобода имеет свою обратную сторону, которая чаще всего выражена в том, что не все, кто решил стать предпринимателем или бизнесменом, могут достичь поставленных целей.

Актуальность темы работы обусловлена тем, что довольно часто встречаются случаи, когда с целью уклонения от погашения сложившейся задолженности перед кредиторами либо в иных корыстных целях недобросовестные должники способны умышленно совершать действия (бездействия), приводящие к банкротству хозяйствующего субъекта. В настоящее время проблема обеспечения экономической безопасности организаций при наличии риска преднамеренного банкротства входит в число наиболее важных проблем антикризисного управления.

Преднамеренное банкротство можно расценивать как умышленное уклонение от исполнения своих обязательств, которое стало причиной материального ущерба другому лицу. Факт нанесения ущерба здесь заключается в том, что

кредитор, имеющий право требовать от должника выплаты положенной суммы, не получает ее.

Однако сам факт вины еще необходимо доказать – банкрот, в действиях которого усматриваются признаки преднамеренного банкротства, попадает под действие презумпции невиновности – другими словами, пока не доказан факт нарушения им норм закона, он считается невиновным.

Задача сбора доказательств возлагается на финансового управляющего – нейтрального и беспристрастного участника процесса. В рамках своей компетенции он проводит анализ экономических операций потенциального банкрота за определенный период, предшествующий подачи им заявления о собственной несостоятельности. При выявлении признаков преднамеренного банкротства соответствующее уведомление направляется в правоохранительные органы.

В качестве таких признаков могут рассматриваться различные действия:

– денежные переводы в пользу аффилированных лиц;

– продажа недвижимости, автомобиля и другого дорогого имущества по заведомо заниженной стоимости;

– возврат долгов отдельным кредиторам в нарушение установленной законом очередности;

– проведение изначально убыточных сделок.

Ответственный за выявление признаков преднамеренного банкротства и сбор доказательной базы –арбитражный управляющий. Выявление аферы происходит через аудит или инвентаризацию.

Проблемные вопросы в данной сфере:

– имеются достаточно сложные и мало изученные проблемы оценки ситуации, связанные с преднамеренным банкротством.

– отсутствует эффективный механизм выявления признаков преднамеренного банкротства;

– имеет место несовершенство методических рекомендаций по выявлению и расследованию преднамеренного банкротства.

Статистика банкротств физических лиц в 2018 году такова, что граждане сами инициировали банкротство в 86,1% случаях, а в 2019-2020 годах таких инициатив стало больше на 4,6% – 90,7% делопроизводств.

В сентябре 2020 года суды признали несостоятельными рекордные 12 225 человек, что на 94,6% больше, чем в сентябре 2019 года.

Столичный регион традиционно лидирует по абсолютному числу граждан-банкротов, но темпы роста количества процедур здесь ниже, чем в целом по стране. В таблице 1, приведены лидеры-регионы по количеству граждан банкротов за 2019-2020 год.

Таблица 1

Лидеры-регионы по количеству граждан-банкротов

Наименование региона	Количество граждан-банкротов (чел)	Прирост (%)
Москва	4585	30,6
Московская область	3957	38,9
Самарская область	3521	71,4

Таким образом, интерес граждан к освобождению от долгов через личное банкротство постоянно растет, поскольку процедуры становятся понятнее и дешевле, а граждане – более информированы. Также в перспективе количество банкротств будет увеличиваться за счет должников, чье финансовое положение ухудшилось за время пандемии. В связи с этим и в начале 2021 года можно ожидать, что число новых банкротов будет удваиваться к таким же периодам предыдущего года, как это происходит в последние месяцы.

СПИСОК ЛИТЕРАТУРЫ

1. Леонов А.И. Использование органами внутренних дел экономической информации при выявлении преднамеренных банкротств / А.И. Леонов // Материалы научно-практической конференции. – Нижний Новгород, 2016. – С.129–133
2. Замураев В.С., Потапчук А.В. Недостатки судебной финансово аналитической экспертизы по делам о преднамеренном банкротстве // Экономика и бизнес: теория и практика. 2017.№5. С. 101104.
3. Электронный ресурс. URL: https://fedresurs.ru/news/8b77432d-3823-415d-8127-8d9cb71953f7?attempt=2 (дата обращения 17.03.21).

УДК 331.108

М. Б. АВАНЕСОВА, Р. А. НИГМАТУЛЛИНА
17_margo@mail.ru
Науч. руководит. – канд. пед. наук, доц. А. Ю. ФАРРАХОВА

Уфимский государственный авиационный технический университет

ДЕЛЕГИРОВАНИЕ ПОЛНОМОЧИЙ И ОТВЕТСТВЕННОСТИ КАК СПОСОБ ОБУЧЕНИЯ ПЕРСОНАЛА

Аннотация. В статье освящены понятия делегирования, ответственности, виды делегирования и полномочий, основные правила, методы и принципы делегирования, взаимосвязь делегирования и обучения персонала.
***Ключевые слова*:** делегирование; ответственность; полномочия; руководитель; исполнитель; принцип единоначалия; норма управляемости; организация.

Делегирование полномочий – это процесс передачи части функций руководителя другим управляющим или сотрудникам для достижения конкретных целей организации. Используется для улучшения и оптимизации рабочей силы руководителя. Другими словами, делегирование означает передачу задач и полномочий определенному лицу (сотруднику организации), которое принимает на себя ответственность за их выполнение [4].

Ответственность – отношение зависимости человека от чего-то (от иного), воспринимаемого им (ретроспективно или перспективно) в качестве определяющего основания для принятия решений и совершения действий, прямо или косвенно направленных на сохранение иного или содействие ему. Объектом ответственности могут быть другие люди, в том числе будущие поколения, общности, а также животные, окружающая среда, материальные, социальные и духовные ценности т.д. [5].

В психологии управления ответственность рассматривается как:

– готовность в собственных решениях или действиях учитывать интересы тех, кого касается решение;

– готовность отвечать за свои действия (что тесно связано с правом на самостоятельные действия);

– готовность отвечать за действия исполнителей задания, если контроль и анализ не установил их личной вины [1].

Важно понять, что делегирование полностью зависит от согласия человека взять на себя полномочия, что саму ответственность делегировать невозможно. Менеджер не может терять ответственность, передавая ее подчиненному. Хотя работник, несущий ответственность за выполнение задания, не обязан выполнять его лично, он остается ответственным за его удовлетворительное выполнение. Например, главврач хирургического отделения делегирует многие важные обязанности медсестрам, но, если пациент умрет из-за того, что сестра перелила ему кровь неправильной группы, отвечать будет главврач, которого могут даже привлечь к суду за преступную халатность. И если торговый агент не выполнит своих плановых заданий на год и в результате весь отдел сбыта не выполнит своего плана, отвечать перед коммерческим директором будет менеджер отдела сбыта, а не торговый агент [4].

Цели делегирования:

– разгрузить руководителей;

– вовлечь и заинтересовать работников;

– повысить профессионализм работников;

–повысить дееспособность нижних звеньев.

Обычно делегируются следующие виды работы:

– рутинная работа;

– специализированная деятельность (т.е. деятельность, которую ваши сотрудники могут выполнить лучше, чем вы);

– решение частных вопросов;

– подготовительная работа (проекты и т. д.).

Никогда не подлежат делегированию:

– постановка целей, окончательное решение по стратегическим вопросам;

– контроль результатов;

– мотивация сотрудников;

– задачи особой важности;

– задачи высокой степени риска;

– необычные, исключительные дела;

– актуальные, срочные дела, не оставляющие времени для объяснений или перепроверки;

– конфиденциальные задачи.

Полномочия представляют собой ограниченное право и ответственность использовать ресурсы организации, самостоятельно принимать решения, отдавать распоряжения и осуществлять управленческие решения.

Обучение персонала – совокупность действий, разрабатываемых в рамках единой концепции обучения организации и ориентированных на систематическое обучение персонала. При этом, данные действия оказывают позитивное влияние на изменение уровня квалификации и производительности работников всех иерархических уровней, удовлетворяя индивидуальную потребность в обучении и потребность организации в обученных сотрудниках.

Делегируя какое-либо поручение, мы создаем условия для обучения персонала (для получения новой информации, формирования умений у сотрудников подразделения), тем самым удовлетворяем потребности в образовании (повышение профессиональной компетентности без отрыва от производства), признании и другие потребности.

Часто сотрудники перекладывают решение собственных задач на руководителя. Это обратное делегирование. Чтобы избежать этой ошибки в делегировании полномочий, нужно помогать подчиненному только в действительно сложных случаях. Но не выполнять работу за него. Необходимо разделить одну трудную задачу на несколько более простых. Если сотрудник не справляется и с этими поручениями, причина в нежелании работать. В такой ситуации нужно подыскивать замену. Например, работник попросил помочь в подготовке сложного отчета. Начальник не стал тратить время на объяснения. Поручил ему собрать данные, изучить шаблоны документа у других сотрудников, составить

графики. По каждому этапу назначил сроки в день – два и потребовал промежуточных отчетов. Через три дня сотрудник предоставил всю необходимую информацию. Начальник показал, как сопоставить и проанализировать сведения, и в тот же день получил отчет. В итоге он потратил минимум личного времени, а подчиненный научился решать проблемы самостоятельно. В данной ситуации рассматривается пример хорошего делегирования и ответственный подход сотрудника к выполнению поставленной задачи.

Примером хорошего делегирования может послужить данная ситуация. Надежда устроилась на должность официанта в ресторан «Ширваншах». Через 4 месяца наступило лето, и все сотрудники по очереди уходили в отпуск, включая администратора Анастасию. Надежда не смогла взять отпуск, так как проработала в этом заведении очень мало. Но за хорошее проявление себя в работе, Надежде доверили должность администратора. Анастасия передала свои полномочия Надежде и обучила:

–работе с R-Keeper;

– ведению и учету по кассе;

– составлению графиков работы сотрудников;

– работе с документацией и инвентаризацией;

– и другим базовым навыкам администратора.

Благодаря хорошему делегированию со стороны Анастасии, Надежда успешно справилась со своими новыми обязанностями, после чего ее повысили до должности второго администратора.

Плохое делегирование и отсутствие ответственности с обеих сторон можно рассмотреть на данном примере. Из-за болезни староста Петрова поручила заполнить журнал заместителю старосте Даниловой, но не объяснила правила оформления. Данилова сделала это так, как посчитала правильным и сдала в деканат. Через день Петрова получила сообщение о том, что журнал заполнен неверно, и нужно в срочном порядке все исправить. Петрова предъявила претензию к Даниловой и сказала, что с ее стороны это был неответственный под-

ход к данному поручению, ведь можно было узнать все, что было непонятно у нее, а также в самом деканате и у старост из параллельных групп. Претензия была не совсем обоснованной, т.к. вина Петровой в данной ситуации тоже присутствует. Петровой необходимо было позаботиться о том, чтобы Данилова до конца поняла ее требования, и удостовериться в правильности заполнения журнала.

Из приведенных выше примеров можно сделать вывод, что правильно делегировать – это очень важный навык для руководителя, да и в принципе для любого человека. Кому-то это дано «от природы», а кому-то это качество нужно в себе развивать. Какими же способами? Существуют различные курсы, семинары, тренинги, а также проверенный способ «метод проб и ошибок», с помощью которого можно самостоятельно научиться делегированию полномочий.

Рассмотрим на примере. В университете студентам дали задание по маркетингу. Одним из условий выполнения задания было разделение на подгруппы из 3-4 человек. В каждой подгруппе преподаватель назначил капитаном по одному человеку, который будет распределять обязанности между студентами. Через неделю пришло время сдавать выполненные задания и оказалось, что не все подгруппы с ним справились. Капитан одной из подгрупп не справился со своей должностью и плохо распределил обязанности студентов в своей команде, из-за этого они не смогли выполнить задание в срок. В других подгруппах все справились с заданием вовремя, и капитаны извлекли из данного назначения полезные уроки по делегированию полномочий.

Делегировать – значит развивать своих подчиненных, поручать им более сложные и важные задачи, раскрывать их личностный потенциал. Делегируя задачи, полномочия, которые сотрудник ранее не делал, или делал не полностью, руководитель обеспечивает его развитие, невольно подталкивает его к приобретению новых знаний, умений, развитию способностей.

Процесс делегирования непременно сопровождается анализом определения навыков, необходимых для выполнения задания. Результат этого анализа есть критерий выбора исполнителя делегируемого задания [2].

Для того чтобы обучения персонала посредством делегирования полномочий и ответственности было успешным, необходимо учитывать следующие правила:

1) передавайте полномочия не из соображений престижа, а исключительно для пользы дела;

2) используйте делегирование как средство усиления уверенности подчиненных в своих силах;

3) будьте готовы поддержать того, кому делегировали задачу;

4) учитывайте то, что, получив задание, подчиненный может принять не самые точные, а порой и ошибочные решения;

5) делегируйте непосредственно, не используя передаточные звенья, чтобы избежать эффекта «испорченного телефона»;

6) в случаях, когда сотрудники совершают ошибки в выполнении делегированных функций, объективно разбирайте существо дела, суть ошибки, а не личностные качества, недостатки и просчеты подчиненного;

7) передав подчиненному задачу и соответствующие полномочия, не вмешивайтесь в ход ее решения без довольно веских оснований, т. е. до тех пор, пока не увидите, что могут возникнуть серьезные осложнения;

8) принимайте на себя ответственность за все решения, которые сделаны вашими подчиненными, получившими от вас необходимые полномочия;

9) «делегировать задачу надо не тому, кто хочет, а тому, кто может и способен ее решить» [3].

Таким образом, в данной работе удалось показать, что делегирование – это инструмент мотивации и развития сотрудников, позволяющий экономить время руководителя и способствующий повышению эффективности деятельности работников. Вовлекая сотрудников в процесс принятия решений, им предо-

ставляется возможность самореализоваться и почувствовать свою значимость в коллективе.

СПИСОК ЛИТЕРАТУРЫ

1. Гольдштейн Г.Я. Основы менеджмента//Учебное пособие, изд 2-е, дополненное и переработанное. Таганрог: Изд-во ТРТУ, 2003
2. Давидович О.С. // Ошибки в делегировании и чек-лист, который их исправит.URL: https://www.kom-dir.ru/article/1659-oshibki-v-delegirovanii?from=PW_Timer_mobile (Дата обращения 18.03.2021).
3. Делегирование: самая суть / Центр дополнительного образования «Элитариум». URL: http://www.elitarium.ru/delegirovanie-rukovoditel-polnomochija-sotrudnik-otvetstvennost-rabota-razdelenie-truda (Дата обращения 18.03.2021).
4. Мескон М., Альберт М., Хедоури Ф.Основы менеджмента // Management / Пер. Л. И. Евенко.– М.: Дело, 1997. – 704с.
5. Ореховский А. И. / Под общ. ред. А. И. Ореховского. – Новосибирск: СибГУТИ, 2005.

УДК 159.9.07

Р. С. АЗЫЛГАРЕЕВА
Az.rozalina@mail.ru
Науч. руководитель – канд. пед. наук, доц. А. Ю. ФАРРАХОВА

Уфимский государственный авиационный технический университет

СОЦИАЛЬНО-ПСИХОЛОГИЧЕСКИЙ КЛИМАТ КАК ПОКАЗАТЕЛЬ УРОВНЯ РАЗВИТИЯ ГРУППЫ

Аннотация. В статье представлен анализ значения социально-психологического климата в развитии группы, раскрывается его сущность. Описываются факторы, влияющие на уровень социально-психологического климата в коллективе. Представлены результаты тестирования по методикам «Диагностика делового, творческого и нравственного климата в коллективе» и «Оценка микроклимата студенческой группы» (В.М.Завьялова), рекомендации по развитию коллектива.
Ключевые слова: социально-психологический климат; трудовой коллектив; группа; социальное развитие; сплоченность; сотрудничество; ответственность.

Благоприятный социально-психологический климат – залог эффективной и производительной работы трудового коллектива на предприятии. В настоящее время существует множество стратегий по формированию благоприятного социально-психологического климата. В таблице 1 представлены самые распространенные методы формирования благоприятного социально-психологического климата, их характеристика с точки зрения достоинств и недостатков [2].

Понятие «психологический климат» по-разному интерпретировалось в психологической и управленческой среде, объединяя все новые и новые характеристики. В многочисленных определениях и интерпретациях социально-психологического климата, предложенных в современной науке, имеется одна общая черта: везде говорится о взаимодействии индивида с организационной средой (табл.1).

Таблица 1

Определение понятия «психологический климат»

Автор	Определение
К. Левин	Социальная атмосфера – некоторая совокупность психологических характеристик организационной среды.
Р.Таджури	Считает, что климат – это относительно устойчивое качество внутренней среды организации, которое ощущается членами этой организации, влияет на их поведение и может быть описано по ряду измерений.
Ш. Гадбуа	Климат организации представляет собой глобальное восприятие ее членами ряда общих, относительно устойчивых свойств этой организации и социальных воздействий, которые происходят внутри нее
С.Кузьмин	Под понятием считает такое социально-психологическое состояние малой социальной группы, которое определяет содержание и характер направленности психологии членов коллектива.
Н.Лутошкина	Подмечает что, суть основной характеристики социально-психологического климата является эмоциональный и психологический настрой всей группы. Другими словами это общее настроение.
А.Покровский	Анализирует социально-психологический климат через стиль взаимоотношений людей, которые находятся в непосредственном контакте друг с другом. Объясняют это так, в процессе формирования складывается система межличностных отношений в коллективе, определяющих психологическое и социальное самочувствие члена группы в отдельности.

Таким образом, можно выделить характеристики, которые называются различными авторами как обязательные признаки коллектива:

1) объединение людей в целях достижения определенной, коллективной цели;

2) наличие добровольного характера объединения, к тому же под добровольностью здесь понимается такая характеристика группы, когда она стала для индивидов, входящих в нее, системой построенных ими отношений на базе совместной деятельности;

3) единство (целостность), что выражается в том, что коллектив выступает всегда как некоторая система деятельности, которой присуще организация и распределение функций, определенная структура руководства и управления;

4) коллектив это особая форма взаимоотношений между его членами, которая гарантирует принцип развития личности вместе с развитием коллектива.

Основными факторами, влияющими на состояние социально-психологического климата в коллективе, являются смысл труда и степень удовлетворения работой; условия труда и быта, удовлетворенность ими; степень удовлетворения характером межличностных отношений с сотрудниками; стиль руководства, личность руководителя, а также степень его удовлетворенности подчиненными [4].

Благоприятный социально-психологический климат характеризуют оптимизм, радость общения, доверие, чувство защищенности, безопасности и комфорта, взаимная поддержка, теплота и внимание в отношениях, межличностные симпатии, открытость коммуникации, уверенность, бодрость, возможность свободно мыслить, творить, интеллектуально и профессионально расти, вносить вклад в развитие организации, совершать ошибки без страха наказания и т.д.

Неблагоприятный социально-психологический климат характеризуют пессимизм, раздражительность, скука, высокая напряженность и конфликтность отношений в группе, неуверенность, боязнь ошибиться или произвести плохое впечатление, страх наказания, неприятие, непонимание, враждебность, подозрительность, недоверие друг к другу, нежелание вкладывать усилия в совместный продукт, в развитие коллектива и организации в целом, неудовлетворенность и т.д. [6].

Для определения социально-психологического климата мною было проведено тестирование по методикам «Диагностика делового, творческого и нравственного климата в коллективе», «Оценка микроклимата студенческой группы» (В.М.Завьялова).Объектом исследования являются студенты 2-го курса в возрасте от 18-20 лет и студенты 4-го курса в возрасте от 21-23 лет.

По результатам тестирования по методике «Диагностика делового, творческого и нравственного климата в коллективе» у студентов 2-го курса доминирует средний уровень по всем трем качествам, что свидетельствует о том, что в группе преобладает ответственность, студенты стремятся к сотрудничеству,

коллективизму, но порой встречаются и конфликтные ситуации, проявление индивидуализма. В целом степень развития деловых качеств имеет удовлетворительную оценку. В тоже время отмечается некоторая социальная незащищенность, обман и средний уровень наличия условий для профессионального и культурного роста.

По результатам тестирования по методике «Диагностика делового, творческого и нравственного климата в коллективе» у студентов 4-го курса доминирует высокий уровеньпо творческому и нравственному качеству, и средний по деловому качеству, что свидетельствует о том, что в группе преобладает достаточно хороший и высокий психологический настрой. Студенты достаточно ответственные, решительные, целеустремленные, студенты стремятся к сотрудничеству, коллективизму.

В результате диагностики «Оценка микроклимата студенческой группы (В.М.Завьялова) тестирования по В.М.Завьялова» выяснилось, что у студентов 2-го курса преобладает средняя степень выраженности психологического микроклимата, что говорит о его неустойчиво благоприятной направленности. Средняя степень характеризуется системой межличностных и личных отношений, опосредованных содержанием коллективной деятельности и основными групповыми ценностями. Эти ценности у членов группы сходны, поэтому личные симпатии и антипатии отходят на второй план.

У студентов 4-го курса преобладает высокая степень выраженности, что характеризуется тем, что ядро межличностных и личных отношений опосредованно связями и отношениями к предмету коллективной деятельности, ее смыслу. На этом уровне сплоченность группы оказывается наиболее высокоразвитой и устойчивой. Для этого уровня характерна общность единств жизненных целей и жизненных планов членов группы, взаимопонимание и взаимоподдержка.

Основываясь на результатах исследования, можно сделать выводы, что у студентов 4 курса психологический климат в группе очень хороший, ониболее

сплоченные, больше знают друг о друге, преобладает коллективистический тип отношений: студенты воспринимают свой коллектив как самостоятельную ценность. На первый план у них выступают проблемы группы и отдельных ее членов, наблюдается заинтересованность, как в успехах каждого члена группы, так и группы в целом, стремление внести свой вклад в групповую деятельность. А на 2-ом курсе преобладает, скорее всего, более индивидуалистический тип отношений. Это означает, что студенты этого коллектива относятся к ней нейтрально, уклоняются от совместных форм деятельности, предпочитают индивидуальный тип работы. Это связанно с тем, что студенты 2-го курса еще не до конца со всеми познакомились и как лучше не узнали друг друга в отличии от 4 курса. В какой-то степени сильно повлияло дистанционное обучение так как целый год просидели дома и не контактировали в жизни друг с другом.

Таким образом, социально-психологический климат в коллективе – это не только проблема сегодняшних социально-психологических сложностей социального и научно- технического прогресса, но одновременно и проблема решения перспективных задач, связанных с моделированием новых, более совершенных, чем прежде, человеческих отношений и человеческих общностей. Проведенное исследование дает основание для дальнейшего изучение проблемы межличностных взаимоотношений в коллективе, а также для выработки эффективных путей их улучшения и благополучного развития.

Для оздоровления социально-психологического климата необходимо применить ряд организационных и социально-психологических приемов.

Организационные приемы предполагают:

1) проведение конкретного эмпирического исследования с целью определения причин неблагоприятных взаимоотношений студентов в группе;

2) принятие коллективного решения об устранении объективных факторов, негативно влияющих на климат;

3) контроль за реализацией коллективного решения и состоянием социально-психологического климата.

СПИСОК ЛИТЕРАТУРЫ

1. Бороздина Г. В. Психология и этика деловых отношений / Г. В. Бороздина. – Юрайт, 2008. – 464 с.
2. Коломинский Н.Л. Психология менеджмента в образовании. Социально-психологический аспект / Н. Л. Коломинский. К.: МАУП, 2000. 286 с.
3. Малимонов М. И. Социально-психологические методы и средства, влияющие на формирование положительного социально-психологического климата в коллективе // Закономерности и тенденции развития науки в современном обществе : сборн. междунар. научно – практ. конф. Красноярск., 2016. 148 – 152 с.
4. Маринко Г.И. Управленческий консалтинг: учебное пособие / Г.И. Маринко. – М.: Инфра-М, 2005. – 380 с.
5. Митасова А.А. Формирования благоприятного социально-психологического климата в коллективе / А.А. Митасова, И.В. Барыло // Мат. XVI междунар. науч.конф (9-10 декабря 2015 г.). – Донецк: «Донецкий национальный университет», 2015. – с. 572-574.

УДК 338

В. А. АЛЕКСЕЕВА, И. Г. КУЛУЕВА
vita.myr@mail.ru, ilzida.kulueva@mail.ru
Науч. руководв. – канд. экон. наук, доц. А. В. СТАРЦЕВА

Уфимский государственный авиационный технический университет

АНАЛИЗ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ НА ПРИМЕРЕ ПАО «ГАЗПРОМ»

Аннотация. В статье рассматривается анализ экономической безопасности предприятия нефтегазовой отрасли на примере ПАО «Газпром». При этом учитывается проведение анализа посредством отражения финансовой деятельности, проведения расчетов и сопоставление с нормативными показателями, которые отражают обеспечение экономической безопасности на предприятии. Рассматривается SWOT-анализ сильных и слабых сторон предприятия в области обеспечения экономической безопасности предприятия.
Ключевые слова: экономическая безопасность; финансовая устойчивость; финансовая безопасность; угрозы; SWOT-анализ.

ПАО «Газпром» является глобальной энергетической компанией. Миссией организации является эффективная работа системы реализации природного газа, обеспечение энергетическими ресурсами потребителей [8]. Для выполнения миссии ПАО «Газпром» стремится стать глобальным лидером, диверсифицируя рынки сбыта, повышая эффективность своей деятельности, увеличивая и используя свой научно-технический потенциал.

Первый шаг оценки экономической безопасности предприятия – составление матрицы SWOT-анализа (таблица 1).

Проведенный анализ позволяет сделать следующие выводы. Наибольший риск представляет собой сочетание слабых сторон корпорации с потенциальными угрозами для нее. Для решения возникающих вследствие этого проблем необходимо направлять наибольшее количество ресурсов компании, осуществлять постоянный мониторинг и контроль за внутренней и внешней средой. Сильные стороны при сочетании с возможностями позволяют минимизировать любые риски, возникающие перед предприятием, и осуществлять наиболее эффективную деятельность. Сочетание сильных сторон с угрозами также уменьшает риски или их воздействие на ПАО «Газпром. А взаимодействие слабых

сторон и возможностей вынуждает предприятие вести свою деятельность в условиях риска, что не раскрывает его потенциал.

Таблица 1

Матрица SWOT-анализа

Сильные стороны (S)	Возможности (O)
S1. Наличие значительной ресурсной базы, которая дает возможность оставаться лидером на рынке в России по объемам добычи газа и нефти, а также занимать лидирующие позиции по запасам ресурсов в мире среди аналогичных компаний. S2. Налаженный производственный процесс посредством выстраивания вертикальной интеграции, необходимой для деятельности инфраструктуры. S3. Значительные инвестиционные ресурсы и богатый опыт реализации проектов разного уровня и значения. S4. Наличие потенциала, позволяющего развить и повысить эффективность процессов переработки. S5. Значительный научно-технический, исследовательский и производственный потенциал [13]. S6. Выстроенная собственная сеть сбыта (до конечного потребителя) на территории России и экспортных терминалов.	O1. Деятельность на крупных месторождениях на территориях Восточной Сибири, которые обеспечивают налоговые льготы. O2. Государство дает приоритет при распределении стратегических месторождений. O3. Возможность разрабатывать новые технологии, использовать передовые технологии для ведения эффективной деятельности, возможность увеличить объемы реализации через собственную сеть сбыта конечному потребителю. O4. Разработка и реализация комплексных программ по расширению и совершенствованию экспортных терминалов для обеспечения их соответствия запланированным объемам экспорта - расширение экспортных возможностей. O5. Расширение использования природного газа как моторного топлива.
Слабые стороны (W)	Угрозы (T)
W1. Снижение доли рынка в России. W2. Государственный контроль создает рамки при реализации инвестиционных проектов (нацелены на решение государственных задач). W3. Подверженность политическим рискам разных государств и мирового политического сообщества в целом. W4. Высокие затраты на производство и реализацию продукции.	T1. Динамика мировых цен на газ, нефть носит труднопредсказуемый характер. T2. Наличие конкурентов на внешних, традиционных для России, рынках [8]. T3. Угроза сохранения или усугубления в долгосрочной перспективе санкций (дискриминационные нерыночные ограничения) со стороны западных стран по доступу к инновационным технологиям и заемным средствам [8].

Рассмотрим вышеуказанные элементы системы экономической безопасности применительно к ПАО «Газпром» (таблица 2).

Таблица 2

Расчет экономической безопасности ПАО «Газпром»

Название коэффициента	Min-допустимое значение	2017 г.	2018 г.	2019 г.
X1 – Коэффициент капитализации	>1	0,391	0,330	0,393
X2 – отношение оборотного капитала к общей сумме активов	>0,1	0,163	0,111	0,088
X3 – коэффициент оборачиваемости активов	>1	0,323	0,278	0,057
X4 – коэффициент текущей ликвидности	>1,5	2,517	2,150	1,742
X5 – коэффициент автономии (финансовой независимости)	>1	0,718	0,751	0,717
X6 – коэффициент рентабельности собственного капитала	>0,2	1,268	2,955	5,935
X7 – отношение нераспределенной прибыли к активам	>0,1	0,321	0,317	0,300
X8 – отношение текущих обязательств к текущим активам	>0,15	0,397	0,464	0,573
X9 – рентабельность активов от чистой прибыли	>1	0,466	1,085	2,130
X10 – коэффициент абсолютной ликвидности	>0,2	0,385	0,512	0,508
Z	>3	2,906	2,946	3,202

Полученные данные свидетельствуют о низком уровне угроз финансовой безопасности и устойчивой тенденции к ее укреплению.Оценка экономической безопасности была рассчитана по существующим методикам, результаты которых показали, что данные дискриминантные модели прогнозирования банкротства могут служить только для цели экспресс-тестирования компаний на риски экономической безопасности, поскольку они используют ограниченное количество узконаправленных факторов,кроме того, имеет значение отсутствие точного прогноза вероятности банкротства и нарушения экономической безопасности компании.

Результаты данной методики позволили выявить проблемные зоны ПАО «Газпром». Для устранения негативных тенденций и укрепления экономической безопасности руководству предприятия необходимо принять управленческие решения по следующим направлениям:

1) контроль капитализации. Дополнительное вливание капитала поможет

оптимизировать данный показатель;

2) нормирование отношения оборотного капитала к общей сумме активов. Необходимо обратить внимание на увеличение доли средств, необходимых для погашения долгов;

3) учет фактора оборачиваемости активов. Для улучшения показателя оборачиваемости актива для ПАО «Газпром» можно применить пересмотр тарифной политики;

4) отслеживание показателя финансовой автономии. Рекомендуется повышать долю активов, покрывающихся за счет собственного капитала, что способствует укреплению финансовой независимости ПАО «Газпром»;

5) поддержание рентабельности активов от чистой прибыли на необходимом уровне, целесообразно осуществлять управление с помощью специальной подсистемы в системе общего управления предприятием или специализированного подразделения в организационной структуре.

В качестве улучшения системы обеспечения экономической безопасности ПАО «Газпром» следует провести мероприятия, рассчитанные на долгосрочную перспективу:

– рекомендуется осуществлять регулярный мониторинг и диагностику экономической безопасности;

– рекомендуется обратить особое внимание на выявленные проблемные направления и для них разработать комплексные мероприятия по предотвращению угроз экономической безопасности.

СПИСОК ЛИТЕРАТУРЫ

1. Гражданский кодекс Российской Федерации. Федеральный закон от 30.11.1994 г. № 51-ФЗ (ред. от 29.12.2020).
2. Акмаева Р.И., Епифанова Н.Ш. Экономика организаций (предприятий). – М.: Феникс, 2018. – 496 с.
3. Арошидзе А. А. Информационная архитектура оценки экономической устойчивости промышленного предприятия / А. А. Арошидзе // Сборник материалов XLIII Международной научно-практической конференции «Актуальные вопросы науки». – М.: «Спутник +», 2018. – С. 32-34.

4. Бездольная Т. Ю., Малахова, Т.Ю. Оценка эффективности аудиторских проверок в условиях цифровизации аудита // Вестник Института Дружбы народов Кавказа Теория экономики и управления народным хозяйством. – 2019. – № 1 (49). – 20 с.
5. Васильева А.И. Осуществление анализа и оценки финансовой устойчивости в современных организациях // МИРЭА – Российский технологический университет. – 2018. – 53 с.
6. Казакова Н.А. Финансовый анализ: учебник и практикум для бакалавриата и магистратуры. – Москва: Издательство Юрайт, 2017. – 470 с
7. Погодина Т.В. Финансовый менеджмент: учебник и практикум для СПО. – Москва: Издательство Юрайт, 2019. – 351 с.
8. Официальный сайт ПАО «Газпром». [Электронный ресурс]. – Режим доступа: https://www.gazprom.ru/

УДК 331.101

Т. Е. БАБИКОВА, Е. Н. САЛМИНА
tanya.babikova02@mail.ru, salmina.yelena@list.ru
Науч. руководв. – канд. экон. наук, доц. А. Н. ШЕРЫШЕВА

Уфимский государственный авиационный технический университет

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ОРГАНИЗАЦИИ ТРУДА В РОССИИ И СТРАНАХ СКАНДИНАВИИ И АЗИИ

Аннотация. В публикации затрагивается тема особенностей организации труда и правового регулирования рабочего времени в Скандинавских странах, странах Азии и России. Особое внимание было обращено таким показателям как рабочее время, отпуск и выходные, пенсионный возраст и оплата труда. Проблема о которой идет речь, изучается многими авторами, но в сравнении с другими странами, поэтому наша статья построена на более тщательных исследованиях стран Скандинавии и Азии. В публикации приведен тщательный и детальный анализ производительности труда в трех странах.
Ключевые слова: безработица; рабочее время; особенности; принцип; переработка; сверхурочная работа.

Рабочее время является одним из центральных институтов трудового права. Изучение рабочего времени России на основе сравнения опыта зарубежных стран необходимо для выявления особенностей, определения целесообразности использования положительного зарубежного опыта.

В нашем докладе проанализирована проблема продолжительности рабочего времени в России и в ряде зарубежных стран на примере Скандинавских и Азиатских стран. Актуальность темы доклада обусловлена тем, что изучение рабочего времени в России на основе сравнения опыта зарубежных стран необходимо для определения целесообразности использования положительного опыта этих стран и восполнения существующих пробелов в знании зарубежного трудового права в этой сфере. Целью доклада является анализ правового регулирования ряда вопросов о продолжительности рабочего времени в России и в зарубежных странах. В статье сравниваются основные нормы трудового права развитых зарубежных стран и России, определяются особенности о продолжительности рабочего времени в зарубежных странах. Акцентируется внимание

на положительных и отрицательных моментах проблемы продолжительности рабочего времени в России и путях ее решения.

Рассмотрим особенности организации труда и правового регулирования рабочего времени в Скандинавских странах, странах Азии и России (табл. 1).

Таблица 1

Особенности организации труда

Показатели	Скандинавские страны	Страны Азии	Россия
Рабочее время	Фиксированное, гибкое Скользящий график работы представляет собой вид гибкого рабочего времени. Обычный режим рабочего времени предусматривает не более 40 часов в неделю на одном и том же рабочем месте.	Продолжительность рабочего времени в Японии по законодательству не должна превышать 40 часов в неделю или восемь часов в день без учета перерывов. Но некоторым предприятиям разрешено устанавливать рабочую неделю продолжительностью до 44 часов. Стандартный рабочий день с 9 утра до 7 вечера.	Согласно статье 91 ТК РФ нормальная продолжительность рабочего времени не может превышать 40 часов в неделю.
Выходные и отпуск	По шведскому закону все работающие на полную ставку имеют право на отпуск в количестве 25 дней в год. Можно получить денежную компенсацию за неиспользованное время отдыха, если вы уходите с работы, не успев «отгулять» свой отпуск. Она составляет 12 процентов от общей суммы зарплаты, заработанной в течение года. Почасовики получают компенсацию в счет отпуска в размере 12 процентов от их брутто-зарплаты.	работодатели обязаны давать работникам по крайней мере один выходной день в неделю или четыре выходных дня в месяц. В Японии нет отпусков. Выходные – это суббота или воскресенье. И, в зависимости от компании, вам положено несколько дополнительных выходных дней в году. Допустим, это 10 дней, но нельзя взять их сразу, а нужно разбить.	Ежегодный основной оплачиваемый отпуск предоставляется работникам продолжительностью 28 календарных дней. Ежегодный основной оплачиваемый отпуск продолжительностью более 28 календарных дней (удлиненный основной отпуск) предоставляется работникам в соответствии с настоящим Кодексом и иными федеральными законами

Окончание табл. 1

Оплата труда	Минимальная почасовая з/п в шведском государстве равняется примерно 100 кронам. Это равноценно 11 евро. Средняя зарплата в Швеции составляет примерно 3 770 евро до вычета налогов. Материальное благосостояние многих шведских семей практически равноценно финансовому благополучию датчан и немцев.	Средняя зарплата в Японии в разрезе профессий остается на высоком уровне и составляет примерно 120 000 долларов в год. Средним доходом японца считается заработная плата от 250 до 400 тысяч иен (130 000–205 000 рублей).	По официальным данным от Росстата, средний доход населения Российской Федерации в 2020 году составил 35 361 рублей в месяц (около 490 $), среднемесячная зарплата — 51 083 рублей (708 $), средняя пенсия — 14 986 рублей (208 $). Номинальная начисленная среднемесячная зарплата в 2020 прогнозируется в размере 47,531 тысячи рублей, в 2021 – 51,066 тысячи рублей, в 2022 – 54,131 тысячи рублей, в 2023 – 57,675 тысячи рублей
Пенсионный возраст	Шведское правительство раздумывает над тем, чтобы увеличить пороговый возраст выхода на пенсию:62 года вместо 61, как сейчас.	С учетом роста продолжительности жизни японцев в стране не раз обсуждали вопрос о повышении пенсионного возраста. Сейчас на пенсию там уходят, как правило, в 65 лет.	Согласно реформе, в 2021 году женщины будут уходить на пенсию с 56,5 лет, мужчины – с 61,5 года. К 2028 году пенсионный возраст женщин будет составлять 60 лет, для мужчин – 65 лет. Кроме возраста, гражданин должен иметь минимум 12 лет рабочего стажа и 21 пенсионный балл

В разных странах существуют особые явления, которые характеризуют отношение людей к своей работе.

В Японии есть проблема «смертей от переработок», существование которой подтверждается не только статистикой, но и самим японским языком, в котором есть даже слово, обозначающее это явление – «Karochi» (буквально переводится как «смерть от переработок»). Основные медицинские причины кароси – инфаркт и инсульт на фоне стресса и недоедания.

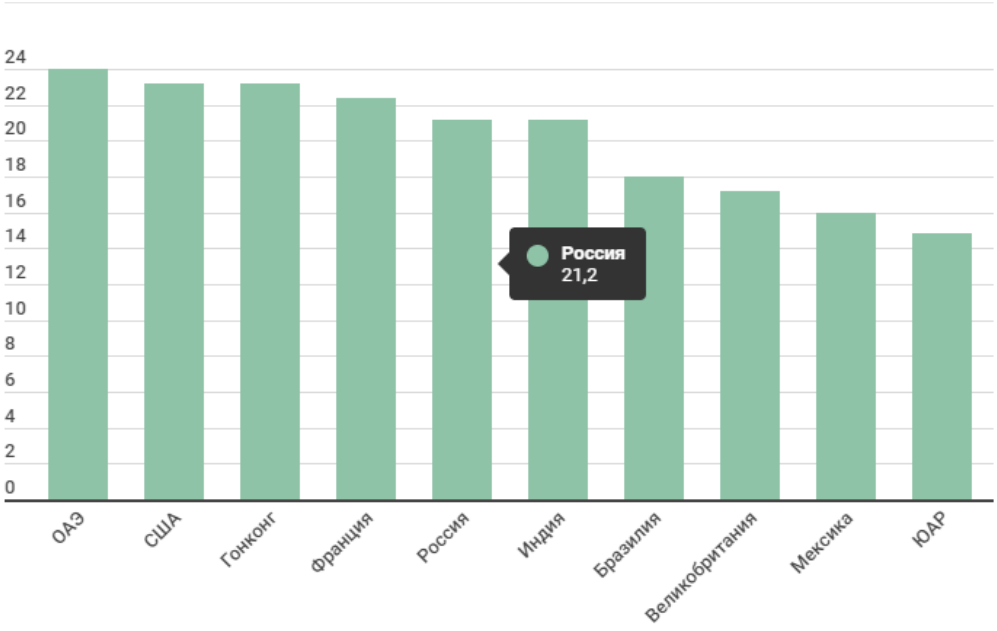
В 2015-2016 финансовом году в Японии было зарегистрировано рекордное число «кароси»– 1456. Организации, защищающие права работников, говорят, что реальные цифры могут быть в несколько раз больше, чем официальная статистика.

Борьба с «кароши». Не так давно правительство страны ввело так называемую «Премиум-Пятницу», когда служащим разрешено уходить с работы в 15:00 в последнюю пятницу каждого месяца. Однако, согласно опросам, только 4 % японских служащих покидает рабочие места так рано.

Рис. 2. Основные причины смерти в Японии

А в Швеции «Лагом» – самое распространенное и самое абстрактно переводимое на русский язык шведское понятие. Это слово как нельзя лучше отражает ментальность страны и может переводиться как «надо ровно столько, сколько надо», или «достаточно», или «в нужной степени». Это слово и есть один из внутренних принципов шведского социализма, о котором все наслышаны.Переработки в стране в принципе не приветствуются: считается, что они плохо сказываются на настроении и продуктивности. Если сотрудник придет на работу с температурой, его тут же отправят домой – независимо от того, горят ли сроки. На зарплату это не повлияет: Национальное агентство социального страхования компенсирует потери, даже если человек вышел из строя на несколько недель.

Специалисты компании MAXIS GlobalBenefitsNetwork (MAXIS GBN) – международный пул, объединяющий 140 страховых компаний в разных странах. На рисунке 3 вы можете увидеть сколько часов сотрудники перерабатывают в разных странах.



*в среднем в месяц

Рис. 3. Переработка в разных странах

По данным их исследования 79% сотрудников во всем мире перерабатывают в среднем 20,4 часа в месяц, то есть почти три полных рабочих дня.

Россияне не отстают от общемировых трендов и тоже тратят на работу все больше времени — в среднем 21,2 дополнительных часа в месяц.

Как выяснили исследователи Высшей школы экономики (НИУ ВШЭ), в 2017 году 4,5 млн россиян трудились более 40 часов в неделю. При этом три четверти перерабатывали до десяти часов в неделю, а остальные проводили в офисе еще больше времени.

Рис. 4. Итоги социального опроса

Опросы hh.ru в свою очередь показали, что 16% опрошенных работников задерживаются на работе каждый день, 43% – несколько раз в неделю, 19% – не более одного раза в неделю и только 8% – никогда не остаются в офисе дольше положенного. При этом чаще всего – в 58% случаев – сотрудники остаются до-

полнительно на 1-2 часа, меньше часа после окончания рабочего дня в офисе проводят 29%, а 11% задерживаются больше чем на три часа.

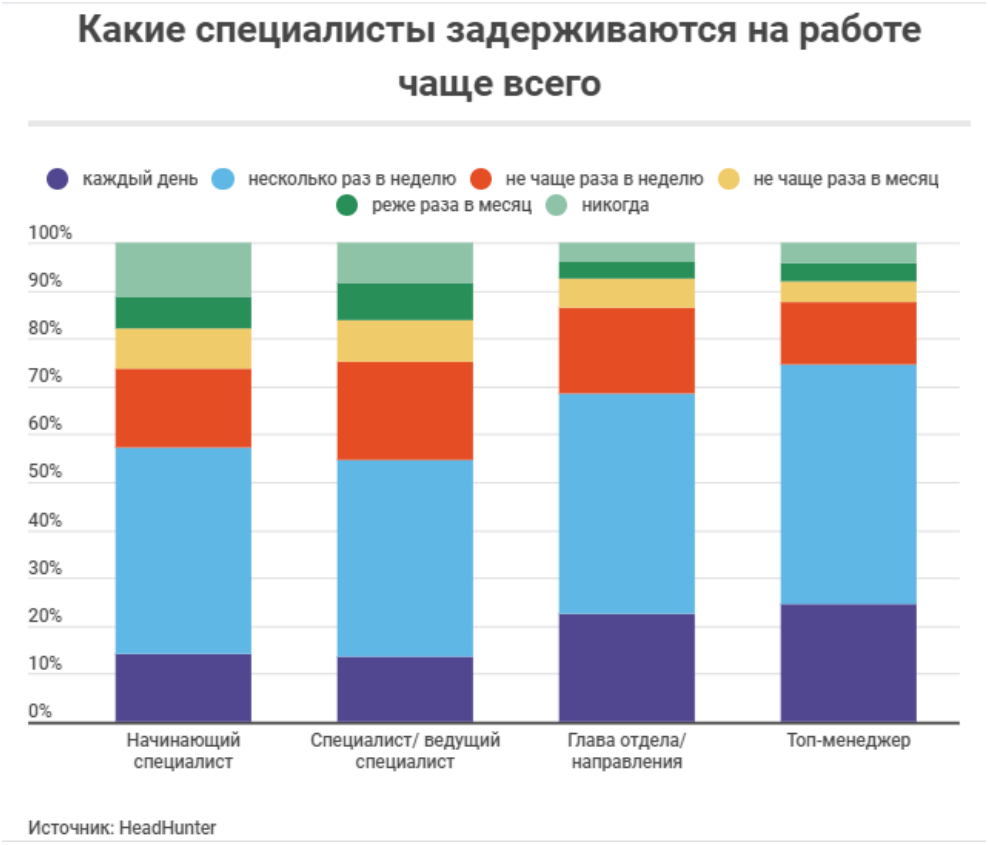


Рис. 5. Показатели задержек в зависимости от должности

По данным статистики видно, что чаще всего специалисты задерживаются несколько раз в неделю, не зависимо от должности.

Все опрошенные ТАСС эксперты отметили, что для России проблема переработок и трудоголизма в принципе новая и поэтому с ней не борются активно, а для многих «трудоголик» по-прежнему звучит как комплимент.

В России производительность труда серьезно отстает от японских показателей. Так, по данным Организации экономического сотрудничества и развития (ОЭСР), по итогам прошлого года производительность труда в Японии составила 46,2 долларов в час (этот показатель отражает объем ВВП, вырабатываемый каждым трудящимся в страны за один час работы в текущих ценах по паритету покупательной способности). В России же этот показатель, по оценкам ОЭСР, составляет лишь около 26,5 долларов, почти вдвое меньше. В Швеции 71 доллар в час.

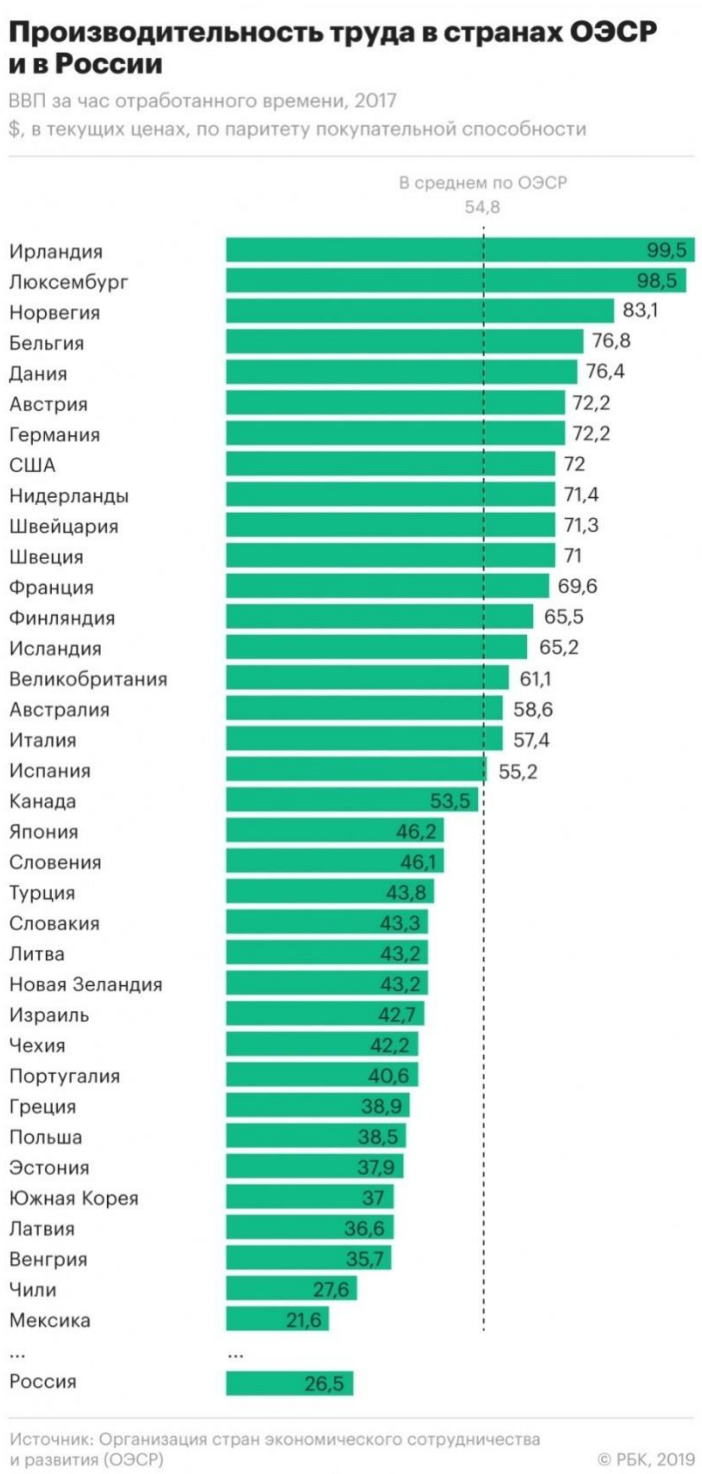


Рис. 6. Производительность труда в странах ОЭСР и в России

Исходя из таблицы 1 и рисунка 6 можно сделать вывод о том, что в Швеции рабочая неделя длится 40 часов с производительностью 71$/ч, в Японии рабочая неделя длится 44 часа с производительностью 46,2$/ч, а в России рабочая неделя длится 40 часов с производительностью 26,5$/ч.

В десятке самых эффективных стран преимущество за небольшими странами Европы (8 из 10), тогда как крупные мировые экономики, такие как Япония, Франция и Великобритания, находятся в конце первой двадцатки. В Стране восходящего солнца производительность падает из-за сокращения и старения населения (Япония опустилась с 17-го на 20-е место).

В целом по показателям Россия более чем в два раза уступает эффективным экономикам, а благодаря мощному технологическому прогрессу, который в мире сейчас поступательно развивается, этот разрыв может серьезно возрасти, если мы своевременно не будем на это реагировать.

Далее рассмотрим отношения людей к сверхурочной работе в зависимости от стажа работы и мотивы работать сверхурочно (рис.7).

Рис. 7. Отношение и мотивы работать сверхурочно

Основными мотивами работать сверхурочно являются варианты «поджимают сроки» 44,2%, «необходимо для моей профессии» 39%, «хочу больше зарабатывать» 23,4% – это весомый аргумент, который связан с достаточно низкой оплатой труда в России, с социальными гарантиями и уровнем благосостояния в целом.

Заключение

Таким образом, самое негативное желание оставаться на работе у сотрудников со стажем до 1 года и от 2 до 3 лет. Возможно, это связано с тем, что вышестоящие сотрудники перекладывают свою работу и ответственность на работников с малым стажем, которые не могут отказать им, так как боятся потерять свое рабочее место.

1) Стаж до 1 года. Они еще не знают работу и не уверены, что захотят остаться, поэтому и текучесть самая большая в этот период. Происходит адаптация к работе и коллективу, которая может длиться достаточно долго. Для решения данной проблемы не стоит нагружать дополнительным объемом в виде сверхурочной работы, а лучше мотивировать работников с перспективой на дальнейшее повышение.

2) Стаж от 2 до 3 лет – они уже освоили работу, наработали высокий уровень компетентности, вероятно хотят повышения статуса, но их начинают загружать дополнительной монотонной работой, которая не помогает им продвигаться по карьерной лестнице. Здесь идет перекладывание работы от руководителей на сотрудников, что вынуждает их оставаться сверхурочно. В России это является распространенной проблемой, поскольку руководители ставят себя намного выше в сравнении с сотрудниками. Можно применить опыт Швеции, где руководитель относится к сотрудникам как к равным. Это не получится сделать быстро, но первоначально можно повысить оплату труда с учетом сверхурочной работы.

С целью развития института рабочего времени представляется необходимым использовать опыт зарубежных стран с учетом применимости каких-либо положений зарубежного законодательства в России, т.к. некоторые положения неприменимы в условиях российской действительности. Нужно учитывать то, что культуру, ментальность нации невозможно поменять одномоментно, должна произойти смена поколений.

Во-первых, нужно стараться изменить отношение между работниками и работодателями. Во-вторых, нужно придерживаться позиции «надо ровно столько, сколько надо», для этого необходимо вмешательство государства с целью пересмотра системы оплаты труда по профессиям.

СПИСОК ЛИТЕРАТУРЫ

1. Бордадын А.Ф. МОТ и Россия. М.; Институт труда.
2. Киселев И.Я. Сравнительное и международное трудовое право. - М.: Дело.
3. Костин Л.А. Международная организация труда. - М.: Издательство «Экзамен».
4. https://crocotime.com/ru/optimizatsiya-rabochego-protsessa-v-kompanii/– «Оптимизация рабочего процесса в компании».
5. Ведущий источник статистики труда (https://ilostat.ilo.org/).

УДК 336.7

А. Д. БОЙЦОВА, Л. И. РАХМАТУЛЛИНА
aleona.boitzova@mail.ru, raxmatullina.99@list.ru
Науч. руководит. – канд. экон. наук, доц. А. В. СТАРЦЕВА

Уфимский государственный авиационный технический университет

ВЛИЯНИЕ ФОНДОВОГО РЫНКА НА ЭКОНОМИЧЕСКУЮ БЕЗОПАСНОСТЬ ГОСУДАРСТВА

Аннотация. Статья показывает взаимосвязь фондового рынка и экономической безопасности государства. Приводится анализ статистических данных по теме. Предлагаются некоторые мероприятия по оживлению ситуации на фондовом рынке, предотвращению угроз безопасности государства.
Ключевые слова: фондовый рынок; угрозы безопасности государства.

Фондовый рынок является неотъемлемой частью финансового рынка, поэтому оказывает непосредственное влияние на экономическую безопасность государства. Как показала практика мировых финансовых кризисов, фондовый рынок является уязвимой составляющей финансовой системы, поэтому рассмотрение предложений по повышению стабильности российского рынка ценных бумаг для обеспечения безопасности национальной экономики является актуальным вопросом в развитии российской экономической системы [1].

Проведем сравнительную характеристику объемов инвестиций в России за последние 10 лет, представленных на рисунке 1.

Российский рынок ценных бумаг является достаточно молодым. В отношении инвестиционной активности наблюдается умеренный рост с перепадами в связи с экономической обстановкой в стране. В 2021 г. в центре внимания выступают нефтегазовый сектор, технологии и инновации. Объем сделок растет в недвижимости, строительстве и потребительском сегменте. Рост инвестиций в основной капитал по официальному прогнозу ожидается порядка 5%.

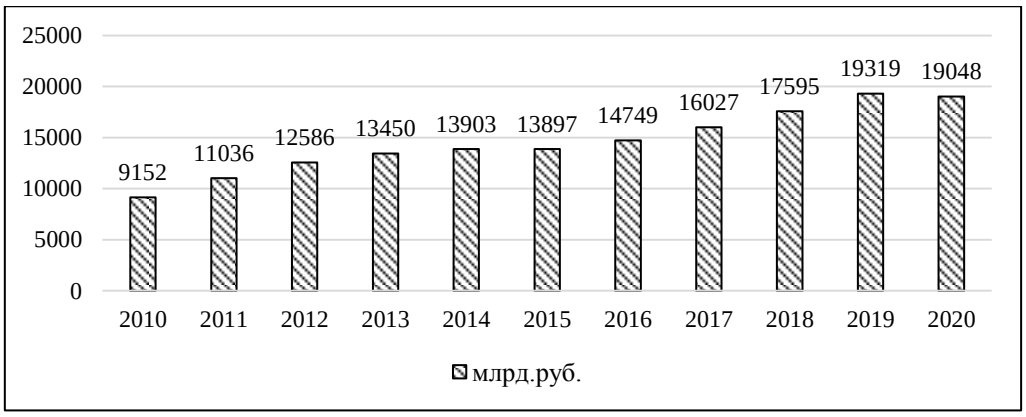


Рис. 1. Динамика инвестиций в основной капитал

На сегодняшний день существует около 200 фондовых бирж в мире. На рисунке 2 представлены 14 самых крупных фондовых бирж.

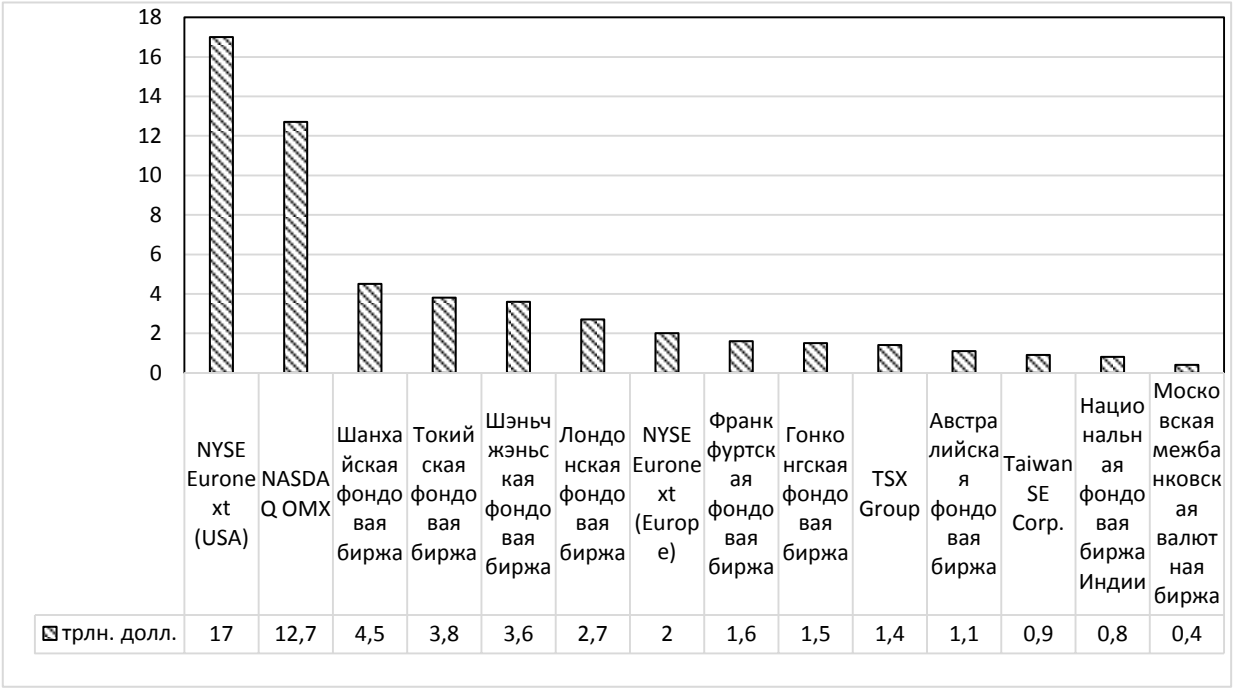


Рис. 2. Мировой рейтинг фондовых бирж по обороту торговли акциями

Так, ММВБ находится на 14-ом месте в мировом списке по обороту торговли акциями. Данный показатель равен 400 млн.долл. В сравнении, у лидера данного рейтинга – группы компаний, образованной в результате слияния крупнейшей в мире Нью-Йоркской фондовой биржи (NYSE) и Европейской биржи Euronext, оборот торговли акциями равен 17 трлнруб., что в 42,5 раза превышает значение этого же показателя в России.

Рассмотрим основные причины непопулярности рынка ценных бумаг.Ключевым фактором являетсяобщая нестабильность всей экономической ситуации. Кризисы 1998, 2008, 2014 годов являются наглядным тому доказательством. Нестабильность в стране, обусловленная высокой волатильностью рубля, которая, в свою очередь, отпугивает крупных инвесторов, предпочитающих более спокойные западные рынки в качестве объектов размещения денежных ресурсов, колебаниями процентных ставок, внешними санкциями, международнымиконфликтами снижает желание инвесторов вкладывать собственные сбережения в экономику России и инструменты российского рынка ценных бумаг и повышают его уязвимость. Как следствие, происходит уменьшение вложений в финансовые инструменты и отток капитала, связанный с желанием инвесторов минимизировать свои риски и дальнейшее инвестирование в более стабильные развивающиеся страны [2].

Важным фактором является и срок существования рынка ценных бумаг в стране. В России он начал свое активное функционирование лишь в 90-х годах, в то время как биржи других государств к тому моменту уже давно были широко известны среди инвесторов. Именно поэтомуему не хватает более опытных игроков для функционирования наравне с лидерами.

Нежелание населения связываться с рынком ценных бумаг также является главной проблемой. Ввиду экономической нестабильности, начавшейся с 2014 года, часть граждан, стараясь сберечь свои деньги от инфляции, прибегают не к инвестиционному поведению, а наоборот, увеличивают свое потребление даже с помощью кредитных ресурсов.

Следующей, не менее важной проблемой является финансовая безграмотность населения. Большинство лиц, получивших доступ к рынку ценных бумаг, становятся банкротами в ближайший год. Даже те частные инвесторы, что хотят разбираться и пробовать свои возможности на рынке ценных бумаг, не имеют необходимой квалификации и быстро уходят с биржи [3].

Таким образом, необходимо стратегическое развитие рынка ценных бумаг, удовлетворяющее основным аспектам развития, включая разработку мероприятий. Существуют различные мероприятия, способствующие продвижению рынка ценных бумаг среди населения.

Ярким примером является создание информационной среды по отношению к рынку ценных бумаг через рекламную кампанию Тинькофф Инвестиции. Это позволяет создать благоприятных имидж рынка ценных бумаг, освещать преимущества и недостатки такого рода инвестиций. С увеличением потока денежных средств на рынке ценных бумаг его условия и качественные характеристики улучшатся и выиграют от этого все стороны. Эффективность маркетинговой коммуникации брокерской платформы Тинькофф подтверждает также шестикратный рост брендового траффика рекламной кампании. Почти 96% целевой аудитории (17,2 млн человек) взаимодействовали с рекламным сообщением Тинькофф Инвестиций не менее одного раза. 83% целевой аудитории увидели рекламу Тинькофф более пяти раз.

Одним из основных условий соответствия современным реалиям является широкое развитие электронной среды. Сейчас существуют онлайн-платформы, позволяющие получать информацию об обращении всех ценных бумаг страны, эмитентах, биржах, обеспечивают возможность саморегулирования и независимости профессиональных участников рынка.

Другой важной составляющей является повышение финансовой грамотности населения.Частично проблему финансовой безграмотности решают брокеры, которые берут на себя функции управления портфелем ценных бумаг. Создание программ повышения финансовой грамотности населения позволит научиться управлять личными средствами, например, через индивидуальный инвестиционный счет, а также предоставлять участникам рынка государственные гарантии безопасности инвестиций [4].

Таким образом, развитие российского фондового рынка – это сложный процесс, который может быть решен только при комплексном подходе со сто-

роны как участников самого рынка, так и государственных органов. По мере развития инвестиционной инфраструктуры и финансовой грамотности населения, решения всех перечисленных проблем, есть надежда, что будет расти и количество отечественных и иностранных инвесторов на российском фондовом рынке, что станет одним из главных факторов его роста и развития.

СПИСОК ЛИТЕРАТУРЫ

1. Афонцев С. Национальная экономическая безопасность: на пути к теоретическому консенсусу // Мировая экономика и международные отношения. - 2014. - № 10.URL.: https://dlib.eastview.com/browse/doc/4485475(дата обращения 13.06.2021г.)
2. Зуева, А.С. Основы безопасности фондового рынка России: учебное пособие/ А.С. Зуева. – Москва: Научно-исследовательский центр финансовой безопасности, 2015.– 210с. URL.: https://search.rsl.ru/ru/record/01006567953(дата обращения 25.05.2021г.)
3. Становление фондового рынка в России и первые уроки его развития [Электронный ресурс]. URL.:http://center-yf.ru/data/economy/ (дата обращения 25.05.2021г.)
4. Эриашвили, Н.Д. Экономическая безопасность: Учебное пособие для студентов вузов / В.А. Богомолов, Н.Д. Эриашвили, Е.Н. Барикаев; Под ред. В.А. Богомолова. - М.: ЮНИТИ-ДАНА, 2016. - 295 с.URL.: https://bookree.org/reader?file=717373 (дата обращения 28.07.2021г.)

УДК 338

Ю. С. ГАВРИЛОВА, Д. А. ЗИНАТУЛЛИН
yu_gavrilovaa@mail.ru, geraldroy2000@mail.ru
Науч. руковод. – асс. Э. Р. ФАТТАХОВА

Уфимский государственный авиационный технический университет

ВЛИЯНИЕ КРИЗИСОВ НА ТЕХНОЛОГИИ УПРАВЛЕНИЯ ЧЕЛОВЕЧЕСКИМ КАПИТАЛОМ

***Аннотация*.** В данной работе рассматривается влияние пандемии коронавирусной инфекции на управление человеческим капиталом: как изменились условия работы в период пандемии, какие действия предпринимали руководители фирм, рассмотрена статистика, а также спрогнозированы возможные последствия.
***Ключевые слова*:** человеческий капитал; пандемия коронавируса.

Из-за пандемии организациям пришлось изменить свои подходы к работе с персоналом и научиться решать новые задачи: контролировать удаленную работу, чтобы избежать потери эффективности, предотвращать выгорание самых продуктивных сотрудников, сохранять социальные связи в команде, не имея возможности организовать живые встречи, и многое другое.

На место живых заседаний пришла компьютеризация. Практически все важные встречи проводились в формате online с помощью различных сервисов (Zoom, CiscoWebexи др). До сих пор данный процесс набирает популярность, а это не может не сказаться на работе с человеческим капиталом.

По данным руководителей различных компаний, эффективность сотрудников в период пандемии снизилась на целых 80%. Сами сотрудники сообщают, что только у 41% снизилась эффективность в период пандемии. К основным факторам данного явления можно отнести эмоциональное выгорание, тревога, депрессия, а для некоторыхсотрудников – потеря смысла самой работы. Статистика представлена на рисунке 1.

Рис. 1. Что происходит с сотрудниками с переходом на удаленную работу

Также руководители многих компаний сообщили, что сотрудники чувствовали себя некомфортно на работе. Помимо вышеперечисленных факторов, у некоторых из них был страх будущего, т.к. они не знали, что будет дальше.

Аналитики считают, что в данной ситуации ключевую роль сыграл именно менеджмент. Именно он помог определить направления работы и последующую коммуникацию между сотрудниками.

Об изменениях работы госслужащих в время пандемии COVID-19 можно сказать, что работы и нагрузки у государственных служащих прибавилось достаточно, нужно было принимать решения оперативно. Стоит отметил, что большая часть руководителей брали на себя ответственность и принимали решения, не запуская кучу процедур по согласованию.

Главная сложность была в том, что удаленный формат работы был сложен для реализации, так как часть программных продуктом не была установлена, а также не у всех сотрудников был доступ к стабильному интернету или же вовсе не было компьютера.

Стоит отметить, что пандемия смогла объединить руководителей и менеджмент для более эффективной работы с сотрудниками. Если же во время оффлайн работы эффективность сотрудника была невидима из-за общей эффективности коллектива, то пандемия смогла раскрыть личные качества и пользу каждого сотрудника.

К сожалению, повышенная нагрузка негативно повлияла на сотрудников, они стали увольняться и это стало еще одной сложностью, которая принесла пандемия, ведь приходилось переформатировать работу всего коллектива.

Период пандемии и «тотального локдауна» сильно затянулся. Многие считали, что он продлится всего лишь 2 недели, однако, пандемия длится уже больше года. В связи с этим событием аналитики рассчитали, как отреагировали различные структуры на затянутость пандемии и карантина. Данные представлены на рисунке 2.

Рис. 2. Тренды изменений в управлении персоналом

Результаты вышеуказанных данных были достигнуты уже ранее применяемыми механизмами. Но уже спустя пару месяцев стало приходить понимание, что некоторые функции, которые были раньше, просто не нужны. Например, ряд форм отчетности, презентации, выступления. Результат вышел на первый план.

Также мы обратили внимание на ряд объединяющих факторов для рабочих коллективов. Так, идея служения общим целям компании помогала сотрудникам сохранять эффективность, ведь все чувствовали необходимость выполнить максимум, оказаться не хуже конкурентов, несмотря на сложную ситуацию во всем мире.

Далее были выявлены причины, по которым снижается эффективность работы у сотрудников различных фирм. Данные представлены на рисунке 3.

Рис. 3. Причины снижения эффективности работы персонала

Исходя из данных рисунка 3, можно сделать вывод, что личная эффективность сотрудников напрямую зависела от навыка их самоорганизации. В «отстающих» оказались как раз те сотрудники, которые не смогли организовать работу на дому, правильно распределить время и расставить приоритеты.

Подводя итог, можно сказать, что кризис очень сильно влияет на управление человеческим капиталом и пандемия COVID-19 прямое тому подтверждение. У многих людей отмечалась потеря интереса к работе, страх за будущее, тревога и т.д. В такой период очень тяжело работать, но руководители все-таки находят методы поддержки персонала в трудные времена и перестраивают условия работы под обстоятельства. Также наблюдается возросшая потребность в новых подходах и решениях. От формального подхода и восприятия, порой навязанных инструментов мы пришли к тому, что, действительно, появился интерес и необходимость в новых процедурах, новых правилах и технологиях. Можно дальше двигаться на длинной дистанции эффективно только в том случае, если мы будем видеть одинаковые цели, совместно идти как с точки зрения коллективов, так и с точки зрения лидеров.

СПИСОК ЛИТЕРАТУРЫ

1. Человеческий капитал Материал из Википедии. [Электронный ресурс] Режим доступа: http:/ru.wikipedia.org/wiki/- 20.04.2017 (дата обращения 04.04.2021).
2. 2016 Human Development Report . [Электронный ресурс] Режим доступа: http://hdr.undp.org/en/2016-report - (дата обращения 11.03.2021).

УДК 364.05

Ю. С. ГАВРИЛОВА, Д. Р. ТОРОПОВА, Н. Р. ЯВАРОВА
yu_gavrilovaa@mail.ru, nata.yava1308@mail.ru
Науч. руководв. – канд. экон. наук, доц. А. Н. ШЕРЫШЕВА

Уфимский государственный авиационный технический университет

МАТЕРИНСКИЙ КАПИТАЛ: ЗАДАЧИ ГОСУДАРСТВА И ПОТРЕБНОСТИ ОБЩЕСТВА

Аннотация. В данной статье рассматривается материнский капитал государственная помощь населению, его основные направления, различные виды мошенничества в сфере материнского капитала. А также предложены рекомендации по улучшению условий материнского капитала и расширению направлений его использования.
***Ключевые слова*:** материнский капитал.

Материнский капитал представляет собой форму государственной поддержки семей, которые воспитывают детей. Программа материнского капитала действует с 1 января 2007 года при рождении или усыновлении ребенка, при условии, что родители не воспользовались правом на дополнительные меры государственной поддержки. С 2020 года материнский капитал можно получить и на первого ребенка.

Размер материнского (семейного) капитала устанавливается в сумме 466617 рублей при формировании сертификата в проактивном (беззаявительном) режиме, если в информационных ресурсах ПФР отсутствуют сведения о предшествующих детях.

Размер материнского капитала в 2021 году составляет 483 881,83 рублей за первого ребенка согласно Федеральному закону от 8 декабря 2020 г. № 385-ФЗ "О федеральном бюджете на 2021 год и на плановый период 2022 и 2023 годов" и 155 550 рублей за второго ребенка. Также для тех семей, где нужна поддержка государства в связи с рождением или же усыновлением второго или третьего и последующих детей, общая сумма материнского капитала составляет 639 431,83 рублей.

Материнский капитал можно потратить лишь на ограниченный спектр услуг, а именно:

1. Образование детей.

2. Улучшение жилищных условий семьи

3. Формирование накопительной части пенсии матери.

4. Социальную адаптацию и интеграцию в общество детей-инвалидов.

Также семьи с доходом ниже двух прожиточных минимумов на человека могут использовать мат. капитал на ежемесячные выплаты на второго ребенка, до тех пор, пока тому не исполнится три года

Согласно статистике, в 2020 году 61% семей, получивших материнский капитал, потратили его на улучшение жилищных условий, 28% семей подали заявления на ежемесячную выплату на второго ребенка из средств мат. Капитала, а 11% оставшихся семей направили средства на образование детей.

Данные представлены на рисунке 1.

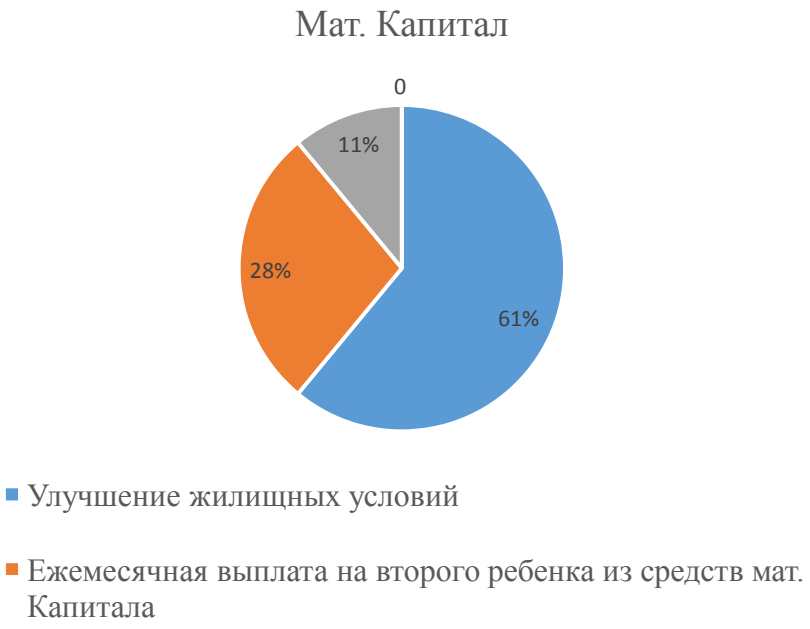


Рис. 1. Статистика использования материнского капитала

Главной особенностью материнского капитала является то, что его нельзя обналичить, что делает его еще более узконаправленным и не дает возможность семьям «развернуться» при выборе услуг. Сам регламент мат. капитала очень «жесткий» и зачастую провоцирует идти на нарушения.

Если же родители решили вложить средства в образование своих детей, то они могут перечислить средства только на счет того учебного заведения, в которое они отправят своих детей или потратить на различные курсы повышения квалификации, но этого уже не предусматривает регламент материнского капитала.

Из-за такого строгого регламента многие люди идут на различные виды мошенничества. Обычно обман заключается в различной цене недвижимости по факту и по документам, мнимой покупке жилья, махинациях с ипотекой.

Например, в договоре купли-продажи указывают стоимость жилья, равную материнскому капиталу, на деле она намного меньше. В такой ситуации за бросовую цену продают дома, в которых невозможно жить. В результате, часть денег получает семья, часть продавец дома, и часть получает риэлтор, который провел сделку. У семьи оказывается в собственности дом, за который нужно платить имущественный налог, но в котором нельзя жить и невозможно продать.

Еще больший риск касается самого договора продажи. Ведь в нем указана большая сумма, и продавец дома может потребовать ее выплаты. Более того, он сможет даже выиграть суд на основании такого договора.

Риэлторы предлагают и другие фиктивные сделки с целью обналичить материнский капитал:

– фиктивная покупка дома, собственность на который у семьи не возникает;

– приобретение жилья низкого качества, ради обналичивания субсидии;

– получение денег наличными путем их мнимого вложения в кооператив или долевое строительство.

При этом процент риэлторов может достигать 50% от суммы материнского капитала, а в некоторых случаях они обманными действиями забирают всю сумму. Родители, согласившиеся на такую аферу, не могут никуда пожаловаться, поскольку их действия также подпадают под уголовное наказание.

Еще один вариант махинаций – приобретение жилья у родственников и друзей. В этом случае:

– меньше шансов быть обманутыми;

– продавец не сможет полностью распоряжаться этой собственностью, без учета интересов семьи, так как совладельцами будут несовершеннолетние дети, а это требует участия органов опеки в любой сделке;

– продавец не сможет доказать мошенничество в суде.

Стоит отметить, что основные проблемы с реализацией материнского капитала, допускающие описанные мошеннические схемы, связаны с отсутствием единого государственного органа, отвечающего за контроль процесса рождения детей, их регистрации, выдачи материнского капитала, его расходования. Эти функции разделены между Минюстом, Минтруда, Минздравом, Росстатом и другими ведомствами.

Также было проведено собственное исследование касательно материнского капитала по вопросам направлений его использования. На основе опроса можно сделать некоторые выводы насколько то, что уже сделано, соответствует потребностям людей.

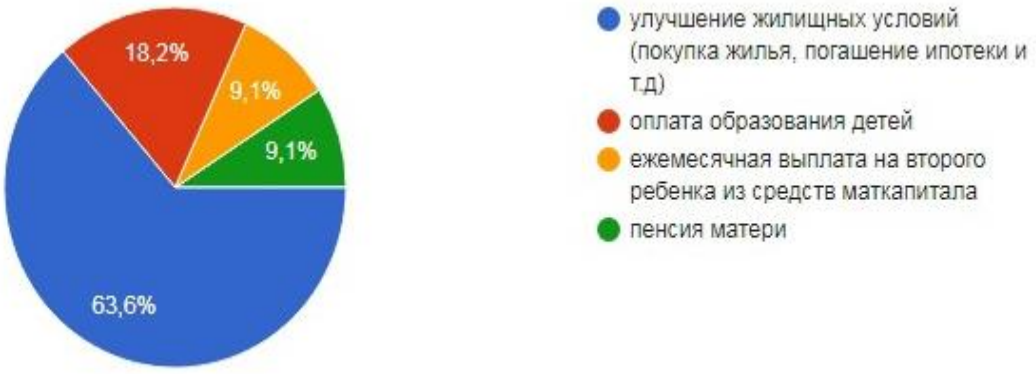


Рис. 2. Результаты опроса населения на вопрос «Каким образом вы хотите воспользоваться материнским капиталом?»

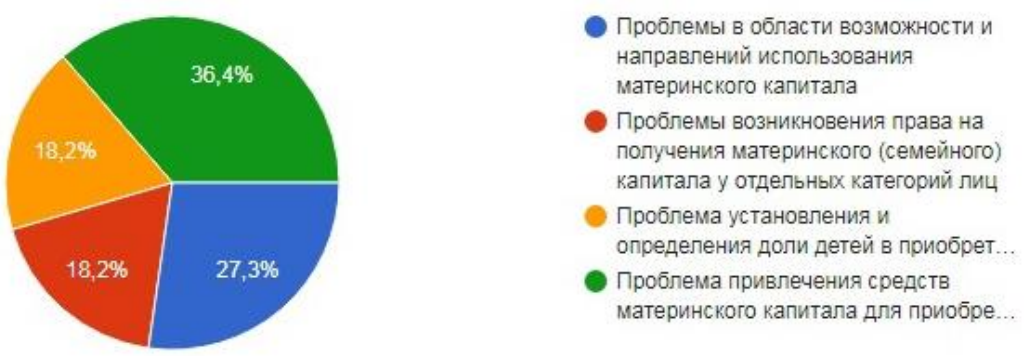


Рис. 3. Результаты опроса населения на вопрос «С какими проблемами Вы столкнулись при получении материнского капитала?»

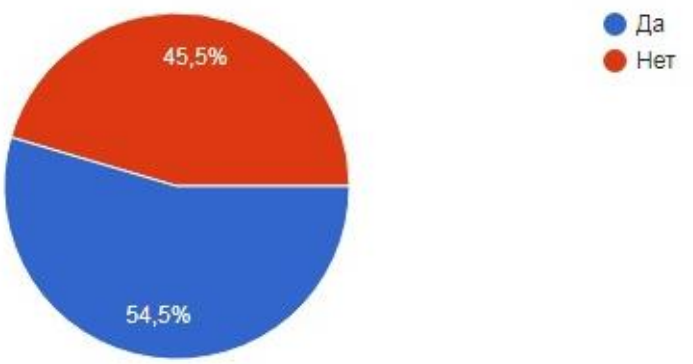


Рис. 4. Результаты опроса населения на вопрос «Как вы считаете, материнский капитал способствует повышению рождаемости?»

Итак, в результате проведенного опроса, видно, что большинство людей сосредоточены на улучшении жилищных условий (покупка жилья, погашение ипотеки и т.д.). Использование материнского капитала для покупки недвижимости является наиболее востребованной формой распоряжения им.

Проблемой является привлечения средств материнского капитала для приобретения жилья с высокой стоимостью. Действительно, стоимость квартир в крупных городах значительно превышает сумму материнского капитала.

Большинство опрошенных считает, что материнский капитал повышает рождаемость. Конечно, молодые родители ощущают поддержку государства

и возможно, у молодых мам есть уверенность в том, что имеется возможность обеспечить ребенка материально.

Подводя итог, можно сказать, что материнский капитал – это, несомненно, большая государственная поддержка семей, но направления использования материнского капитала слишком ограничены. Чтобы сделать его более удобным, государство может предпринять следующие действия:

1) расширить спектр услуг, которые предоставляет материнский капитал. Это должны быть не только вышеупомянутые категории, но и новые важные. Например, нужно сделать так, чтобы мат. капитал можно было направить на покупку необходимых лекарств или же на операцию не только для ребенка, но для и родителей. Также можно предусмотреть покупку автомобиля;

2) дать возможность обналичить определенный фиксированный процент материнского капитала;

3) перевести денежные средства материнского капитала на счет ребенка, которым он сможет пользоваться по достижении 18-ти лет.

На данный момент государство делает все возможные улучшения материнского капитала и с каждым годом он становится все лучше и удобнее.

СПИСОК ЛИТЕРАТУРЫ

1. Семейный кодекс Российской Федерации от 29.12.1995 N 223-ФЗ (ред. от 29.05.2019) // «Российская газета», N 17, 27.01.1996.
2. Федеральный закон от 29.12.2006 N 256-ФЗ (ред. от 02.08.2019) «О дополнительных мерах государственной поддержки семей, имеющих детей»//«Российская газета», N 297, 31.12.2006.
3. Федеральный закон от 27.07.2010 N 210-ФЗ (ред. от 01.04.2019) «Об организации предоставления государственных и муниципальных услуг»//«Российская газета», N 168, 30.07.2010. Материалы судебной практики
4. Благодарова Е. Материнский капитал и ипотека – проблемы и споры // Жилищное право. – 2016 г. – № 9. – С. 31-40. 11) Даньшина Д.Н. К вопросу о материнском (семейном) капитале // Молодой ученый. – 2016. – № 10-3 (114). – С. 42-43.
5. Меркулова А. В. Материнский капитал: вопросы теории и практики / А.В. Меркулова // Ученые записки Орловского государственного университета. – 2019. – № 6. – С. 336-339.
6. Останина Н.А. Материнский капитал – матерям и детям / Н.А. Останина // Вопросы социального обеспечения. – 2016. − № 15. – С. 15-16.
7. Пенькова А.С., Чермит Р.Р., Коваленко Е.А. К вопросу о материнском капитале // Научные революции: сущность и роль в развитии науки и техники: Сборник статей Международной научно-практической конференции. – М.: МГУ, 2017. – С. 143-145.

8. Петрова В.С. Проблемы социально-экономического развития Ханты-Мансийского автономного округа – Югры / Петрова В.С. // Научно-методический электронный журнал Концепт. 2017. № S1.–С. 36- 41.
9. Полуян А.В. Правовой режим имущественных отношений супругов // Актуальные проблемы современного частного права. – М.: Законовед, 2016. – С. 276-278.
10. Рудых С.Н. О материнском капитале // Проблемы современного законодательства. Мат. III Всерос. науч.-практ. конф. – М.: РПА Министа России, 2015. – С. 72-75.
11. Торосян Р.А. Проблемы обеспечения равенства мужчин и женщин в сфере семейных отношений // В сборнике: 100-летие юридического образования в Саратовской области Материалы Международной научно-практической конференции в рамках Международного научного симпозиума, посвященного 100-летию гуманитарного образования в СГУ. 2018. – С. 121.

УДК 336.1

Д. А. ГРИГОРЬЕВА, А. А. САБИТОВА, Д. А. СЕРГЕЕВА
gridasha@gmail.com,alsu_sabitova_00@mail.ru,dashas2029@mail.ru
Науч. руководов. – ст. преп. О. П. МЕНДЕЛЬ

Уфимский государственный авиационный технический университет

ВЛИЯНИЕ COVID-19 НА КОРРУМПИРОВАННОСТЬ ГОСУДАРСТВЕННЫХ ЗАКУПОК В СФЕРЕ ЗДРАВООХРАНЕНИЯ

Аннотация. В данной статье рассматривается факт связи коррупции в государственных закупках в сфере здравоохранения в периодCOVID-19.
Ключевые слова: сфера здравоохранения; COVID-19; государственные закупки; условия пандемии; коррупция; противодействие коррупции.

Во время мировой пандемии COVID-19 высокий рост коррупции наблюдается в отрасли здравоохранения, в данной сфере особенно пострадали государственные закупки.

Данная тема является наиболее актуальной, так как за прошедшее время пандемии случаи коррупции в сфере медицинских государственных закупок начали возрастать, а точное окончание пандемии не удалось предсказатьеще ни одномуэпидемиологу, и не исключено, что вторая волна была заключительной.Необходимые препараты, средства индивидуальной защиты и прочие важные вещи, которые должны быть в общей доступности, стали продаваться за немыслимые деньги. Это произошло из-за того, что в дело вступил основной экономический принцип – спрос рождает предложение. Созданный ажиотаж, подкрепленный паникой среди населения, привел к тому, что маски, антисептики, противовирусные и другие товары стали исчезать с полок. При этом предприятия не были готовы к такой ситуации и не смогли вовремя восполнить дефицит. Как итог – резкий скачок цен.

Такая же проблема коснулась государственных закупок: медицинские учреждения и аптечные пункты не были готовы к подобной ситуации, как следствие произошла нехватка лекарств, а в больницах аппаратов ИВЛ, КТ и прочих, для поддержки жизнедеятельности человека. Государство для того, чтобы исправить положение и ускорить снабжение объектов здравоохранения всеми

необходимыми средствами, внесло корректировки в Федеральный закон «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» №44 от 30.10.2020, срок его действия составляет один календарный год. В данный закон были внесены следующие изменения[1]:

– продлили сроки действия отдельных контрактов;

– разрешили проводить закупки у единственного поставщика;

– COVID-19 признали обстоятельством непреодолимой силы (форс-мажором);

– увеличили лимиты для закупок малого объема;

– изменили правила работы с гарантийными обязательствами;

– отменили проверки;

– перешли на дистанционное рассмотрение жалоб;

– разрешили менять существенные условия контракта;

– списывают неустойку.

Например, отмена проверки может привести к таким последствиям, как ошибка в заключение контракта, что приведет к не сертифицированным препаратам, не соответствующему оборудованию, завышению цен гигиенических средств, не своевременной поставке препаратов, подмене лекарств.

Из-за упрощения этапов формирования государственных закупок 80% сделок проходит без необходимой конкуренции и проверок, то есть закупки осуществляются в режиме ЧС, при этом известно, что на рынке есть более 30 поставщиков. Например, в республике Башкортостан известен случай, когда производилась закупка аппаратов ИВЛ на сумму более 1,3 млрд. рублей, а самый большой контракт был заключен с одним поставщиком, который ранее не участвовал в тендерах по государственным закупкам, на сумму более 560 млн. рулей – данная закупка была произведена в режиме ЧС[6].

В это время, Международная организация «Группа государств по борьбе с коррупцией» (CRECO), созданная Советом Европы (СЕ), заявила о возросших

коррупционных рисках в сфере закупок медицинских средств в условиях пандемии COVID-19[3].

По данным Генпрокуратуры коррупция в сфере государственных закупок нами была составлена таблица 1. В ней представлены показатели за 2019 и 2020 год.

Таблица 1

Коррупция в сфере государственных закупок

Наименование	2019 год	2020 год
Выявлено нарушений (тыс.)	145,4	153,8
Направлено исков в суд	1 338	1 531
Привлечено к административной ответственности (чел.)	12 970	12 945

Таким образом, прирост составил:

1) в выявленных нарушениях – 5,8%;

2) в направленных исках в суд – 14,4%;

3) в привлечении к административной ответственности произошла снижение на 0,2%.

В 2020 году коррупция в сфере медицинских закупок составила 34 миллиарда рублей. Есть примеры нанесения ущерба бюджету при исполнении договора на поставку оборудования, который оценивается в десятки миллионов рублей.Например, в Иркутской области был разорван контракт на 237 млрд. руб. из-за поставок контрафактных масок, это могло произойти из-за изменения закона №44, о котором упоминалось выше [5].

Коррупция в закупочной деятельности прослеживается не только в контрафактных медицинских продуктах, но и товарах, которые продаются выше рыночной стоимости. Известна ситуация, когда медицинские маски закупались по 18-20 рублей за штуку, в то время как их средняя цена составляла 8 рублей. Только по республике Башкортостан подобные случаи уже оцениваются в более чем в 2 млн. рублей.

Например, без конкурентных торгов был заключен контракт на поставку КТ в новый ковид-госпиталь Стерлитамака, закупка оборудования была на сумму 63 183 300 рублей, в то время, как на сайте конкурента данные аппараты

обошлись бы в 47 845 262рублей. Стоит отметить, что закупка происходила под предлогом ЧС [6].

Для того, чтобы понизить показатель коррумпированности государственных закупок в сфере здравоохранения государство приняло такие меры:

1) маркировать лекарственные продукты – это обеспечит их подлинность и сертифицированность;

2) эффективные регуляторы условий участия в закупках (требования к участникам в закупках) – помогает выходить на проверенных поставщиков;

3) приказом Генерального прокурора РоссийскойФедерации от 27 июля 2016 г. № 459 утвержден межведомственныйплан мероприятий по предупреждению и пресечению «откатов»,выявлению и устранению коррупционных проявлений приосуществлении закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд; и так далее[2].

В Законе о закупках много внимания уделено контрольным мероприятиям. Это любые контрольные мероприятия надзорных органов власти – ФАС России, Счетной палаты, прокуратуры, Следственного комитета, МВД и др. контроль со стороны различных общественных объединений.

Обратимся к зарубежному опыту государственных закупок на примере Китая. Правительственные учреждения и юридические лица Китая обязаны приобретать товары и услуги отечественного производителя. Исключение только одно – предпочтение в пользу зарубежных исполнителей можно отдать только в том случае, если отечественные аналоги стоят на 20% дороже импортных.

Китайской федерацией логистики и закупок (CFLP) был создан Единый официальный китайский сайт для размещения госзакупок, на котором открыто предоставляется информация о поставщиках, ценах и покупателях, публикуются детали сделок[7].

В Китае закупочная деятельность должна удовлетворять следующим трем условиям:

1) закупки должны осуществляться государственными органами,государственными учреждениями, общественными организациями на всех уровнях;

2)закупки должны проводиться по тем товарам, услугам, работам, которые представлены в CPCatalogue или стоимость которых выше пороговых значений;

3) закупки должны проводиться за счет бюджетных средств.

Закупающие организации не вправе прекратить процесс торгов после того, как заявка-извещение или письмо-приглашение уже выдано.

Прекращение торгов может быть оправдано,если:

– существуют менее трех поставщиков, которые соответствуют квалификационным требованиям;

– возникает противоправное поведение, что ставит под сомнение справедливость проведения торгов;

– торговая цена превышает уровень бюджета и закупающая сторона способна оплатить закупки;

– закупка отменена в связи с существенными изменениями.

Таким образом, государственные закупки в Китае имеют свою специфику, заключающуюся в том, что они используются для снижениязависимости национальных производителей от конъюнктуры мировых финансовых рынков. Китай жестко регламентирует формы участия иностранного капитала в национальной экономике и вместе с тем обеспечивает открытость зарубежным странам относительно потоков ресурсов и товаров.

На основании данных, приведенных в статье, для большей прозрачности государственных закупок в медицине, рекомендуется проводить следующие мероприятия:

1) введения контроля служебной переписки;

2) через СМИ и интернет распространять о неотвратимости наказания за совершенные деяния;

3) ввести систему индивидуальных инструкций для сотрудников, где будут прописаны все шаги при осуществлении государственных закупок;

4)проведение специальных тренингов по разъяснению составов, ответственности и наказания за правонарушения в области госзакупок.

Наиболее эффективной рекомендацией будет являться мероприятие, связанное с информационной прозрачностью на всех этапах закупочной деятельности: доступность правовых актов, устанавливающих общие правила закупок, открытый доступ ко вспомогательным документам (методикам, инструкциям) в сфере осуществления закупок (рис. 1).

Рис. 1. Схема прозрачности государственных медицинских закупок в России

На рисунке 1 представлена схема самой перспективной мерой обеспечения прозрачности закупок.После публикация информации в интернете на официальном сайте, на главной (стартовой) странице медицинского учреждения должна быть прямая ссылка на раздел, посвященный закупкам или для перехода на раздел, посвященный закупкам, требуется совершить не более трех переходов с главной страницы. Также на официальном сайте учреждения необхо-

димо публиковать разъяснения по поступившим от участников закупок запросам, и учреждению надо заблаговременно информировать поставщиков путем публикации на официальном сайте о внесении изменений в регламентирующие закупочную деятельность документы. Вдобавок желательно иметь на официальном сайте интерактивные обучающие программы (презентации) для поставщиков, желающих принять участие в закупках[4].

Данные мероприятия помогут предотвратить коррупцию в сфере медицинских закупок, путем прозрачности и доступности всех действий и этапов, что, в свою очередь, повысит уровень экономической безопасности страны.

Можно сделать вывод, что действенная борьба с коррумпированностью государственных закупок в сфере здравоохранения, нуждается в надлежащем уровне государственной ответственности, мельчайшей проработке законопроектов и изменений законов, а также их усилий в равной степени с усилиями гражданского общества и частного сектора. COVID-19 имеет негативные последствия, которые влекут большие затраты, поэтому появляется большая необходимость в разработке и доработкеантикоррупционных реформ.

СПИСОК ЛИТЕРАТУРЫ

1. Федеральный закон «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» № 44-ФЗ от 05.04.2013 [Электронный ресурс]. URL: –http://www.consultant.ru/(последняя редакция от 30.10.2020).
2. Приказ прокурора РоссийскойФедерации от 27 июля 2016 г. [Электронный ресурс]. URL: –https://genproc.gov.ru/
3. Коррупция и пандемия COVID-19 [Электронный ресурс]. URL: –https://newsmaker.md/
4. Обеспечение информационной прозрачности [Электронный ресурс]. URL: – https://sudact.ru/
5. РБК: Росфинмониторинг сообщил об отмывании денег под предлогом пандемии[Электронный ресурс]. URL: –https://www.rbc.ru/
6. Теневые закупки республики Башкортостан в 2020 году [Электронный ресурс]. URL: – https://proufu.ru/
7. Китайский сайт по государственным закупкам. [Электронный ресурс]. URL: – http://www.china-cpp.com/

УДК 338.124

А. Т. ДАВЛЕТГАЛИНА, Г. Р. МУЛЛАБАЕВА
guzelkamullabaeva@mail.ru
Науч. руководв.– ст. преп. О. П. МЕНДЕЛЬ

Уфимский государственный авиационный технический университет

АНАЛИЗ ВЛИЯНИЯ ПАНДЕМИИ COVID-19 НА МАЛЫЙ И СРЕДНИЙ БИЗНЕС РОССИИ

Аннотация. В данной статье были рассмотрены проблемы, с которыми столкнулись малый и средний бизнес России в период пандемии коронавируса COVID-19. Был проведен анализ и указаны пути решения проблем. Выбранная тема актуальна, так как предпринимательство является одним из приоритетных направлений государственной политики России, поэтому стабилизация ситуации и скорейший выход из кризисного периода очень важны для российской экономики.
***Ключевые слова*:** малый и средний бизнес; пандемия; коронавирус; влияние пандемии COVID-19.

Новая экономическая политика предполагала государственное регулирование смешанной экономики с использованием плановых и рыночных механизмов.

Наверное, нет такой сферы в России, да и вообще в мире, которой не коснулась вспышка пандемии коронавирусной инфекции COVID-19. Экономический кризис, вызванный пандемией, оказал большой удар на малый и средний бизнес, которые вносят большой вклад не только в национальную, но и в мировую экономику. Если посмотреть статистику, то мы увидим, что на долю МСП приходится до 90% от всех компаний в мире, более 70% мировой занятости и 50% ВВП, а значит они являются основными субъектами экономической среды [6]. Но, к сожалению, в связи с карантином многие компании были вынуждены временно закрыться, резко сократился совокупный спрос и значительно увеличилась безработица. Результаты коронавирусаной инфекции для российской экономики имеют долгосрочный характер, поэтому, если даже ограничения постепенно снимаются, перед бизнесом предтсоит усердная работа по принятиям решений в период экономического кризиса.

Рассмотрим опрос аналитического центра НАФИ, проводивший исследование о том, как пандемия коронавируса повлияла на российский

бизнес. Результаты опроса представлены на основе опроса 1 500 предпринимателей со всей России, самого опрос был в конце марта 2020 года. Респондентам задавали вопрос: «На Ваш взгляд, какие отрасли российской экономики, какие сферы бизнеса больше всего страдают или могут пострадать от распространения коронавируса?». Данные опроса показали, что пострадали все отрасли. Самый большой удар от коронавирусной инфекции ощутили или удар отрасли, представленные на рисунке 1 [4].

Рис. 1. Динамика наиболее пострадавших от влияния пандемии коронавируса отраслей, в % от всех опрошенных предпринимателей

По итогам данного опроса были выделены топ-10 отраслей, на которые вирус оказал наибольшее влияние. Больше всего пострадал бизнес, который предоставлял услуги, работал в сфере развлечений, питания и обслуживания. В связи с закрытием транспортных сообщений со многими странами колоссальные убытки понесли предприниматели, работающие в сфере туризма и отдыха. Ситуация складывается таким образом, что люди больше думают о товарах первой необходимости, чем о развлечениях и прочих второстепенных потребностях. Рассмотрим мнения предпринимателей, которые высказались по поводу влияния коронавируса на финансовые показатели компании. Данные представлены на рисунке 2 [4].

Рис. 2. Оценка влияния пандемии на российскую экономику предпринимателями, в % от всех опрошенных

Исходя из данных, представленных в диаграмме, можно сделать вывод: 85% предпринимателей указали, что распространение коронавируса негативно повлияло на финансовые показатели их организации. Под ударом и малый бизнес: в компаниях с численностью сотрудников до 100 человек негативные последствия особенно ощутимы (их отметили 87% предпринимателей), в компаниях со штатом более 100 человек негативные последствия отмечали чуть реже (78%). Женщины-предприниматели чаще говорили о негативных последствиях, чем мужчины (.90% и 82% соответственно). Две трети женского бизнеса (68%) – это небольшие организации с численностью штата до 15 человек, работающие в сфере услуг, культуры, спорта и организации мероприятий.

Данные анализа о влиянии пандемии на малый и средний бизнес очень пугающие. Без помощи государства из этой ямы предприятиям просто не выбраться, потому что ущерб огромный. Поэтому, Правительством Российской Федерации были предложены следующие меры поддержки в

условиях осложнения эпидемиологической обстановки для поддержки среднего и малого бизнеса:

– снижение страховых взносов (с 1 апреля 2020 года до 31 декабря 2020 года);

– моратория на банкротство (с 7 октября по 7 января 2020 года);

– моратория на проверки бизнеса;

– налоговые каникулы;

– кредитные каникулы;

– отсрочка арендных платежей (с 1 апреля 2020 года по 1 октября 2020 годы);

– беспроцентные кредиты на заработную плату (не позднее 30 ноября 2020 года).

Остается открытым вопрос: «Все ли так просто? И реально ли получить поддержку государства?». Вопрос спорный и весьма противоречивый. Например, касаемо отсрочки арендных платежей – в марте-апреле-мае, эта мера зависела непосредственно от согласия/несогласия самого арендодателя, поэтому многие предприятия продолжали залезать в долги и выплачивать аренду, а многие и вовсе вынуждены были съехать из-за нехватки денежных средств на ее выплату. Общероссийский народный фронт (ОНФ) опубликовал исследование на тему «Оценка эффективности мер поддержки малого и среднего предпринимательства». Таким образом, результаты опроса были следующие: 52% опрошенных указали, что по ОКВЭД (общероссийскому классификатору видов экономической деятельности) их организации относятся к перечню пострадавших отраслей. Большинство МСП, которые не попали в перечень, хотели бы получить поддержку, предназначенную для пострадавших отраслей. Доля тех, кто, обращались за поддержкой государства составляет 78%, из них 51% запрашивали или хотели бы запросить кредит для выплаты зарплат по ставке 0%, 42% – кредит по ставке 8,5% (74% столкнулись с отказом банков при оформлении льготного кредита по ставке 0%, 87% – с отказом

банков по кредиту 8,5%). Опрос проводился с 22 по 29 мая 2020 г. В нем приняли участие 2746 предпринимателей из всех регионов России. Несмотря на сложность ситуации, на данный момент удается держать ее под контролем. Государственные меры по поддержке малого и среднего бизнеса помогут пережить непростое время, но с оговоркой: поддержку Правительства получают не все нуждающиеся компании. В заключении отметим, что малые и средние предприятия общепризнанно составляют основу международных и национальных экономик и находятся в поле зрения большинства правительств. Несмотря на изменение внешней среды, которое обусловлено пандемией и всеобщим экономическим кризисом, предприятия такого масштаба остаются уязвимы перед серьезными экономическими изменениями, в том числе и перед глобальными [2]. Однако содействия и помощи государства не всегда достаточно: не все предприятия могут получить господдержку либо не в полной мере. Основные вызовы для малого и среднего бизнеса в условиях пандемии – это финансовая неустойчивость, снижение спроса, риск заражения персонала, нарушение функционирования предприятия как такового.

Рассмотрим зарубежный опыт помощи бизнесу во время пандемии. США, например, в марте предыдущего года объявили о введении налоговых каникул до 3-х месяцев, Дональд Трамп поросил Конгресс одобрить 50 млрд рублей и направить их на поддержку малого и среднего бизнеса, также в США начали выдавать кредиты по ставкам 3,75% для малого бизнеса. Власти Италии 8 марта 2020 года объявили о налоговом кредите для любой компаний, у которых выручка сократилась на 25 и более процентов во время коронавирусной эпидемии. Другие страны тоже предпринимали различные меры, чтобы помощь бизнесу в стране. Если сравнить Россию с другими странами, то главная проблема это то, что нашли власти не могут предпринять четкие действия и масовая истерия в СМИ.

Для поддержки малого и среднего бизнеса в России нужно разработать:

– предоставить гранты и субсидии предпринимателям, для компенсации падения доходов;

– реализовать структурные меры, помогающие МСП адаптироваться к новым методам работы и (цифровым) технологиям. Внедрять цифровые стратегии особенно в век новейших технологий задача каждого предпринимателя для развития бизнеса. Основные мероприятия проекта:обеспечение дистанционного доступа к сформированному реестру оцифрованных региональных услуг организаций инфраструктуры поддержки МСП, органов власти, органов местного самоуправления и институтов развития; создание мобильного приложения для доступа к сервисам Цифровой платформы; предоставление условий для осуществления сбыта товаров, работ (услуг) с помощью цифрового сервиса – агрегатора маркетплейсов на Цифровой платформе; осуществление подбора кадров, а также получение предложений от соискателей на трудоустройство, в том числе за счет интеграции с существующими сервисами подбора персонала и «Электронной трудовой книжкой»; реализация механизма адресного подбора мер, сервисов и решений «жизненных ситуаций» и проактивного одобрения инструментов поддержки, обеспечивающего получение необходимого результата с минимальным набором действий;

– внедрять специальные схемы для мониторинга влияния кризиса на МСП и улучшения управления мерами политики, связанными с МСП;

– новая льготная кредитная программа «ФОТ 3.0», на которую будет направлено порядка 7,7 млрд рублей. Участие могут принять гостиничный и ресторанный бизнес, сфера культуры, туризма, спорта и развлечений. Размер кредита будет зависеть от количества сотрудников, занятых в организации. Максимальная сумма – 500 млн рублей. Главное условие: заемщик должен сохранить не менее 90% рабочих мест в период действия кредитного договора. Эта программа даст МСП новый шаг к развитию [5].

СПИСОК ЛИТЕРАТУРЫ

1. Департамент международного и регионального сотрудничества СП РФ. Дайджест: под-

держка МСП в контексте COVID-19. [Электронный ресурс]. URL: https://ach.gov.ru/upload/pdf/Covid-19-SME.pdf (дата обращения 04.03.2021).
2. Доклад РСПП о ситуации в российских компаниях на фоне пандемии COVID-19. [Электронный ресурс]. – Режим доступа: URL: https://media.rspp.ru/document/1/0/a/0a74470429f3dea0e8a73556494ff698.pdf (дата обращения 05.03.2020).
3. Официальный сайт Федеральной налоговой службы. Единый реестр субъектов малого предпринимательства. [Электронный ресурс]. – Режим доступа: URL: https://rmsp.nalog.ru/statistics.html (дата обращения 04.13.2021).
4. Официальный сайт аналитического центра «НАФИ». Влияние эпидемии коронавируса на бизнес и потребность в господдержке. [Электронный ресурс]. URL: https://nafi.ru/projects/predprinimatelstvo/rossiyskiy-biznes-i-koronavirus-chast-1-predprinimateli-o-vliyanii-epidemii-na-ikh-biznes-i-o-potreb/ (дата обращения 07.03.2021).
5. Официальный сайт информационного агентства «ТАСС». Как эпидемия коронавируса влияет на малый и средний бизнес в России. [Электронный ресурс]. URL: https://tassbiz.ru/help/kak-epidemiya-koronavirusa-vliyaet-na- malyj-i-srednij-biznes-v-rossii/ (дата обращения 04.03.2021).
6. Кучумов А.В., Печерица Е.В., Волошинова М.В. Человеческие ресурсы в системе экономической безопасности предприятий в сфере услуг. Вестник Национальной академии туризма.– 2020. –№ 2 (54). –С. 24-26.

УДК 338.2

Д. П. ЕЖОВ, Н. В. МУСАВИРОВ
edp01@yandex.ru
Науч. руководит. – канд. пед. наук, доц. А. Ю. ФАРРАХОВА

Уфимский государственный авиационный технический университет

МИССИЯ БАНКА КАК ОСНОВА СТРАТЕГИЧЕСКОГО УПРАВЛЕНИЯ

Аннотация. В статье представлен анализ значения миссии для стратегического развития банка. Центральным моментом миссии является ответ на вопрос: «Какова главная цель организации?». Цели организации определяются после получения формулировки миссии, то есть миссия, с одной стороны, дает возможность установить, какие цели необходимо поставить, чтобы деятельность предприятия соответствовала его миссии, а с другой, отсекает «часть» возможных целей. Раскрываются миссии и ценности кредитных организаций.
Ключевые слова: миссия; организация; стратегия; развитие; цель; план; ценности; структура; банки.

Миссия – одно из основополагающих понятий стратегического управления. Разные ученые давали различные формулировки миссии (табл.1).

Таблица 1

Понятие «миссия»

Автор	Определение
Майкл Мескон	Миссия – смысл существования компании с позиции удовлетворения потребностей клиентов, реализации конкурентных преимуществ, мотивации сотрудников фирмы
Франклин Хедоури	Миссия – это основная общая цель организации – четко выраженная причина ее существования. Цели вырабатываются для осуществления этой миссии
Виханский О. С.	Миссия – это философия и предназначение, смысл существования организации

Миссия и цели организации – это программные положения, на которых строится вся ее деятельность. Миссия – это наиболее общее описание того, для чего создана компания, какую задачу она призвана решить. При этом стоит отметить, что получение прибыли не может быть миссией компании – она должна быть более широкой и показывать, каким образом компания может быть полезна обществу. В этом нет никакого противоречия, ведь, в конце концов, только будучи каким-то образом полезной и востребованной компания может рассчитывать на то, что ее продукты будут покупаться, а значит, и на получение прибыли[1].

Для того чтобы лучше уяснить, что такое миссия, приведем примеры миссий известных компаний (табл. 2).

Таблица 2

Миссии известных компаний

Название компании	Миссия
ПАОЛукойл	Миссия компании – обращать энергию природы на благо людей.
McDonalds	Миссия компании – предоставление быстрого и качественного обслуживания с помощью стандартных продуктов.
Microsoft	Миссия – помогать людям и бизнесу полностью раскрывать свой потенциал при помощи электронных технологий.
Walt Disney	Миссия студии– делать людей счастливыми.

Стоит делать четкое различие между такими понятиями, как миссия и цель организации. Если миссия – это наиболее общее описание причины существования организации, то цель – это четкое описание тех заданий, которые необходимо выполнить для того, чтобы воплотить миссию в реальность.

Цели компании могут быть кратко- и долгосрочными, а также изменяться в ходе ее деятельности, в то время как миссия остается неизменной на протяжении всего периода деятельности фирмы. Таким образом, миссия и цели предприятия представляют собой единое целое философское ядро ее деятельности – миссия отвечает на вопрос «зачем нужна наша компания?», а цели отвечают на вопрос «что нужно сделать для того, чтобы осуществить миссию и, соответственно, оправдать ее существование?». Только при наличии такого ядра компания будет осуществлять свою деятельность эффективно и методично[2].

Определять миссию организации необходимо с учетом следующих критериев:

1) миссия организации – это реалистичная цель, которую возможно достичь. Она должна быть амбициозной, мотивировать к развитию, но и учитывать возможности компании;

2) главная цель организации должна быть направлена на решение определенной потребности общества, приносить пользу людям;

3) миссия организации – это мощный стимул для эффективной работы ее сотрудников;

4) доступность миссии для понимания и согласие с ней всех членов компании – один из основных критериев стратегии организации. Если миссия будет нечетко сформулирована существует риск хаотичной работы и разногласий внутри коллектива;

5) уникальность – важный критерий философии работы организации и фактор скорости ее развития. Компания должна стараться делать то, что не делают другие, и решать те проблемы, которые до нее еще никто не решал. Но для определения того, в чем компания будет уникальна, необходимо провести анализ потребностей общества в той нише, которую она планирует занять;

6) стратегическая миссия организации должна содержать руководство к действию, т. е. определять ориентиры развития компании сегодня и завтра. Необходима уверенность в том, что мотивирующей силы миссии хватит на планируемый срок ее существования;

Существуют и ошибки при формировании миссии:

–содержание миссии весьма далеко от реального бизнеса организации и ее отношений с клиентами;

– миссия содержит стандартные фразы, не несущие конкретики и не дающие понять, что именно делает или собирается делать организация;

– миссия никак не связана с планами организации, с тем направлением, к которому организация реально движется;

– сотрудниками организациимиссия не воспринимается как некое направление для своих действий, а скорее как элемент обязательных правил.

Для примера рассмотрим миссии кредитных организаций (табл. 3).

Таблица 3

Миссии кредитных организаций

Банк	Миссия	Ценности
ПАО Сбербанк	Мы даем людям уверенность и надежность, мы делаем их жизнь лучше, помогая реализовывать устремления и мечты. Наша миссия определяет смысл и содержание деятельности Сбербанка, подчеркивая его важнейшую роль в экономике России. Наши клиенты, их потребности, мечты и цели есть основа всей деятельности банка как организации. Миссия банка также устанавливает амбициозную цель наших устремлений – стать одной из лучших финансовых компаний мира – и подчеркивает, насколько важны для Сбербанка его сотрудники, и насколько реализация его целей невозможна без реализации их личных и профессиональных целей. Высокие цели достигаются командой единомышленников, которых объединяет общая система ценностей.	Наши ценности – основа отношения к жизни и работе, внутренний компас, помогающий принимать решения в сложных ситуациях, принципы, верность которым мы храним всегда и везде. Ориентиры, которые помогают нам принимать верные решения в любых ситуациях: Я – лидер Мы – команда Все – для клиента
АО «Альфа-банка»	Пройдя долгий путь от товарищества с ограниченной ответственностью до российского лидера в сфере финансовых услуг, Альфа-Банк сохранил главное — заботу о клиентах. Его миссия в том, чтобы помогать людям и компаниям в улучшении жизни, дать простые и удобные решения как повседневных, так и самых важных вопросов	В отношении: бизнеса – предпринимаются смелые, дерзкие, амбициозные, но обдуманныешаги;потребителя – экономится каждая минута его времени, в ежедневную работу интегрируются новые технологии, повышается эффективность менеджеров.
ПАО Уралсиб	Мы – Банк-партнер. Мы дарим уверенность в будущем и открываем новые перспективыразвития для наших клиентов. Каждый день мы находим лучшие финансовые решения,гарантируем прозрачные и удобные расчеты для эффективности вашего бизнеса идостижения ваших личных целей.	Мы последовательны Мы ответственны, Мы результативны Мы динамичны, В основе нашей работы – уважение к каждому клиенту. Мы уверены, что взаимодействиемежду клиентом и Банком должно строиться на честности и доверии – только в этом случае сотрудничество будет взаимовыгодным.

Подводя выводы, можно сказать, что каждая организация, рассмотренная в таблице, имеет перед собой четко поставленные цели, они похожи друг на

друга, и заключаются в том, чтобы сделать жизнь людей лучше, давая им возможности для реализации их личных амбиций.

Компании создаются и закрываются каждый день. Многие фирмы, которые имеют качественный продукт или услугу, несмотря ни на что, со временем становятся банкротами. Причина этого кроется в том, что их стратегией является лишь заработок денег. Но в бизнесе не стоит зацикливаться лишь на этом, чтобы обеспечить себе будущее.

Крупные корпорации и международные компании уже давно поняли важность определения миссии компании. Их руководству стало ясно, что деньги не являются единственной ценностью, а настоящую значимость имеет процесс деятельности и стратегия должна основываться на фундаментальных человеческих ценностях, которые присущи каждой личности, например, повышать качество предоставляемых организацией товаров и услуг, предоставлять комфортные условия сотрудникам компании, тем самым улучшая этот мир.

СПИСОК ЛИТЕРАТУРЫ

1. Виханский О.С. Менеджмент: Учебник / Виханский О.С., Наумов А.И. – М.: Экономистъ, 2006 – 29 с.
2.Тебекин А.В. Менеджмент организации: Учебник / Тебекин А.В., Касаев Б.С. – М.: КНОРУС, 2007– 224 с.
3.Официальный сайт ПАО «Сбербанк» URL: https://www.sberbank.ru (дата обращения 05.04.2021).
4. Официальный сайт АО «Альфа банк» URL : https://alfabank.ru/ (дата обращения 05.04.2021).
5.Официальный сайт ПАО «Уралсиб» URL: https://www.uralsib.ru/(датаобращения 05.04.2021).

УДК 343.9

Л. В. КАМАЛТДИНОВА, Э. А. КАРИМОВА
exovixxbts@mail.ru, elya_karimova_98@mail.ru
Науч. руководв. – канд. юр. наук, доц. З. З. ТАЛЫНЕВА

Уфимский государственный авиационный технический университет

КИБЕРПРЕСТУПНОСТЬ В СФЕРЕ ЦИФРОВОЙ ЭКОНОМИКИ КАК НОВАЯ УГРОЗА ДЛЯ ОБЩЕСТВА

Аннотация. Изучена статистика и аналитические данные, размещаемые на официальных сайтах МВД России. В целях разработки эффективных мер противодействия данному явлению определены его характерные черты и факторы, способствующие его развитию, представлены некоторые направления противодействия преступности в данной сфере.
***Ключевые слова*:** киберпреступность; общественная опасность; противодействие экономическим преступлениям.

В наши дни киберпреступления создают множество проблем для общества: личных, финансовых и даже становится угрозой национальной безопасности. Только за последние несколько лет были украдены данные сотни миллионов кредитных карт и десятки миллионов страховых свидетельств. Хакеры взломали даже ядерные центрифуги и перехватили управление беспилотными дронами.

Сейчас, несмотря на значительное снижение количества преступлений, совершаемых в России, уровень экономической преступности являетсябольшим (рис. 1).

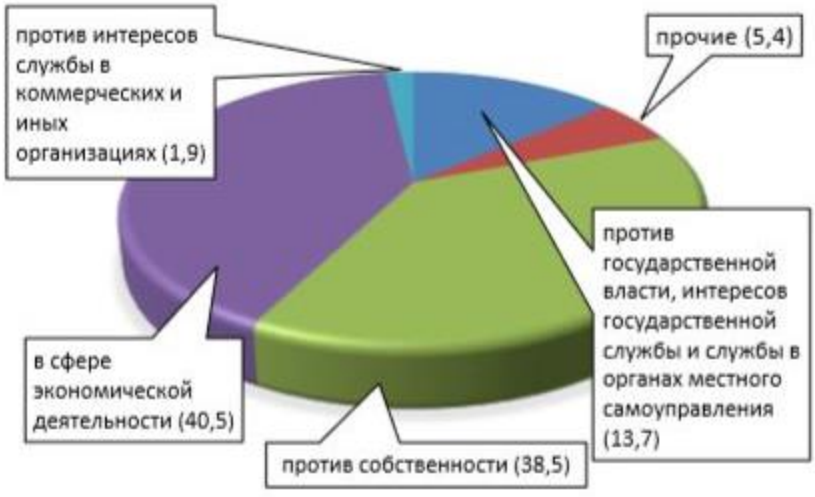


Рис. 1. Структура преступлений в России за 2020-ый год, %

По рисунку 1 видно, что удельный вес экономических преступлений в общем массиве преступлений составляет 40,5%. За 2020-ый год МВД России выявил причиненный ущерб в пятьсот миллиардов рублей (от 370-ти тысяч экономических правонарушений) [2].

Так как большое количество преступлений в экономической сфере совершаются с помощью компьютеров, ИТ-технологий и сети «Интернет», в 2021-ом году произошел рост преступлений (зарегистрированных) на 2,4 %, а именно:

– с помощью «мировой паутины»– возросло на 51,3%

– с использованием средств мобильной связи – увеличилось на 39%.

Так, когда в конце 2020-го года доля преступлений в сфере ИТ-технологий было 17%, то сейчас в 2021-году он возрос до 25% [2].

Далее рассмотрим структуру противоправных деяний в экономической сфере деятельности.

PwC, являющийся международной сетью компаний, предлагающих услуги в области консалтинга и аудита,провелза 2020-ый год Всемирный обзор экономических преступлений, который можно посмотреть на рисунке 2. В данном исследовании участвоваловсего пять тысяч людей из разных стран.

Рис. 2. Основные виды экономических преступлений, % [6]

Согласно отчету, 47% мировых компаний за последние два года сталкивались с мошенничеством в среднем шесть раз (ст. 159–159.6 УК РФ). К числу наиболее распространенных типов инцидентов относятся:

– мошенничество со стороны клиентов – 35%;

– киберпреступления – 34% (ст. 272–274.1 УК РФ);

– незаконное присвоение активов – 31%;

– взяточничество и коррупция – 30% (ст. 285–293 УКРФ) [1].

Остановимся накиберпреступлениях и рассмотрим данную сферу более подробно.

Киберпреступность, по сути, является преступной деятельностью, направленной на неправомерное использование компьютера, компьютерной сети или сетевого устройства. Данное незаконное деяние совершается киберпреступниками или хакерами, которые зарабатывают таким способом себе на жизнь [4].

Важно знать, что из-за всеобщей цифровизации мира, параллельно растет и преступность в экономической сфере, которая негативно влияет на общее состояние страны, представляя угрозу национальной безопасности.

Так, всего в 2020-ом году в России было зарегистрировано более 510,4 тысячи киберпреступлений, что на 75,2 % больше, чем за тот же период прошлого года. Значительное число из них происходит через Интернет и по телефонным устройствам. В общем количестве зарегистрированных преступлений их доля увеличилась с 10,4% в январе 2019-го года до 17,7 %. Почти все такие преступления (98,6 %) выявляются органами внутренних дел [2].

Также, по статистике Генпрокуратуры, совершение кибермошенничества в 2020-ом году составило около 70% всех краж, совершенных путем обмана или злоупотребления доверием. В течение года было выявлено более 237 тысяч эпизодов, что на 73,4% больше, чем в 2019-ом году. В 25,8 тыс. случаев использовались электронные платежные средства, причем увеличение числа таких де-

яний зафиксировано в большинстве регионов страны (чаще всего в Саратовской и Омской областях, а также Пермском крае) [3].

По данным Департамента правовой статистики и информационных технологий Генпрокуратуры, в 2020-ом году значительно возросло количество краж с банковских счетов и электронных кошельков. Если в 2019-ом году их было почти 94 тысячи, то в 2020-ом году – более 169,5 тысяч [3].

Правоохранительные органы, на данном этапе развития современных ИТ-технологий, не совсем готовы к разрешению проблем, преступлений, в киберсреде. Так, в первом полугодии 2020-го года произошло резкое увеличение числа киберпреступлений – на 92%, при этом уровень раскрываемости в этой сфере остается низким – 25 %.

Кроме того, вспышка пандемии в начале 2020-го года сопровождалась ростом числа мошеннических схем в Рунете. Одина из них – рассылка поддельных электронных писем, в том числе с доменов, похожих на адреса государственных учреждений. Организация Касперского выявила3 тысячиопасных ресурсов, где присутствуют такие слова, как covid (ковид) и coronavirus (коронавирус).

Волна хищений бонусов с карт лояльности также началась в начале марта 2020-го года. Количество попыток списания накопленных баллов с личных счетов на сайте увеличилось в несколько раз и достигло нескольких тысяч в месяц. Мошенники получают доступ к личному счету клиентов, а затем пользуются его бонусами при оплате своих покупок. Такой случай хищения был выявлен в магазинах «Магнит», который изрядно подпортил имидж торговой сети.

Миллиарды долларов – это ежегодные потери мировой экономики от экономических преступлений, совершаемых в киберпространстве. Большинство из данных преступлений могут причинить существенный вред имущественным отношениям и нормальному порядку предпринимательской или иной экономической деятельности, тем самым создавая угрозу национальной безопасности страны.

Приведем основные причины возникновения киберпреступлений в экономической сфере на рисунке 3.

Рис. 3. Основные блоки причин совершения незаконных деяний в сфере экономики

Так как социально-экономическиеи юридические причины компьютерной преступности в современной России носят актуальный характер, остановимся на них и рассмотрим более подробно на рисунках 4 и 5.

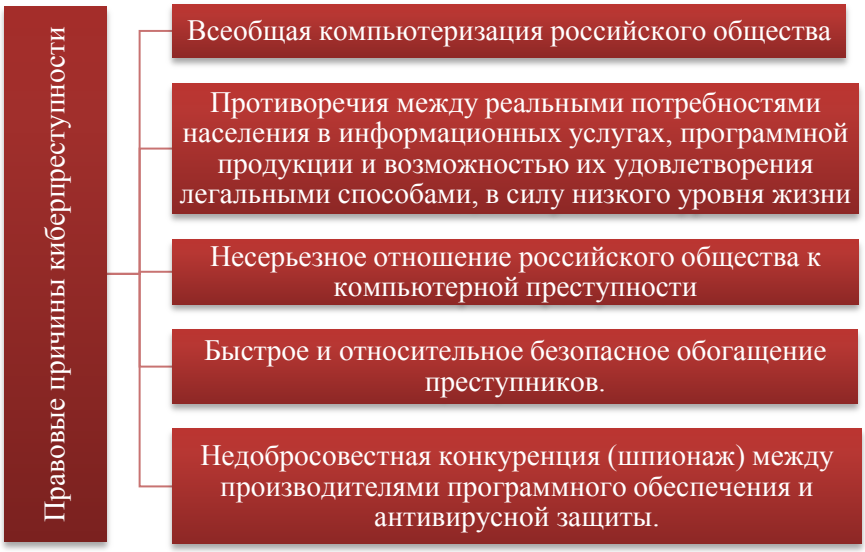


Рис. 4. Перечень основных социально-экономических причин возникновения преступности в экономической сфере РФ

Также с точки зрения юриспруденции можно выделить ряд причин возникновения киберпреступлений.

Рис. 5. Перечень основных юридических причин возникновения преступности в экономической сфере РФ

Таким образом, можно подытожить, что все причины совершения преступлений в цифровой сфере сложны и взаимосвязаны. Поэтому, давать каким-либо причинам, например экономическим, главный и фундаментальный характер, а другим, наоборот, второстепенный и незначительный характер – неправильно и ненаучно.

Министерство внутренних дел Российской Федерации совместно со средствами массовой информации, банковскими учреждениями и другими организациями регулярно проводит профилактическую работу по предупреждению преступлений, связанных с хищением денежных средств граждан с использованием информационно-телекоммуникационных технологий.

Также, при обращении граждан в отдел полиции с заявлениями, не имеющими отношения к экономическим преступлениям, сотрудники органа дознания, следователи проводят профилактическую работу и заполняют лист индивидуальных профилактических бесед с целью изменения поведения потерпевшего, в котором разъясняются следующее:

– работники банков не осуществляют звонки клиентам с просьбой предоставления персональных данных, номеров карт и другойинформации;

– не осуществляют СМС рассылки;

– никогда не сообщать незнакомым людям номер банковской карты и CVC-код;

– нельзя переходить по ссылкам на незнакомые ресурсы;

– сотрудники полиции, как и других правоохранительных и государственных органов не осуществляют звонки, в том числе и с «телефонов доверия», гражданам для подтверждения законности предлагаемых им финансовых операций с использованием банковских карт и других финансовых инструментов.

Вдобавок профилактическая работа объясняет людям, что:

– даже самые убедительные доводы звонящего о необходимости совершения каких-либо манипуляций с банковским счетом и денежными средствами, хранящимися на нем, являются формой обмана, направленной на завладение моими денежными средствами;

– данные карты не подлежат разглашению и являются строго конфиденциальными;

– при поступлении входящего звонка на телефон с любым предложением, связанным с проведением любой операции по банковской карте, необходимо прервать разговор и обратиться на телефон горячей линии, указанный на оборотной стороне карты [5].

В завершение научной работыприведем меры по противодействию совершения киберпреступлений в цифровой среде.

На данном этапе развития страны необходимо продумать соответствующее наказание, усилить действующие санкции, за неправомерное использование цифровой среды. Также необходимо предоставить правоохранительным органам современные ИТ-технологии и квалифицированные кадры, специализирующиеся в области информационной безопасности. И, в целом, перенять зарубежный опыт стран, которые, в свою очередь, преуспели в борьбе с киберпреступлениями.

В результате, учитывая вышеизложенный научный, нормативный, аналитический, статистический материал, можно сделать вывод о том, что устранение вышеизложенных причин совершения неправомерных деяний в ИТ-сфере должно быть симметричным и адекватным со стороны общества, предполагающим устранение всех обстоятельств и условий, их порождающих (политических, правовых, социальных, экономических, кадровых и других) как государственными силами, так и общественными организациями. Таким образом, профилактика и противодействие компьютерной преступности в современной России должны быть всеобъемлющими и комплексными.

СПИСОК ЛИТЕРАТУРЫ

1. Уголовный кодекс РФ от 13 июня 1996-го года № 63-ФЗ // Собрание законодательства Российской Федерации, 1996 г.
2. Официальный сайт Министерства внутренних дел Российской Федерации [Электронный ресурс]: МВД России, 2021 г. Режим доступа:https://xn--b1aew.xn--p1ai.
3. Официальный сайт Генеральной прокуратуры Российской Федерации [Электронный ресурс]: портал правовой статистики, 2021 г. Режим доступа: https://genproc.gov.ru.
4. Официальный сайт Kaspersky [Электронный ресурс]: АО «Лаборатория Касперского» – 2021 г. Режим доступа: https://www.kaspersky.ru/resource-center/threats/what-is-cybercrime.
5. Суходолов А.П., Колпакова Л.А., Спасенников Б.А. Проблемы противодействия преступности в сфере цифровой экономики // Всероссийский криминологический журнал, 2017 г. Т. 11, № 2. с. 258–267.
6. PwC [Электронный ресурс]: Международная сеть компаний, предлагающих услуги в области консалтинга и аудита/пресс-центр, 2017 г. – TueApr 06 12:06:56 UTC 2021 г. Режим доступа:https://www.pwc.ru/ru.

УДК 338.1

В. С. КАМЕНЕВ
vad.kameneff@yandex.ru
Науч. руководитель – канд. экон. наук, доц. С. М. ДАВЛЕТШИНА

Уфимский государственный авиационный технический университет

ПРЕДНАМЕРЕННОЕ БАНКРОТСТВО КАК УГРОЗА ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ГОСУДАРСТВА

Аннотация. Актуальность данной темы заключается в том, что в современной России все чаще встречаются случаи, когда, с целью уйти от задолженности перед кредиторами, физические и юридические лица умышленно приводят хозяйствующий субъект к банкротству. В соответствии с действующим законодательством данное действие квалифицируется как преднамеренное банкротство.
Ключевые слова: банкротство; преднамеренное банкротство.

Юридические и физические лица в процессе своей деятельности вступают в денежные отношения с другими организациями, банками, государственными структурами и т.д. Возникающие обстоятельства имеют сроки исполнения, согласованные со сторонами заключения договора, соглашения, нарушение которых ведет к рискам, в последствии могут привести к банкротству организации. Коммерческая деятельность такого предприятия прекращается, имущество реализуется для удовлетворения требования кредиторов. Для понимания сущности такого явления как преднамеренное банкротство, разберемся что такое банкротство?

Несостоятельность (банкротство) (далее также – банкротство) – признанная арбитражным судом или наступившая в результате завершения процедуры внесудебного банкротства гражданина неспособность должника в полном объеме удовлетворить требования кредиторов по денежным обязательствам, о выплате выходных пособий и (или) об оплате труда лиц, работающих или работавших по трудовому договору, и (или) исполнить обязанность по уплате обязательных платежей. [1]

Однако, институт банкротства зачастую является объектом преступной деятельности, так как схема признания лица банкротом нередко используется в

неправомерных целях: уклонение от налогов, от кредиторской задолженности, что и является преднамеренным банкротством.

В стратегии экономической безопасности Российской Федерации на период до 2030 г., подписанной Президентом РФ от 13.05.2017 г. №208, говорится, что предотвращение преднамеренного банкротства и иных противоправных действий в отношении субъектов экономической деятельности является одной из основных задач по реализации направления, касающегося обеспечения безопасности экономической деятельности. [2]

Согласно статье 196 Уголовного кодекса Российской Федерации, под преднамеренным банкротством понимается умышленное создание или увеличение неплатежеспособности предприятия, которое совершил его руководитель, либо собственник, а также индивидуальный предприниматель в личных интересах или интересах третьих лиц, повлекший большой ущерб или иные тяжкие последствия, посредством заключения заведомо невыгодных сделок, принятия на себя чужих долгов в качестве поручителя и действий, ведущих к невозможности удовлетворить требования кредиторов Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ.

За данное преступление в качестве меры наказания могут быть применены: штраф, в размере от 200 тыс. руб. до 500 тыс. руб. или в размере заработной платы или иного дохода, полученного за срок от 1-3 лет; работы принудительного характера на срок до 5 лет; лишение свободы на срок до 6 лет с выплатой штрафа в размере до 200 тыс. руб. [3]

Стоит заметить, что в некоторых случаях предприятие приходит к неплатежеспособности неумышленным способом – в результате недобросовестного отношения к исполнения обязанностей, экономических ошибок и т.д. В этом случае арбитражный суд может признать отсутствие состава преднамеренного банкротства.

Согласно статистическому бюллетеню Единого федерального реестра сведений о банкротстве на 31.12.2018 г. (см. табл. 1), количество заключений о

наличии признаков преднамеренного банкротства растет с каждым годом в периоде с 2015 по 2018 гг.[4]

Таблица 1

Динамика количество заключений о наличии признаков преднамеренного банкротства

	2015 г.	2016 г.	2017 г.	2018 г.
Количество заключений о наличии признаков преднамеренного банкротства	906	1 310	1 636	1 876
Количество заключений об отсутствии признаков преднамеренного банкротства	7 526	11 167	18 291	23 043
Количество заключений с признаком «недостаточно информации»	2 448	3 409	4 447	4 877
Доля заключений о наличии признаков преднамеренного банкротства	8%	8%	7%	6%

Данное явление есть угроза для безопасности предприятия, государства и общества в целом, так как велики ее негативные последствия. Поэтому преднамеренное банкротство является особым элементом криминальной экономики в системе экономической безопасности экономики государства, что выделяет ее высокую опасность данного явления и показывает ее важность для изучения.

В настоящее время в России не существует универсальной методики анализа финансовой отчетности и хозяйственной деятельности организации, предполагающей комплексное изучение предприятия с учетом специфики отрасли, в которой оно работает. В то же время зарубежные ученые и специалисты в области банкротства хозяйствующих субъектов, а также причин его возникновения доказали, что из рассчитанного набора финансовых показателей лишь немногие являются информативными, более точно прогнозирующими возможность банкротства, причины его образования. В связи с этим, используемые за рубежом модели прогнозирования банкротства и оценки кредитного риска неприменимы к условиям российской экономики.

Поэтому, в сфере борьбы с преднамеренным банкротством предлагается некоторыми авторами такая система диагностики, которая включает в себя 3 основных шага:

1) проведение авторского коэффициентного анализа, который включает в себя 16 коэффициентов, разделенных на 4 группы (платежеспособность, ликвидность, рентабельность и финансовая устойчивость);

2) применение системы выявления сделок предприятия, направленных на преднамеренное банкротство, включающей в себя анализ строк баланса;

3) выборка из всех количеств сделок, которые негативно повлияли на финансово - экономическое состояние предприятия, а именно, тех сделок, которые привели предприятие к преднамеренному банкротству (сделки должны были стать причиной банкротства).

Первым шагом является проведение коэффициентного анализа финансово-хозяйственной деятельности предприятия. как говорилось выше, данный шаг включает в себя анализ четырех финансовых показателей: платежеспособность, ликвидность, рентабельность и финансовая устойчивость.

Беря во внимание классические методы поведения финансового анализа для подобных целей [10,12], а также особенность данного исследования, в систему показателей платежеспособности были включены показатели:

1) общая платежеспособность;

2) степень платежеспособности по текущим обязательствам;

3) степень платежеспособности общая;

4) коэффициент платежеспособности.

Основная масса применяемых коэффициентов широко используются при проведении различных финансовых анализов на предприятиях различных типов. Эта группа показателей была выбрана в качестве основного показателя, поскольку платежеспособность компании является основным условием, определяющим ее банкротство, в особенности преднамеренное. Анализ динамики этих показателей платежеспособности может помочь определить период такой операции и идентифицировать саму сделку. [7]

Ко второй группе относятся показатели ликвидности. Если рассматривать данный показатель со стороны анализа предприятия на обнаружение на нем

преднамеренного банкротства, то показатель ликвидности может указать, насколько ликвидны активы предприятия.

При анализе деятельности и операций главы предприятия важным элементом является анализ ликвидности. На практике основными действиями, направленными на преднамеренное банкротство, являются операции, направленные на замену ликвидных активов неликвидными. Следовательно, использование этих коэффициентов поможет выявить сроки совершения этих операций и определить их влияние на ликвидность.

Поэтому, показателями ликвидности являются:

1) коэффициент цены ликвидности;

2) коэффициент абсолютной ликвидности;

3) коэффициент текущей ликвидности;

4) коэффициент быстрой (срочной) ликвидности.

Третья группа – показатели рентабельности предприятия. Для предприятия, находящегося на грани банкротства, данные показатели являются актуальными, так как динамика показателей рентабельности может показать эффективность работы предприятия, а также позволит узнать, насколько эффективно были использованы привлеченные и заемные средства предприятия. В состав коэффициентов рентабельности входит:

1) коэффициент общей рентабельности;

2) коэффициент рентабельности прямых затрат;

3) коэффициент рентабельности продаж;

4) коэффициент рентабельности активов.

Последнюю группу рассчитываемых показателей составляют показатели финансовой устойчивости. Эти показатели были выбраны из-за их значимости для компании, находящейся на грани банкротства. Это показатели финансовой устойчивости, которые характеризуют независимость каждого элемента активов компании и активов в целом и позволяют оценить, является ли компания достаточно устойчивой в финансовом отношении.

1) коэффициент финансовой зависимости;

2) коэффициент обеспеченности собственными средствами;

3) коэффициент автономии;

4) коэффициент соотношения заемных и собственных средств.

Второй шаг предложенной системы диагностики преднамеренного банкротства является одной из важнейшей частью описанной системы, так как он описывает новую систему выявления сделок компании, направленных на преднамеренное банкротство. Данный метод реализуется путем анализа коэффициентов, показывающих динамику определенных показателей бухгалтерского учета, свидетельствующих о наличии умышленного банкротства в компании, с целью дальнейшего выявления операций, которые могут повлиять на устойчивость компании.

Главным методом в данном шаге является оценка влияния сделок, который показывает, как определенная сделка оказала влияние на общеэкономическую стабильность предприятия.

Третий шаг включает в себя метод оценки влияния сделок, который показывает, как повлияло изменение значения отдельно взятой строки бухгалтерского баланса под влиянием определенной сделки на исследуемый показатель. Данный шаг заключает в себе 5 этапов:

1 этап: находим значение строк отчетности рассчитываемых коэффициентов на последнюю отчетную дату перед началом осуществления исследуемой сделки;

2 этап: корректируем значение строк на изменения, вызванные хозяйственными операциями, осуществляемыми в рамках данной сделки;

3 этап: пересчитываем коэффициенты с учетом изменений строк отчетности;

4 этап: производим сравнение рассчитываемых коэффициентов до и после корректировки строк на изменения, вызванные исследуемой сделкой;

5 этап: производим оценку динамики коэффициентов и даем предварительное заключение о возможности нацеленности исследуемой сделки на преднамеренное банкротство.

Несмотря на все выше сказанное, следует отметить, что, к сожалению, невозможно охватить весь спектр сделок, осуществление которых могло повлечь за собой неплатежеспособность компании, из-за проверки ограниченного количества статей баланса. Предложенный выше метод позволяет исследовать те сделки, которые невозможно увидеть при простой проверке на предмет преднамеренного банкротства, и продемонстрировать их реальную важность для формирования экономической устойчивости предприятия.

Введение такой системы диагностики преднамеренного банкротства поспособствует развитию открытого и честного бизнеса в нашей стране, а также увеличит ее экономическую конъюнктуру, так как главы предприятий потеряют возможность уйти от исполнения обязанностей через осуществление преднамеренного банкротства. Также это позволит обеспечивать высокую экономическую и производственную безопасность государства, что снизит финансовый ущерб от подобной незаконной деятельности.

Работа такой системы диагностики преднамеренного банкротства значительно повысит уровень экономической безопасности. Результатом может стать уменьшение ущерба от данной незаконной деятельности, который по оценкам некоторых исследователей составляет около 5 миллиардов рублей ежегодно, что существенно сказывается на бюджетных и налоговых поступлениях в федеральный бюджет.

Таким образом, данная система будет содействовать созданию налоговой, финансовой и производственной безопасности, а уменьшение числа осуществляемых преднамеренных банкротств благоприятно скажется на общеэкономической конъюнктуре.

СПИСОК ЛИТЕРАТУРЫ

1. Федеральный закон от 26.10.2002 N 127-ФЗ (ред. от 30.12.2020) "О несостоятельности (банкротстве)" (с изм. и доп., вступ. в силу с 02.01.2021)
2. Указ Президента РФ от 13.05.2017 г. № 208 «О Стратегии экономической безопасности Российской безопасности на период до 2030 года» // СЗ РФ. – 2017. – № 20. – Ст. 2902.
3. "Уголовный кодекс Российской Федерации" от 13.06.1996 N 63-ФЗ (ред. от 30.12.2020) УК РФ Статья 196. Преднамеренное банкротство
4. Федресурс www.fedresurs.ru
5. Постановлением Правительства Российской Федерации от 27.12.2004 N 855.
6. Азрякова И.В. «Определение зоны повышенного риска с целью выявления признаков преднамеренного банкротства» // Вестник финансового университета. – 2011. – № 3. – с. 61-65
7. Азиятов М.М. «Понятие и признаки преднамеренного банкротства» // Проблемы экономики и юридической практики. – 2010. – № 5. – с. 129-130.
8. Львова Н.А. «Теория и практика преднамеренного банкротства» // Вестник Санкт-Петербургского университета. серия 5. экономика. – 2004. – № 4. – с. 113-122.
9. Тарасенко К.М. «Роль маркетинговых инноваций в системе мер экономической профилактики преднамеренного банкротства предприятий и индивидуальных предпринимателей»., 2010.
10. Вержбицкая И.В «Применение методов экономического анализа при выявлении признаков фиктивного и преднамеренного банкротства» // Современные тенденции в экономике и управлении: новый взгляд. – 2012. – № 17. – с. 142-146.
11. Чистопашина С.С., Полисюк Г.Б. «Характеристика банкротства как важнейшей экономической категории в условиях кризиса и основные причины его возникновения» // Эко. – 2011. – № 47. – с. 52-56.
12. Виноградова М.М. «О возможности применения методологических положений и рекомендаций по проведению анализа финансового состояния хозяйствующего субъекта, разработанных различными министерствами и ведомствами, при производстве судебных экономических экспертиз» // Теория и практика судебной экспертизы. – 2011. – № 1(21). – с. 94-101.

УДК 336.7

Ю. О. КИРИЛОВА, М. М. ШАБАНОВА
Yulia000.Kirilova@yandex.ru
Науч. руководитель – канд. экон. наук, доц. А. В. СТАРЦЕВА

Уфимский государственный авиационный технический университет

ОСНОВНЫЕ УГРОЗЫ БЕЗОПАСНОСТИ ФУНКЦИОНИРОВАНИЯ ФОНДОВОГО РЫНКА

Аннотация. Выявляются взаимосвязь фондового рынка и основных угроз безопасности. Сегодня именно фондовый рынок является наиболее уязвимой частью всего финансового рынка, поэтому в данной статье рассматриваются кризисы фондового рынка и их воздействие на экономическую безопасность государства, возникающие из-за нестабильности рынка ценных бумаг, предлагаются варианты их снижения.
Ключевые слова: экономическая безопасность; фондовый рынок; кризис.

Актуальность темы состоит в том, что на современной этапефондовый рынок играет значительную роль в развитии рыночной экономики страны, способствует аккумулированию, перераспределению в более выгодные сферы денежных средств и капиталов, опосредует взаимоотношения между субъектами экономики. Невыполнение фондовым рынком своих функций парализует экономические связи и представляет угрозу экономической безопасности государства, то есть существует зависимость экономического состояния государства от уровня экономической безопасности фондового рынка.

Обеспечение экономической безопасности фондового рынка подразумевает возможность использования различных механизмов защиты интересов государства и государственных финансов, возможность переводить средства в нуждающиеся отрасли экономики, оперативно реагировать на рыночные изменения, а также разнообразные преступные действия, направленные на дестабилизацию экономической безопасности фондового рынка.

Рассмотрим кризисы фондовых рынков и их влияние на экономическую безопасность:

1) обвал фондового рынка. Мировой финансово-экономический кризис 2008 года, начавшийся в кредитном секторе США, привел к массовым прода-

жам ценных бумаг на фондовых биржах. Произошло резкое падение цен на облигации и значительное сокращение их выпуска. Падение акций США стало катализатором коллапса в других странах, связанных с американской экономикой, что привело к мировой рецессии. Отсутствие ликвидности на мировом рынке капитала также сказалось на российской экономике. Это привело к падению российского фондового рынка и снижению цен на внутренние облигации.

Первой жертвой экономического кризиса 2008 года стал инвестиционный банк «КИТ Финанс», имеющий невыполненные обязательства по операциям РЕПО, по разным оценкам, в размере 6–10 млрд рублей. Далее следуют Связьбанк, Собинбанк, Глобэкс. Только продажа спасает их от полного банкротства. Их покупатели - РЖД и АЛРОСА, ВЭБ, близкие к государству структуры. Правительству пришлось прибегнуть к использованию золотовалютных резервов страны.

В период кризиса многие компании имеют значительные долги перед банками, поставщиками оборудования и материалов. Поэтому, когда возникают трудности с продажей промышленных товаров и, как следствие, сокращением притока денежного капитала, многие фирмы становятся неплатежеспособными должниками. Например, в Нижегородской области в 2008 г. возбуждалось около 170 процедур банкротства в отношении предприятий региона. Оказавшись банкротами, некоторые прекратили свою деятельность, другие получили новые ссуды или отсрочку платежей, но на очень сложных условиях, в основном в виде повышения процентных ставок. Многие предприниматели, попавшие в долговую петлю, обращались за кредитами на любых условиях, чтобы избежать банкротства. Это привело к резкому росту процентных ставок. В России по официальным данным долги по иностранным кредитам составляли 700 млрд долл. США.

Таким образом, можно сказать, что кредитный кризис вызывает спад производства и распространяется на реальный сектор экономики.

В связи с волной банкротств, смывающей значительную часть оборотного капитала и удерживающей на поверхности тех, кто своевременно выплачивал векселя, спрос на ссудный капитал резко падает. Решающим фактором здесь является сокращение производства товаров и услуг и, в частности, сокращение новых инвестиций в основной капитал.

Доля инвестиций в основной капитал в ВВП – это один из показателей экономической безопасности. В период кризиса 2014- 2015 гг. этот показатель был самым низким за последние десять лет и в 2015 г. составил 17,8%;

2)глобальный крах фондовых рынков начался 19 февраля 2020 года. В «черный понедельник» – 9 марта – все три показателя сократились всего за сутки более чем на 7%: эта рецессия была признана наиболее губительной со времен кризиса 2007 года.

В «черный четверг» – 12 марта – Нью-Йоркская фондовая биржа обвалилась на 9%, а итальянская BorsaItaliana– на 17%.

Причинами очередного финансового кризиса, вызванного пандемией COVID-19, называют:

1) остановку работы 70-90% производственных объектов и предприятий услуг в охваченных вирусом странах;

2) временный паралич экономики Китая, которая начала свое восстановление с середины марта 2020 года;

3) война цен на нефть между Россией и Саудовской Аравией;

4) замедление мировой торговли ввиду закрытия границ более 80 стран мира.

Нынешний итог неблагоприятного влияния пандемии на фондовые рынки: сокращение индекса S&P 500 на 29,5% всего за 19 дней. Динамика биржевых торгов волатильная: если 13 марта показатель увеличился на 12%, то в последующие дни терял по 2–4% за сутки.Также можно сказать, что данный кризис достаточно сильно повлиял на экономическую безопасность страны. Уро-

вень ВВП уменьшился, кредитно-банковская система стала не стабильной, повысился уровень инфляции.

Мы выделили несколько кризисов на фондовом рынке, которые негативно повлияли на экономическую безопасность России. Руководству страны следует обращать внимание на все эти кризисы при определении направлений развития государства. Необходимо принять меры для их устранения или хотя бы минимизации, поскольку без этого экономической безопасности, а вместе с ней и безопасности страны в целом, не будет достаточных гарантий.

Можно рассмотреть несколько действий, с помощью которых возможно предотвратить фондовые кризисы:

1) официально разработать и принять на законодательном уровне документ, содержащий перечень индикаторов экономической безопасности фондового рынка и их пороговых значений;

2) для успешного применения официальных показателей экономической безопасности необходимо осуществлять их мониторинг и оперативно реагировать на их изменения.

Таким образом, подведем итог, говоря о вышесказанных кризисах фондовых рынков и их влиянии на экономическую безопасность страны, можно сказать, что кризисы негативно влияют на экономическую безопасность. Также мы смогли выделить несколько действий, которые позволят предотвратить кризисы фондовых рынков.

СПИСОК ЛИТЕРАТУРЫ

1. Экономическая безопасность России: Общий курс: Учебник / Под ред. В.К. Сенчагова. - М.: Дело, 2008.
2. Экономическая и национальная безопасность: Учебник / Под ред. д.э.н., проф. Л.П. Гончаренко. - М.: ЗАО «Издательство «Экономика», 2015.
3. Экономическая безопасность: учеб. пособие для студентов вузов / В.А.Богомолов. -М.: ЮНИТИ-ДАНА, 2020.
4. Финансово кредитный словарь Том 1 (1961), с.143.
https://studbooks.net/2018805/ekonomika/krizisy_istorii_rossii (Кризисы в истории России)

УДК 336.76

З. М. МАКАРЕНКО
zahar-makarenko@mail.ru
Науч. руководит. – канд. экон. наук, доц. А. В. СТАРЦЕВА

Уфимский государственный авиационный технический университет

ПЕРСПЕКТИВЫ И РИСКИ КОМПАНИЙ ПО ПРИОБРЕТЕНИЮ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ (SPAC)

Аннотация. В последнее время на фоне роста фондового рынка, масштабного притока новых инвесторов многие частные компании приняли решения стать публичными. Это способствует росту популярности компаний по приобретению специального назначения (SPAC) как альтернативы классическому IPO. В статье рассмотрен механизм реализации SPAC, определены преимущества и риски для всех участников, а также рассмотрены проблемы, создаваемые этими компаниями, и пути их решения.
Ключевые слова: SPAC; IPO; слияние; акция; варрант.

Компания по приобретению специального назначения или SPAC (specialpurposeacquisitioncompany) – компания, создаваемая с целью слияния с частной компанией, которая хочется стать публичной, минуя процедуру IPO. Фактически компании SPACявляются пустышками, поскольку не имеют активов, не осуществляют никакой деятельности, кроме поиска компании для слияния. Данная деятельность получила наибольшую популярность в США.

История таких компаний начинается с первичного публичного размещения их юнитов, каждый из который включает себя акцию и часть варранта. По правилам Комиссии по ценным бумагам(SEC), акции SPAC размещаются по фиксированной цене в 10 долларов. Средства, полученные при первичном размещении, помещаются на эскроу-счет и их можно потратить только на приобретение частной компании. Срок их существования– 2 года [3]. Если за этот срок менеджеры не смогли найти подходящую компанию, то происходит ликвидация SPAC, а средства возвращаются инвесторам. В случае, когда цель для слияния найдена, происходит голосование инвесторов, результатом которого является либо слияние, либо отказ от него и дальнейший поиск уже другой компании.

Рассмотрим мотивы всех сторон и риски, которые они на себя принимают. Основными бенефициарами в случае успешного слияния являются менеджеры SPAC. Они имеют возможность приобрести около 20% акций компании за номинальную стоимость, их прибыль не ограничена. Главный риск, который они на себя берут – потеря денежных средств, затраченных на создание технической компании, в результате ликвидации. Не менее важен репутационный риск: если менеджеры не смогут за 2 года найти компанию-цель, то им будет сложно попробовать себя в этом деле еще раз.

Для частного бизнеса SPAC– возможность выйти на биржу с меньшими затратами денег и времени. В среднем выход на биржу через слияние со SPACзанимает 3–4 месяца, в случае IPOэтот процесс может занять несколько лет. Время очень ценно для частных компаний, поскольку большая их часть старается выйти на биржу, когда на рынке царит бычий тренд и имеется возможность привлечь больше денежных средств [1].

Для инвестора это возможность вложиться в успешный бизнес, которого еще нет на рынке. Эскроу-счета гарантируют безопасность вложенных средств. Если инвестору не понравится конечная компания, то он может проголосовать против, вернуть акции и получить свои деньги обратно. Но при этом у него остается варрант, который сохраняет за ним возможность заработать при удачном стечении обстоятельств.

На сегодняшний день компании по приобретению специального назначения набирают популярность (рис. 1). Только лишь за 1 полугодие 2021 года было проведено больше публичных размещений SPAC, чем за 5 предыдущих лет. Резкий рост популярности вызывает опасения по поводу появления пузыря в этой сфере.

Только сейчас на рынке около 445 компаний по приобретению специального назначения ищут цель для слияния. В связи с этим возникает вопрос: смогут ли они найти хорошие частные компании? Если нет, то в лучшем случае по истечению срока своей жизни они ликвидируются. Однако, как показывают

данные за период с 2003–2021 гг. из 1059 компаний только 90 были ликвидированы [4].

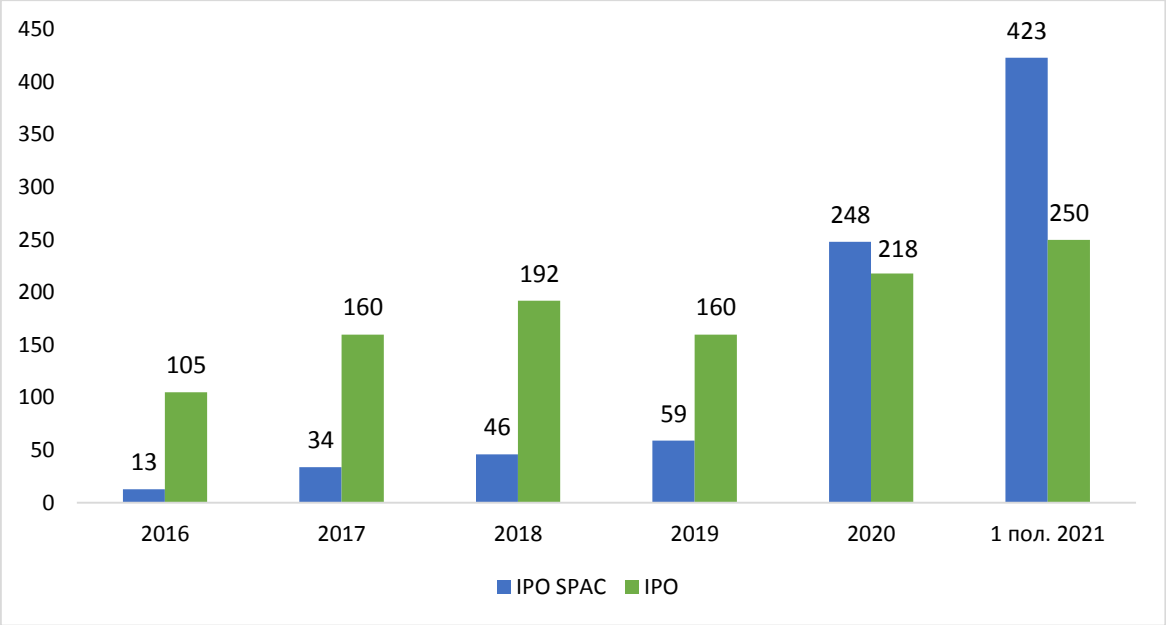


Рис. 1. Количество IPOSPACи IPO в США [4]

В худшем случае может произойти волна слияний с некачественными компаниями. Есть несколько причин, которые могут к этому привести. В случае ликвидации менеджеры несут убытки на миллионы долларов, которые они потратили на создание SPAC. Поэтому они заинтересованы в слиянии даже с некачественными компаниями. При этом, дажеесли после слияния акции упадут в цене, то менеджеры останутся в плюсе, поскольку они получают 20% долю за номинальную стоимость. Это может значительно снижать их мотивацию, несмотря на репутационные риски.

Конечно, слияние не может произойти только лишь по решению менеджеров, нужно получить одобрение со стороны инвесторов. По данным Майкла Клауснера из StanfordLawSchool и Майкла Олрогге из NYU SchoolofLaw медианная доля возвратов акция составляет 73% [2]. Таким образом, получается, что многие инвесторы голосуют за слияния, а затем предъявляют свои акции к возврату. Так происходит, потому что инвесторы имеют не только акции, но и варранты, которые они оставляют у себя в надежде на получение прибыли в будущем. В результате на рынок может выйти множество не очень качествен-

ных компаний, в частности стартапов, которые даже не имеют реальной продукции, как было с компанией Nikola.

Мне кажется, чтобы не допускать этой ситуации, необходимо пересмотреть некоторые требования к SPAC. Во-первых, пересмотреть систему вознаграждения менеджеров и привязать ее к результатам их деятельности, в частности выдавать им варрантывзамен их 20% доли. Во-вторых, нужно отменить возможность возврата акций в случае голосования за слияние илиуменьшать количество варрантов у инвестора в случае, если он предъявляет акции к возврату.

Таким образом, компании по приобретению специального назначения имеют ряд преимуществ и в настоящий момент становятся альтернативой традиционному IPO. В дальнейшем необходимо ужесточить регулирование SPAC, чтобы не допустить выхода на биржу некачественных компаний.

СПИСОК ЛИТЕРАТУРЫ

1. Vatsal, G., SPAC: Special Purpose Acquisition Company // Independently published, 2021. С. 17–18
2.Klausner M.,OhlroggeM., RuanM.,A Sober Look at SPACs // Finance Working Paper № 746/2021. 2021. – URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3720919/ (датаобращения: 02.09.21)
3. Дубровский А., Мафия SPAC: кто зарабатывает на компаниях-пустышках и есть ли пузырь на рынке // Forbes. 2021. URL: https://www.forbes.ru/finansy-i-investicii/420765-mafiya-spac-kto-zarabatyvaet-na-kompaniyah-pustyshkah-i-est-li-puzyr-na (дата обращения: 03.09.21)
4. Официальный сайт SPACAnalytics [Электронный ресурс]. URL: https://www.spacanalytics.com/ (дата обращения: 01.09.21)

УДК 33.338

В. Р. МОХОВА, Р. Р. ЗИЯТДИНОВА
veronikamohova5@gmail.com
Науч. руководв. – ст. преп. И. В. ДМИТРИЕВА

Уфимский государственный авиационный технический университет

ФОНДОВЫЙ РЫНОК В РОССИИ: СОВРЕМЕННОЕ СОСТОЯНИЕ

Аннотация. Фондовый рынок является важным инструментом экономического роста, так как способен трансформировать сбережения в инвестиции. Поэтому в условиях мирового кризиса исследование условий формирования и тенденций развития российского фондового рынка является актуальным. В данной статье рассматриваются основные проблемы, препятствующие эффективному развитию фондового рынка в России. Дается сравнение фондовых бирж России и США, по которым можно выделить критерии работы этих рынков, исходя из необходимых составляющих для успешной торговли. На основе анализа фондового рынка России предложен комплекс мер по устранению проблем развития: привлечение отечественных и иностранных инвесторов, увеличение эмитентами дивидендной доходности по акциям, совершенствование нормативно-правовой базы и системы налогообложения и др.
Ключевые слова: фондовый рынок; проблемы развития фондового рынка в России; состояние фондового рынка на сегодня.

Фондовый рынок в России является сравнительно молодым, поэтому многие западные рейтинговые агентства продолжают относить его к категории развивающихся рынков, для которых характерна более высокая степень доходности, объясняющаяся, в свою очередь, и более высокой степенью риска.

Фондовый рынок – это место, где происходит торговля акциями, облигациями, валютами и прочими активами. Понятие рынка затрагивает не только функцию передачи ценных бумаг, но и другие операции с ними, такие, как выпуск и налогообложение. Кроме того, он позволяет устанавливать справедливое ценообразование.

Рынок ценных бумаг имеет определенные признаки:

– у него всегда есть фиксированная торговая площадка, например, фондовый рынок Московской биржи;

– обязательно наличие специализированного механизма отбора товаров (активов), отвечающих определенным требованиям;

– установлены торговые процедуры по времени и стандартам;

– все оформление сделок централизованно;

–деятельность всех участников рынка контролируется уполномоченными органами;

– существуют официальные котировки активов.

Ценные бумаги играют большую роль для экономики России, так как большая их часть является одним из способов финансирования инвестиций. Рынок ценных бумаг дает всем субъектам экономики доступ к получению необходимых им денежных средств.

У развития фондового рынка в современной России есть ряд проблем.

На сегодняшний день российский фондовый рынок и его возможности не привлекают большинство потенциальных российских инвесторов по тем или иным причинам.

Анализ литературы по данной проблематике показал, что к основным проблемам, препятствующим эффективному развитию фондового рынка России, можно отнести следующие.

Во-первых, низкий уровень капитализации российского фондового рынка. На сегодняшний день стоимость всех публичных компаний страны не превышает 39% от ВВП России. К примеру, в 2007 г. капитализация фондового рынка составляла 107,7% от размера российской экономики. Сейчас на территории России функционирует 10 бирж, причем 80% от общего объема продаж совершаются на трех: Московская биржа (ММВБ-РТС); Валютная биржа Санкт-Петербурга (СПВБ); Сибирская межбанковская валютная биржа (СМВБ).

Самыми важными показателями фондового рынка в России, конечно же, по сей день являются Московская биржа и Валютная биржа Санкт-Петербурга.

Площадка, ныне носящая имя «Московская биржа», основана ближе к концу 2011 года. На фондовом рынке Московской биржи осуществляется сделки с использованием акций российских и иностранных компаний, инвестиционных паев и облигаций.В последние годы ММВБ состоит в ТОП-20 мировых

лидеров по количеству заключаемых сделок. Мосбиржа открывает брокерам возможность взаимодействовать с 6 рынками. На этой бирже осуществляется самый большой объем торгов.

В среднем на фондовом рынке проходит дневной оборот примерно на 1,3 трлн руб. Торгуются на бирже 294 акции 234 компаний.

На рынке представлены фьючерсные контракты на следующие группы активов:

– на индексы РТС, ММВБ и ММВБ (мини) и на волатильность российского рынка;

– на акции наиболее крупных компаний;

– на валютные пары доллар США/российский рубль, евро/доллар США, доллар США/японская иена и т.д.

– на процентные ставки однодневных кредитов RUONIA;

– на товарные активы — нефть сорта Brent, золото, серебро, платину и палладий.

Самые активные акции, которые котируются почти на всех биржах представлены на рисунке 1. В целом именно акции этих компаний уже долгое время являются самыми покупаемыми и продаваемыми на рынке ценных бумаг за последние несколько лет. Также в топ лидеров входят такие акции, как РУСАЛ, Яндекс, Магнит, Роснефть, Татнефть, ММК ОАО и др.

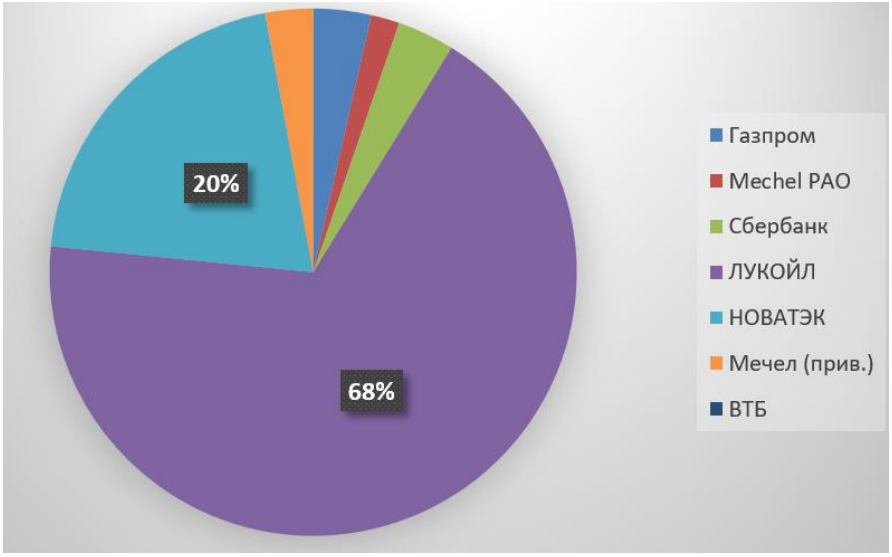


Рис. 1. Самые активные акции на МосБирже

Вторая причина – это отсутствие современной системы центров клиринговых расчетов, независимых регистраторов, обеспечивающих информационную «прозрачность» рынка для всех участников фондового рынка, а также развитой инфраструктуры и достаточного информационного обеспечения. В настоящее время на биржах России информация об эмитентах и их ценных бумагах раскрывается недостаточно хорошо.

Высокая степень мошенничества на российском фондовом рынке отталкивает потенциальных внутренних и внешних инвесторов.

И последняя, но не по важности, проблема – действующее в России налогообложение операций по движению фондовых активов. Например, российское налоговое законодательство взимает налог не с номинальной стоимости акций, а с их рыночной стоимости, поэтому наблюдается отток инвесторов, предпочитающих те площадки, где государство стремится снизить уровень налогообложения операций.

Таким образом, перечисленные проблемы в настоящее время являются препятствием для увеличения вовлеченности и активности на российском фондовом рынке внутренних и внешних инвесторов и как следствие, успешного развития фондового рынка России.

Перспективы развития фондового рынка состоят во вполне реальном разрешении указанных проблем.

– снижение законодательных требований для более легкого вхождения на рынок частных инвесторов и мелких компаний, желающих разместить свои акции и увеличить свой оборотный капитал.

– повышение культуры инвестирования среди населения.

В целом перспективы на 2021– 2022 годы далеки от идеальных. Многое зависит от того, как быстро рассеется эпидемиологическая неопределенность в мире. Вместе с тем, кризисные времена открывают новые возможности. В этом году было и угрожающее падение стоимости активов, и взлет целых секторов, а не только отдельных компаний.

Что касается фондового рынка России на сегодня.

В 2020 году весь мир перенес кризис. Но не зря говорят, что кризис – это время новых возможностей. К концу года рублевый индекс не только отыграл все потери, но и обновил максимум, завершив год на отметке 3289,02 пункта (+7,98% по сравнению с началом года). Однако долларовый РТС подвело ослабление рубля, он продемонстрировал отрицательную динамику, потеряв за год 10,42%.

Нефтяные котировки после весеннего стресса не смогли восстановиться в полном объеме, чему отчасти способствовал новый всплеск заболеваемости COVID-19 осенью. Однако новости об успешных испытаниях противокоронавирусных вакцин и последовавших за этим прививочные кампании в нескольких странах помогли котировкам "черного золота" закрепиться в конце года выше $50 за баррель Brent.

Если сравнить фондовый рынок России и США, то можно выделить основные критерии работы этих рынков, исходя из необходимых составляющих для успешной торговли:

– ликвидность. Российская фондовая биржа обладает высоким потенциальным ростом для долгосрочных вложений с дальнейшей перспективой роста. Это, пожалуй, ее основной плюс. Минус в том, что компаний, которые торгуют своими акциями на фондовом рынке РФ – чуть больше 300. Для сравнения – число акций мировых компаний на крупных американских биржах более 5000 и увеличивается с каждым днем.

Еще одним важным недостатком у российского фондового рынка считают его зависимость от цены на нефть. В случае ее изменения он реагирует самый первый, что негативно сказывается на стоимости ценных бумаг. Также российские биржи на 80% зависят от политической ситуации в стране. Когда политизированность американских бирж менее 30%.

В Америке даже финансовый кризис не может повлиять на рост цен большинства акций. Около половины всего мирового фондового рынка прихо-

дится на США. Комиссия российских бирж намного выше американских. На американском рынке доходность составляет 30% и более годовых;

– надежность. Хоть российский фондовый рынок и перспективный, в виду того, что он еще слишком молод, заниматься торговлей акциями там тяжело. Для этого нужно выбирать биржи США, где можно купить сверх ликвидной акции крупнейших корпораций. Именно поэтому торговать ценными бумагами лучше всего на американской бирже.

Для успешного развития фондового рынка в нашей стране необходимо провести комплекс мер, который будет включать в себя:

1. совершенствование законодательства;

2. улучшение механизмов привлечения инвесторов и защиты их интересов;

3. совершенствование регулирования на финансовом рынке;

4. предупреждение и пресечение недобросовестной деятельности на фондовом рынке;

5. формирование положительного имиджа российской фондовой биржи.

В заключении можно отметить, что решение изложенных задач позволило бы создать надежную базу долгосрочного роста российского финансового рынка и повышение его роли как в рамках национальной, так и мировой экономики. Однако это невозможно будет сделать без фундаментальных изменений в экономике России, снижении ее зависимости от цен на нефть, снижения политических рисков в стране, усовершенствования борьбы с коррупцией.

СПИСОК ЛИТЕРАТУРЫ

1. Рынок ценных бумаг. Под редакцией В.А. Галанова, А.И. Басова.Москва. «Финансы и статистика», 2001.
2. Рынок ценных бумаг. Под редакцией В. И. Колесникова, В. С. Торкановского.– Москва. «Финансы и статистика», 1998.
3. Колтынюк Б.А. Рынок ценных бумаг. Учебник для студентов ВУЗов, обучающихся по экономическим специальностям. Санкт-Петербург.Изд-во Михайлова В.А., 2000.
4. Под редакцией Н.Ю. Сайбель, А.В.Ковальчук. Фондовый рынок: проблемы и перспективы развития // Финансы и кредит – 2018.

УДК 336.7

А. И. ПАНИНА, Э. И. ЗАРИПОВА
panina.anechka@bk.ru
Науч. руководит. – канд. экон. наук, доц. А. В. СТАРЦЕВА

Уфимский государственный авиационный технический университет

СТАТИСТИЧЕСКИЙ АНАЛИЗ ИНФЛЯЦИОННЫХ ПРОЦЕССОВ В РОССИЙСКОЙ ФЕДЕРАЦИИ

Аннотация. В статье определяются основные факторы, присущие современной российской экономике, проводится анализ статистических данных по инфляции и обосновывается необходимость поддержания инфляции на приемлемо низком уровне.
Ключевые слова: инфляция; инфляционный процесс; инфляционные факторы; уровень цен; последствия; причины; антиинфляционная политика.

В экономической теории существует немало определений понятия инфляции, но все они сводятся к тому, что инфляционные процессы выражены в переизбытке в рамках обращения денежной массы, и как следствие, неконтролируемого роста стоимости товаров на рынке. Как известно инфляция сопровождается ростом цен на товары и обесценением национальной валюты. Инфляция в различных ее проявлениях – неизбежный спутник развития современной экономики. Уровень инфляции является объектом внимания не только ведущих экономистов страны, но и обычных граждан. Поэтому на сегодняшний день в России особую актуальность приобретает необходимость реализации комплекса мер по стабилизации инфляции на минимальном уровне.

На сегодняшний день инфляция является экономическим и социально-политическим феноменом, то есть зависит от социально-экономической ситуации и общественных настроений.

Выделим основные инфляционные факторы: рост совокупного спроса и сокращение совокупного предложения,повышение тарифов ЖКХ и цен на энергоресурсы со стороны естественных монополий,инфляционные ожидания [5].

Характерной особенностью российской экономики является зависимость от мировой валюты – долларизация национальной экономики [3]. Данное явле-

ние также сосредотачивает в себе инфляционный эффект: ослабление курса рубля приводит к росту цен на импортные товары и, таким образом, воздействует на инфляцию.

Мировой и национальный опыт свидетельствует о том, что инфляцию вполне можно регулировать и не допускать серьезных и непредсказуемых ситуаций. В России важную роль играет антиинфляционная политика, реализуемая Банком России [4].В этих условиях особую значимость приобретает налогово-бюджетная политика, рассматриваемая в качестве инструмента оживления спроса, стабилизации бизнес-циклов, снижения уровня безработицы и, таким образом, стабилизации в инфляционной сфере.

В 2020 Россия находилась на 4 месте по уровню инфляции в мире.

Так уровень инфляции в России по месяцам за 2019-2020 гг., представлен на рисунке 1 [5].

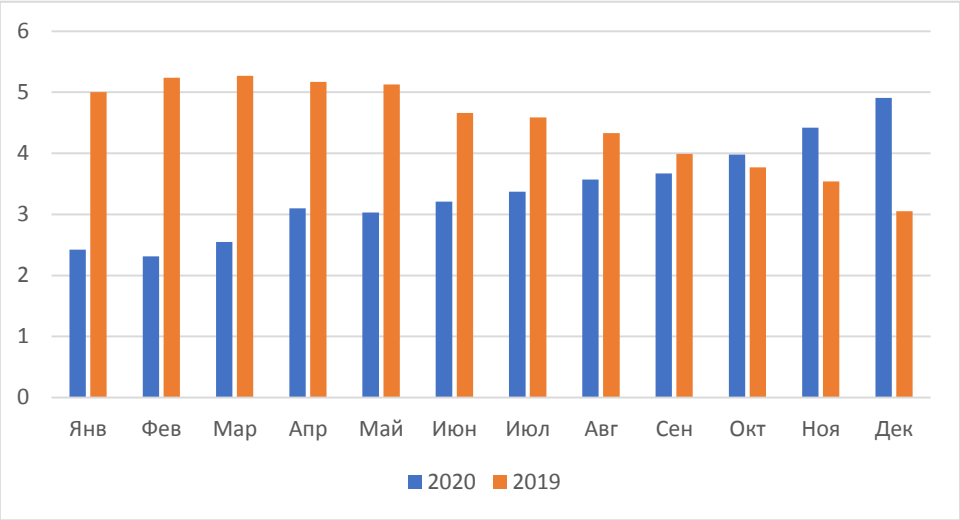


Рис. 1. Диаграмма уровня инфляции по месяцам в годовом исчислении, %

Инфляция в апреле 2020 года ускорилась до 3,1% по сравнению с апрелем 2019 года, ускорение по сравнению с мартом 2020 года– до 0,8%.

Годовая инфляция в марте составила 2,5%, в феврале – 2,3%, в январе – 2,4%.

За январь-апрель потребительские цены выросли на 2,6% по сравнению с аналогичным периодом прошлого года. Продовольственные товары в апреле

подорожали на 1,7% по сравнению с мартом 2020 года, в том числе продовольственные товары без плодоовощной продукции – на 0,9%.

Непродовольственные товары в апреле стали дороже на 0,4% по сравнению с предыдущим месяцем, услуги – на 0,1%.

В апреле существенное влияние на динамику цен на продовольственные товары оказал рост цен на плодоовощную продукцию. Банк России объясняет ускорение роста цен в марте-апреле ослаблением курса рубля вследствие падения цен на нефть и упреждающим спросом у населения на товары первой необходимости и продукты длительного хранения в условиях введения ограничительных мер для борьбы с коронавирусом.

В сезонно сглаженном выражении текущий рост цен находится вблизи уровней декабря 2018-го – начала 2019 года, когда инфляция временно ускорилась из-за снижения курса рубля и повышения НДС с 18 до 20%, указывает регулятор[2].Прогноз инфляции на 2020-2024 гг. представлен в таблице 1.

Таблица 1

Прогноз инфляции в РФ на период 2020-2024 гг., в % [6]

Год	Прогноз	Макс	Мин
2021	4.0%	4.75%	3.25%
2022	3.8%	4.18%	3.43%
2023	3.4%	3.78%	3.03%
2024	3.5%	3.88%	3.13%

Так по мнению аналитиков минимальный уровень инфляции будет зафиксирован в 2023 году на уровне 3,03-3,4 %.

О состоянии спроса со стороны населения можно судить по данным Росстата об инфляции в сегменте нерегулируемых рыночных услуг: юридических, образовательных, медицинских, школ вождения, языковых школ и т. д. Действительно, в середине 2019года спрос был ослабленным, цены в этом сегменте росли на 2,8-2,9% в годовом выражении, но в октябре – ноябре их рост ускорился сначала до 3,8%, а потом до 4,1%. Спрос на эти услуги лучше всего отражает изменения бюджета домохозяйств, он меньше зашумлен волатильностью курса или погоды.

Сейчас решения ЦБ влияют на спрос не напрямую, а через доходности ОФЗ. Ключевая ставка близка к нейтральному диапазону (6%), а доходность ОФЗ – к своему справедливому уровню: бескупонная доходность 10-летних ОФЗ составляет 6,3-6,4%, пятилетних – порядка 6%. Доходности ОФЗ формируют все ставки в экономике – например, по пятилетним ОФЗ можно прогнозировать средние ставки ипотеки – они выше примерно на 2,5 п. п. Скорее всего, все остальные ставки будут постепенно приходить в соответствие с этими доходностями.

Существуют следующие причины инфляционных процессов:

– рост государственных расходов. Государственные расходы могут существенно возрасти по нескольким причинам: войны, экономические кризисы, чрезвычайные происшествия. Именно в этот период государство начинает увеличивать денежную массу в стране для того, чтобы покрыть все эти расходы;

– увеличение объемов кредитования населения и юридически лиц. В данном случае речь идет о массовом кредитовании, при котором требуется дополнительное количество денежных средств, объем которых может спровоцировать рост инфляции;

– рост цен естественных монополий. Данные компании, не имея прямых конкурентов, могут позволить себе увеличивать цены на производимую продукцию и услуги. В этом случае рост цен на одни товары становится причиной роста цен на другие товары;

– снижение курса национальной валюты. Снижение курса национальной валюты при большой доле импортируемых товаров ведет к увеличению расходов как государства, если оно является импортером, так и юридических и физических лиц;

– неэффективная бюджетно-налоговая политика государства. Рост налогов, сборов, акцизов, а также их дополнительное введение, приводит к общему росту цен. Например, введение утилизационного сбора на автомобили приведет к равно пропорциональному увеличению стоимости автомобилей [1, с. 28].

Рассматривая проблемы инфляции со стороны государства, необходимо отметить тот факт, что государство является основным регулятором этого экономического явления. Отрицательные последствия инфляции для государства заключаются в росте расходов и снижении доходов бюджета, что может привести к его дефициту и повышению уровня внешнего и внутреннего государственного долга.

В большей степени при высоких темпах инфляции страдают категории граждан, чья заработная плата начисляется и выдается из бюджета. К таким категориям относятся врачи, учителя, воспитатели и др. Именно величина их заработка, как правило, не может превысить темпы роста инфляции в период экономической нестабильности. Инфляция затрагивает даже тех людей, которые просто копят свои деньги. При максимальной ставке по вкладам в 5% (ПАО «Сбербанк»), уровень инфляции в 2018 году составлял 4,27%. Получается, что в целом ставка по вкладам должна превышать уровень инфляции и не позволить денежным средствам обесцениться. Хотя по факту реальный уровень инфляции куда больше, представляемого нам государством.

Рассмотрим примеры изменения цен на основные товары для того, чтобы определиться с реальным уровнем инфляции:

– молоко – 26 руб. в 2009 году и 55 руб. в 2019 году (разница 55/26*100 = 211%). Таким образом, прирост стоимости молока составил в среднем 110%;

– бензин (АИ 92)– средняя стоимость на начало 2009 года составляла 18 руб./лит., в 2019 году средняя стоимость 1 литра бензина той же марки составляет 42 руб. (разница 42/18*100 = 233%). Таким образом, прирост стоимости молока составил в среднем 130%;

– новый автомобиль ToyotaCorolla. Стоимость такого нового автомобиля в 2009 году в обычной комплектации составляла 630 тыс.руб., сегодня же стоимость такого же автомобиля составляет более 1 млн. 300 тыс.руб. Фактически увеличение стоимости более чем в два раза.

В целях снижения риска роста инфляции, необходимо:

– проводить работу в области перехода расчетов на национальные валюты между странами поставщиками и экспортерами;

– контролировать рост государственных расходов и создавать различные резервы на случаи непредвиденных ситуаций;

– повышать эффективность экономической системы в целом, что позволит минимизировать риски, связанные с проявлением причин инфляции.

СПИСОК ЛИТЕРАТУРЫ

1. Алехин Б.И. Динамика инфляции в России и США / Б.И. Алехин // Экономический журнал. – 2017. – №44. – С. 2-30.
2. СтатБюро [Электронный ресурс]: официальный сайт.URL: https://www.statbureau.org/ru (дата обращения 26.10.2020).
3. Стратегия повышения финансовой грамотности в Российской Федерации на 2017 – 2023 годы от 25 сентября 2017 г.N 2039р [Электронный ресурс]: – URL: http://www.consultant.ru/document/cons_doc_LAW_278903/ 39ec12b6377db7506 f0726bd8f489685673ccb8d/ (дата обращения 26.10.2020).
4. Маслов А. В., Карчава Н.Э., Бердышев А. В. Характеристика инфляции в современной России // Студенческий форум: электрон. научн. журн. 2017. № 9(9). // [Электронный ресурс] URL: https://nauchforum.ru/journal/stud/9/23855 (дата обращения 26.10.2020).
5. Федеральная служба государственной статистики (Росстат). // [Электронный ресурс] URL: http://www.gks.ru. (дата обращения 26.10.2020).
6. Центральный банк Российской Федерации официальный сайт. // [Электронный ресурс] URL: http://www.cbr.ru (дата обращения 26.10.2020).

УДК 331

А. И. ПАНИНА
panina.anechka@bk.ru
Науч. руководитель – канд. пед. наук, доц. А. Ю. ФАРРАХОВА

Уфимский государственный авиационный технический университет

СТИЛЬ УПРАВЛЕНИЯ КАК ФАКТОР ФОРМИРОВАНИЯ ОРГАНИЗАЦИОННОЙ КУЛЬТУРЫ

Аннотация. Управление персоналом на современном этапе характеризуется определенными специфическими способами взаимодействия с персоналом. В статье представлено понимание стиля управления, его характеристики и классификация. Рассматривается взаимосвязь стиля управления и организационной культуры.
***Ключевые слова*:** руководитель; управление; стиль руководства; организационная культура.

За последние десятилетия было проведено множество исследований с целью изучения стилей управления, которые определяют характер действий руководителей по отношению к их подчиненным.

Стиль управления – это совокупность методов воздействия руководителя на работников, определенный тип его поведения по отношению к ним. От стиля управленческой деятельности зависит не только степень общей эффективности деятельности организации, в зависимости также находится мотивация персонала и его лояльность, производительность труда, степень вовлеченности сотрудников в принятие управленческих решений, морально-психологический климат в коллективе и другие [1]. Иными словами, стиль и характер действий руководителя по отношению к своим сотрудникам во многом определяет то, насколько быстро и эффективно будет развиваться и действовать организация и ее персонал. Рассмотрим стили управления персоналом (табл. 1).

Таблица 1

Стили управления персоналом

Стиль	Достоинства	Недостатки
Авторитарный	Точность отдаваемых приказов. Быстрые темпы выполнения. Не требует существенных экономических расходов. В новых компаниях позволяет ускорить процесс адаптации.	Нет работы над созданием благоприятного климата. У персонала слаба, развита мотивация. Текучесть кадров.

Окончание табл. 1

Демократический	Вопросы обсуждаются коллегиально. Благоприятная атмосфера в коллективе. Инициативность персонала в работе. Создаются инновации. Достижение результата с минимальными издержками. Комфортные условия труда.	Требует много сил и внимания со стороны руководства. На работу принимаются высококвалифицированные специалисты.
Либеральный	Лояльное обращение к персоналу. Выплата высокооплачиваемой зарплаты. Лояльное отношение к персоналу. Возможность проявить лидерские качества.	Двойственность в управления.

Основой жизненного потенциала любой организации является ее внутренняя культура. Организационная культура определяет, ради чего люди стали членами организации, как строятся отношения между ними, какие устойчивые нормы и принципы жизни они разделяют, что они считают хорошим или плохим и многое другое. Все это не только отличает одну организацию от другой, но и существенно влияет на успех ее деятельности.

Культура организации представляет собой сложный набор важных предположений, бездоказательно принимаемых и разделяемых членами группы или организации. Часто организационная культура трактуется как принимаемая большинством членов организации философия и идеология управления. Наиболее часто организационная культура понимается как ряд общих для всех сотрудников организации ценностей и убеждений, которые влияют на эффективность формулирования и реализации стратегии [7]. Существует множество определений организационной (корпоративной) культуры. В основной массе понятие «организационная культура» включает три ключевых элемента [6].

Первый – это базовые предположения, которых придерживаются члены организации в своем поведении и действиях. Эти предположения часто связаны с утвердившимися в организации представлениями индивида об окружающей среде (группе, организации, обществе, мире) и ее компонентах (природе, пространстве, времени, работе, отношениях и т.д.).

Второй – это ценности (или ценностные ориентации), которых может придерживаться индивид в принятии решений и последующих действиях. Цен-

ности помогают индивиду ориентироваться в том, какое поведение следует считать допустимым или недопустимым. Так, в некоторых организациях считается, что «клиент всегда прав», поэтому в них недопустимо обвинять клиента за неудачу в своей работе.

Третий – это «символика», посредством которой ценностные ориентации «передаются» членам организации. Многие фирмы имеют специальные, предназначенные для всех документы, в которых они детально описывают свои ценностные ориентации. Однако содержание и значение последних наиболее полно раскрываются работникам через «ходячие» истории, легенды и мифы. Их рассказывают, пересказывают, толкуют. В результате этого они иногда больше влияют на индивидов, чем те ценности, которые записаны в рекламном буклете компании.

Таким образом, организационная культура – это набор наиболее важных предположений, принимаемых членами организации и получающих выражение в заявляемых организацией ценностях, задающих людям ориентиры их поведения и действий[3]. Эти ценностные ориентации передаются индивидам через «символические» средства духовного и материального внутриорганизационного окружения. Рассмотрим типы организационных культур предприятия (табл. 2).

Таблица 2

Типы организационных культур

Тип	Характеристика
Клановая культура	Характеризуется высоким уровнем гибкости и внутренним фокусом. Представляет собой дружественный коллектив, члены которого имеют общие ценности и принципы. В таком типе культуры организация и ее подразделения рассматриваются как большая семья, а руководители компании играют роль воспитателей. Для организаций с таким типов организационной культуры характерен высокий уровень сплоченности коллектива. В основе приверженности организационным ценностям лежат традиции и преданность коллектива. Наибольшее значение в таких компаниях придается моральному климату внутри коллектива и его сплоченности. С точки зрения взаимодействия с внешней средой такая организация определяет свой успех через заботу о потребителях.

Окончание табл. 2

Адхократическая культура	Для адхократической культуры организации также характерен высокий уровень гибкости и дискретности, но, в отличие от клановой, она ориентирована вовне. Адхократическая культура организации представляет собой собрание активных и творческих личностей. Для достижения целей в рамках адхократической культуры сотрудники идут на личные жертвы, принимают на себя риски. Руководители такого типа организации являются новаторами, рисковыми бизнесменами. Элементом, который объединяет коллектив и менеджмент в адхократической организационной культуре, является преданность новаторству и стремление к экспериментам. В адхократической культуре организации поощряется стремление к лидерству и инновационность, а также творчество и свобода.
Бюрократическая культура	Для нее характерна стабильность и высокий уровень контроля, а также ориентация вовнутрь. Формируется в структурированных компаниях с высокой степенью формализации внутренних взаимоотношений. Руководители в такой культуре выполняют роль координаторов и организаторов. Наиболее важным в иерархической организации является поддержание хода ее деятельности, действия в соответствии с планом. Сотрудников в такой организации объединяют формальные правила и официально установленные, документально закрепленные политики.
Рыночная культура	Доминирует в организациях, ориентированных на результат. Сотрудники организации с рыночной культурой постоянно конкурируют друг с другом, что обеспечивает здоровые взаимоотношения в коллективе, способствующие решению задач. Руководители таких компаний являются твердыми, требовательными и непоколебимыми администраторами. Сотрудники рыночной организации объединяют свои усилия для достижения общей корпоративной цели, стремятся к победе. Ценности такой организации определяются успехом на рынке и репутацией.

Взаимосвязь стиля управления на предприятии и организационной культуры находит свое отражение в типе личности руководителя. Так, известный американский ученый Э. Шейн считает, что изучение организационной культуры начинается с «поверхностного» или «символического» уровня, включающего такие видимые внешние явления, как применяемая технология и архитектура, использование пространства и времени, наблюдаемое поведение, язык, лозунги и т.п., или все то, что можно ощущать и воспринимать через известные пять чувств человека (зрение, слух, ощущение, вкус, запахи, осязание) [6]. На этом уровне вещи и явления легко обнаружить, но не всегда их можно расшифровать и понять в терминах организационной культуры.

Значение организационной культуры заключается в том, что она придает сотрудникам организационную идентичность, определяет внутригрупповое

представление о компании, стимулирует самосознание и высокую ответственность работника, выполняющего поставленные перед ним задачи.

Для создания модели эффективного управления организацией, нами было смоделировано взаимодействие стилей управления, типов личности руководителя и типов организационной культуры. За основу взята «Трехкомпонентную модель эффективного управления организацией» разработанную Оганян К.К. Рассмотрим отдельные элементы этой модели во взаимодействии (табл. 3):

1) тип личности руководителя гармоничный по А.Ф. Лазурскому, тип организационной культуры клановый по Э. Куинну и С. Камерону, стиль управления командный по Р. Блейку и Дж. Мутону;

2) тип личности руководителя страстный по Хеймансу Ле Сенна, тип организационной культуры адхократический по Э. Куинну и С. Камерону, стиль управления новаторско-аналитический по Т. Коно;

3) тип личности руководителя новатор, деятель, служитель, игрок, рационалист по Ю.М. Резнику, тип организационной культуры личностный по Г. Харрисону, стиль управления демократический по Р. Лайкерту.

Таблица 3

Трехкомпонентная модель эффективного управления организацией

Тип личности руководителя	Тип организационной культуры	Стиль управления
Гармоничный Гармоничный тип личности руководителя по А. Ф. Лазурскому характеризуется высшим уровнем психологического развития. Для «Гармоничного» руководителя важнейшими общечеловеческими идеалами являются: альтруизм, знание, красота, религия, общество, внешняя деятельность, система, власть.	Клановая Клановая культура напоминает большие семьи с общими интересами и крепкими дружескими отношениями. Сотрудники сплочены благодаря верности организации и ее традициям. Руководители обладают значительным авторитетом и нередко воспринимаются, как родители.	Команда Предполагает командное руководство. Руководитель, придерживающийся командного стиля управления, прилагает максимум усилий, как в принятии производственных вопросов, так и в решении вопросов подчиненных. Он пытается сплотить всех работников, вовлечь их в процесс принятия основных решений, направленных на достижение целей, стоящих перед организацией.

Окончание табл. 3

Данный руководитель ориентируется на реализацию интересов производства в сопровождении с высокой степенью учета интересов людей.	Организационному стилю управления, который иначе называют командным, аналогично присущи такие свойства как: высокая сплоченность коллектива, преданность делу.	Благодаря этому значительно повышается удовлетворенность подчиненных своей работой, а также достигается высокая эффективность деятельности всей организации.
Страстный «Страстный» тип личности руководителя по Хеймансу Ле Сенна – это энергичный новатор и одновременно хороший организатор. Он отражает следующие элементы менеджерского поведения: преданность фирме, разнообразие идей, множество альтернатив, способность быстрого принятия решения и обеспечения хорошей интеграции.	Адхократическая Динамичное, предпринимательское и творческое место работы, поощряется готовность к риску, личная инициатива и свобода действий со стороны сотрудников. Лидеры – новаторы. Связующая сущность – преданность экспериментированию и новаторству.	Новаторско-аналитический При новаторско-аналитическом стиле управления решения принимаются в процессе взаимодействия различных уровней управления, многие идеи генерируются в результате простого накопления информации и проекты объединяются во всеобъемлющем плане – планомерное принятие решений.
Тип личности руководителя по Ю.М. Резнику характеризуется следующим разновидностями: 1. новатор (творчески-преобразующий тип); 2. деятель (активный тип); 3. служитель (исполнение долга); 4. игрок (рыночный тип, склонный к риску и лишениям); 5. рационалист (сознательный, социально-активный тип).	Личностная культура Личностная культура – это культура обособленных индивидов, объединяющихся для достижения своих личных интересов. В основе личностной культуры лежит идея о том, что организация вторична по отношению к личности.	Демократический Демократический стиль управления по Р. Лайкерту характеризует личность руководителя, как человека, заинтересованного в участии подчиненных в деятельности организации. Работники в данной организации мотивируются посредством участия в процессе принятия решений.

После проведения анализа совместимости типов личности руководителя, стилей управления и типов организационной культуры было выявлено несколько новых типов управления организацией: семейный, инновационно-творческий и личностно-ориентированный, которые в дальнейшем могут послужить инструментом для руководителей в создании эффективного управления организацией (табл. 4).

Таблица 4

Интегральная трехкомпонентная модель эффективного управления организацией

Тип эффективного управления организацией	Компоненты модели		
	Тип личности	Стиль управления	Тип организационной культуры
Семейный тип	Гармоничный (по А. Ф. Лазурскому)	Команда	Клановая
Инновационно-творческий тип	Новатор, деятель, служитель, игрок, рационалист	Демократический	Личностная культура
Личностно-ориентированный тип	Страстный	Новаторско-аналитический	Адхократическая

Из всего вышесказанного можно сделать вывод, что не существует единственно верного стиля управления. На стили руководства оказывает влияние развитие менеджмента как науки, появление новых тенденций в мире бизнеса. Руководитель должен идти в ногу со временем и умело комбинировать различные стили управления.

Один стиль руководства может являться фоном, а остальные применяться в зависимости от ситуации. Необходимо сохранять гибкость и иметь четкое понимание того, что от способа взаимодействия с персоналом зависит степень эффективности его работы и уровень его психологической удовлетворенности.

СПИСОК ЛИТЕРАТУРЫ

1. Акофф Р. Планирование будущего корпорации: пер. с англ. / под ред. В. Т. Рысина. М.: Прогресс, 1985. С. 51.
2. Бгашев М.В. Модель формирования стиля руководителя // Бюл. науки и практики. – 2018. – Т. 4, № 5. – С. 485-494.
3. Исопескуль О. Ю. Управленческие дискурсы организационной культуры. М.: Наука, 2014. С. 179.
4. Лазурский А.Ф. Классификация личностей // Избранные труды по психологии. М.: Наука, 1997. С. 5- 266
5. Мельникова Е.В. Влияние стиля руководства на социально-экономическое развитие современной организации // Студенческий. – 2019. – № 1/3 (45). – С. 71-73.
6. Мубаракшина О.А., Марченко Н.В. Влияние организационной культуры на эффективность деятельности организации //Вестник Омского университета. Серия: Экономика.2017. № 1(57). С.108-118.
7. Оганян К. К. Междисциплинарные исследования личности в социологии: сравнительный анализ / К. К. Оганян. – М.: ИНФРА-М, 2016. – 215 с.

УДК 338.1

Е. Э. САЙФУТДИНОВА, Д. Э. ТАГИРОВА, Д. С. КАСПРАНОВА
lizasft00@mail.ru
Науч. руководит. – асс. Э. Р. ФАТТАХОВА

Уфимский государственный авиационный технический университет

ВЛИЯНИЕ ПАНДЕМИИ COVID-19 НА ПРОДОВОЛЬСТВЕННУЮ БЕЗОПАСНОСТЬ РФ

Аннотация. В статье рассматриваются последствия пандемии Covid-19 для продовольственной безопасности Российской Федерации, описываются основные проблемы, недостатки и сбои в продовольственной системе государства. Приведены меры и способы решения проблем, а также оценены масштабы негативных последствий для экономики страны.
***Ключевые слова*:** продовольственная безопасность; экономика; Covid-19.

Продовольственная безопасность – элемент национальной безопасности государства. Ситуация, при которой все люди в каждый момент времени имеют физический и экономический доступ к достаточной в количественном отношении безопасной пище, необходимой для ведения активной и здоровой жизни.

В условиях распространения коронавирусной инфекции продовольственная безопасность всего мира столкнулась с рядом серьезных угроз. В настоящее время острый кризис, связанный с продовольствием иисточниками средств к существованию, переживают 135 миллионов человек в 55 странахмира. Еще 183 миллиона человек живут в условиях отсутствия продовольственнойбезопасности на уровне, близком к критическому. У 75 миллионов детей в возрасте до пяти летнаблюдается отставание в росте, 17 миллионов детей страдают от истощения.

Число голодающих в мире начало расти еще до Covid-19. Несмотря на наличиепродовольствия в значительных объемах, сохраняется фундаментальная проблема неравенствав доступе к возможностям здорового питания. Пандемия обнажила недостаткипродовольственных систем, в самом неблагоприятном положении оказались наиболеемаргинализированные группы населения во всех странах.

Во-первых, вусловиях пандемии основная проблема заключается не в наличии продовольствия, а вдоступе к нему. Это серьезная угроза, поскольку люди, которые вынужденызарабатывать себе на жизнь, могут лишиться доходов и возможности покупать продуктыпитания.

Во-вторых, вызывали беспокойство сбои в продовольственной товаропроводящейцепочке. Некоторые страны поспешно вводили экспортные ограничения и задерживалипостановку на место стоянки судов, груженых фруктами и овощами. Потребители в паникескупали и запасали продукты.

Пандемия привела к серьезному спаду мировой экономики, а ухудшение экономического положения является одним из ключевых факторов,снижающих эффективность усилий по ликвидации голода и неполноценного питания. Снизился спрос на экспортную продукцию, и прекратилась деятельность туристическойиндустрии.

Серьезно пострадали страны с низким и средним уровнем дохода, особенно страны ссамым низким уровнем дохода, в которых количество людей, живущих в условиях голода инищеты, наиболее велико. Страны этих категорий не располагают потенциалом и средствамидля стимулирования экономики и защиты источников средств к существованию наиболееуязвимых слоев населения, поэтому им потребуется существенный объем финансирования со стороны международных кредиторов.

На фоне пандемии ситуация в странах, импортирующих продовольствие, ухудшилась, а Россия, которая в последние годы ограничивала импорт и развивала собственное производство, укрепляет позиции.Пока большинство стран страдают от разрыва цепочки импортных поставок, Россия по большинству продуктов питания закрывает потребности населения собственными силами.

Во второй половине января 2020 года в России была утверждена новая «Доктрина продовольственной безопасности». Согласно ей продовольственная независимость определяется как уровень самообеспечения в процентах, рассчитываемый как отношение объема отечественного производства сельскохозяй-

ственной продукции, сырья и продовольствия к объему их внутреннего потребления. На рисунке 1 представлен график уровня самообеспечения продуктами питания в соответствии с «Доктриной продовольственной безопасности России».

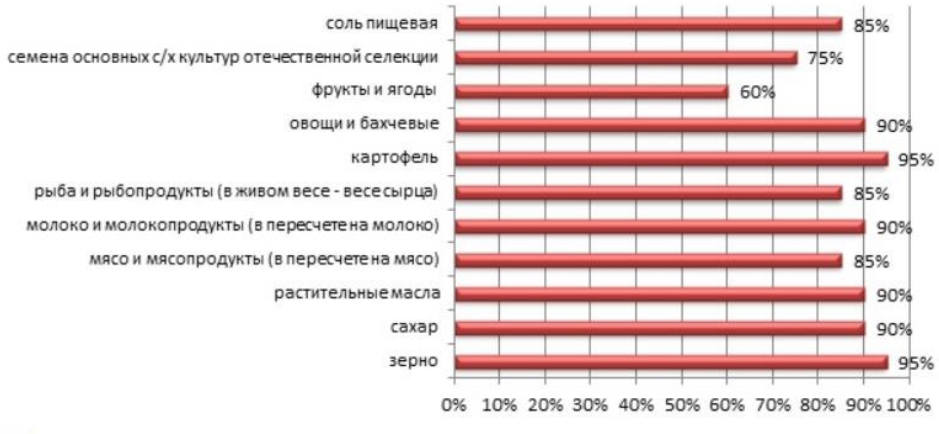


Рис. 1. Уровень самообеспечения продуктами питания в соответствии с «Доктриной продовольственной безопасности России», %

В марте российские компании уже нарастили экспорт в денежном выражении почти на треть до 2,2 млрд. долл. (к аналогичному периоду прошлого года), следует из данных ФТС. При этом в тройке лидеров - пшеница (плюс 245 млн долл.), подсолнечник (плюс 114 млн долл.), подсолнечное масло (плюс 88 млн долл.) (рис. 2).

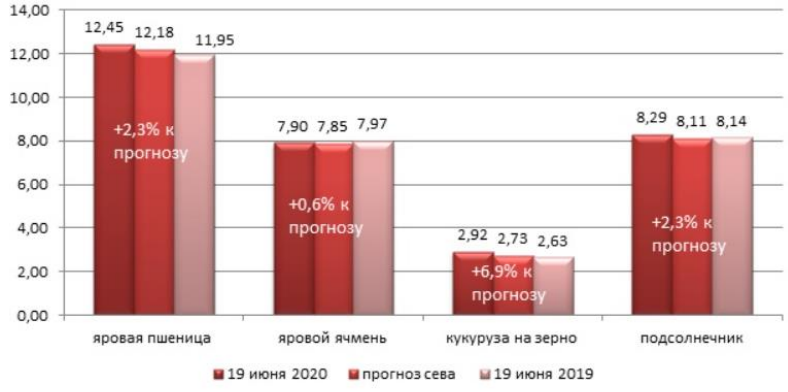


Рис. 2. Фактические и прогнозные значения посевных площадей под яровые пшеницу, ячмень, кукурузу на зерно и подсолнечник по состоянию на 19 июня 2020 года в хозяйствах всех категорий, млн. га

По большинству ключевых позиций потребности внутреннего рынка обеспечиваются либо полностью, либо почти полностью. Так, удельный вес российской продукции в общем объеме ресурсов внутреннего рынка по итогам 2019 года по зерну превышал 99%, сахару и картофелю – 95%, мясу и мясопродуктам – 90%. По многим позициям внутреннее производство продуктов питания превышает пороговые значения, указанные в Доктрине продовольственной безопасности страны, подписанное 21 января 2020 года. Например, по сахару оно составляет 90%, по зерну – 95%, мясу – 85%. При этом нужно учитывать наличие госрезерва на случай катаклизмов.

Сельское хозяйство - одна из немногих отраслей, которую пандемия не затронула напрямую. По всем направлениям АПК в России наблюдается рост. И на этот сезон также складывается благоприятный прогноз по валовому сбору зерновых, масличных культур. Увеличены посевные площади под гречиху, рис, кукурузу, овес, овощи и картофель (рис. 3).

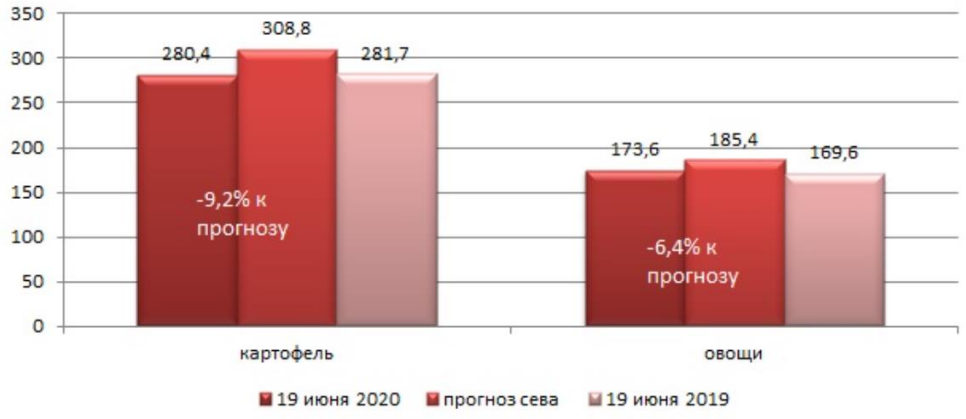


Рис. 3. Фактические и прогнозные значения посевных площадей под картофель и овощи по состоянию на 19 июня 2020 года в с/х организациях и КФХ, тыс. га

У продовольственной безопасности страны, кроме физической доступности продовольствия, есть еще две характеристики - экономическая доступность (то есть способность населения купить это продовольствие), а также безопасность и качество продовольствия. После пандемии доходы большинства населения во всем мире упали. В этой ситуации необходимо поддержать

спрос и простимулировать экономику. Самым действенным способом являются программы продовольственной помощи малоимущим и закупки для государственных нужд.

Касаемо самого российского АПК, последствия COVID-19 отрасли могут сулить большие перспективы для развития. В отдельных сегментах еще сохраняется импортозависимость– например, в производстве говядины, сырого молока, молочных продуктов, овощей. Ослабление курса рубля делает импортную продукцию менее привлекательной и, тем самым, повышает инвестиционную привлекательность проектов в этих отраслях внутри страны. Для самообеспеченности российского рынка по молоку потребуется ввести в эксплуатацию ферм общей мощностью 3 млн т сырья в год. А чтобы обеспечить Россию фруктами, нужно посадить 60 тыс. га садов интенсивного типа.

В рамках мер стимулирования экономики во всех странах активно начали удовлетворятьпотребности наиболее уязвимых слоев за счет повышения эффективности оказания чрезвычайной продовольственной помощи. Без доступа к питательным продуктам человек не может быть здоров. Вследствие массовых увольнений семьям становится трудно обеспечить себя продовольствием. Во всем мире закрываются школы, и множество детей не получает полноценного школьного питания.

Глобальные торговые каналы начали постепенно становиться открытыми. Без открытой торговли невозможно функционирование глобальных продовольственных рынков. В уязвимом положении оказываются страны, зависящие от импорта продовольствия, так как поставки замедляются, а валюта этих стран обесценивается. Можно предполагать, что в большинстве стран вырастут цены на продовольствие. Для стимулирования потребления и производства и поддержания функционирования продовольственных товаропроводящих цепочек необходимо повышать прозрачность рынков и координацию между торговыми партнерами и не допускать установления торговых ограничений.

Было решено выделять ресурсы ключевым секторам и предприятиям, в первую очередь малым и средним. Решающее значение имеет обеспечение доступа мелких фермеров к рынкам. Кроме того, чтобы продолжать производить продовольствие, они должны получать денежные субсидии и доступ к финансированию. Медперсонал на местах может следить за состоянием здоровья работников. Всем работникам выдали защитное снаряжение. Склады и перерабатывающие предприятия частично были переоборудованы так, чтобы работники могли соблюдать требования по социальному дистанцированию.

Пандемия коронавирусной инфекции заставляет обратить внимание на необходимость срочного решения существующей с давних пор проблемы неравенства. Одним из методов решения этой проблемы является расширение программ социальной защиты с предоставлением уязвимым домашним хозяйствам возможности получать денежные средства и введением моратория на налоговые и ипотечные платежи. Необходимо охватить этими программами тех, на кого они не были ориентированы ранее.

В долгосрочной перспективе целью мер стимулирования, направленных на устранение существующих угроз продовольственной безопасности, должно быть повышение устойчивости продовольственных систем к будущим пандемиям. Для этого продовольственные системы должны быть перестроены так, чтобы они в большей степени способствовали оздоровлению рациона мелких производителей, рыбаков и скотоводов и устойчивому использованию природных ресурсов, биоразнообразия и экосистемных услуг.

Таким образом, среди всех рисков и угроз обеспечения продовольственной безопасности в России в 2020 г., особо негативное влияние приобрели экономические риски, связанные с ухудшением внешней конъюнктуры экономики, а также геополитические риски, связанные с нарушением взаимоотношений с зарубежными партнерами. Следует отметить, что та концепция продовольственной безопасности России, что была подписана Президентом в начале 2020 г., может быть выполнена лишь при условии развития сельских территорий,

обеспечения производителей современной техникой, поддержки аграрной науки, расширении направлений торговли.

СПИСОК ЛИТЕРАТУРЫ

1. ФЗ «О качестве и безопасности пищевых продуктов» от 02.01.2000 №29-ФЗ (ред. от 13.05.2021)
2. Указ Президента РФ от 21.01.2020 N 20 "Об утверждении Доктрины продовольственной безопасности Российской Федерации"
3. Федеральная служба государственной статистики «Росстат» [Электронный ресурс]. Режим доступа: http://www.gks.ru/wps/wcm/connect/rosstat_main/rosstat/ru/statistics/accounts
4. Условия и основные критерии обеспечения продовольственной безопасности [Электронный ресурс] / Научный журнал КубГАУ, №92(08), 2013г. URL: http://ej.kubagro.ru/2013/08/pdf/09.pdf (дата обращения: 11.05.2021).
5. Продовольственная безопасность региона в условиях вступления России в ВТО [Электронный ресурс] / Электронный научный журнал «Международный студенческий научный вестник». URL: http://www.scienceforum.ru/2014/pdf/854.pdf (дата обращения: 11.05.2021).
6. Продовольственная безопасность и продовольственная независимость России: исторический аспект [Электронный ресурс] / КиберЛенинка. URL: http://cyberleninka.ru/article/n/prodovolstvennaya-bezopasnost-i-prodovolstvennayanezavisimost-rossii-istoricheskiy-aspekt (дата обращения: 11.05.2021).
7. Продовольственная безопасность и инвестиции в контексте вызовов современности [Электронный ресурс] / интернет-журнал «Науковедение», №4, 2014г. URL: http://naukovedenie.ru/PDF/99EVN414.pdf (дата обращения: 11.05.2021).

УДК 33.338

Е. О. САФОНОВА, А. А. САБИТОВА
lizwzz@yandex.ru, alsu_sabitova_00@mail.ru
Науч. руководит. – ст. преп. И. В. ДМИТРИЕВА

Уфимский государственный авиационный технический университет

ВЛИЯНИЕ ПАНДЕМИИ COVID-19 НА УРОВЕНЬ БЕЗРАБОТИЦЫ В РОССИИ

Аннотация. В данной статье рассматривается проблема макроэкономического характера, а именно, влияние пандемии коронавирусной инфекции на уровень безработицы в России. Для того чтобы обеспечить безопасность населения, сокращаярост числа заболевших коронавирусом, в 2020 году были приняты карантинные меры. Они негативно повлияли на все сферы общественной жизни. Российская экономика также попала под удар. Пандемия вынудила многие предприятия временно закрыться, что привело к резкому падению объемов производства. Это и стало сильнейшим потрясением для рынка труда России.
Ключевые слова: безработица; коронавирус; пандемия; рынок труда; занятость населения.

В марте 2020 года ВОЗ объявила вспышку коронавируса пандемией. Она затронула все сферы жизни, в том числе и негативно повлияла на уровень безработицы.

За время эпидемии коронавируса в России безработица выросла на 30%. Многие компании во время карантина сократили сотрудников или вовсе перестали существовать. В соответствии в предоставляемыми данными интернет-рекрутмента HeadHunter, 45% работодателей заявляли о сокращении примерно 20% состава сотрудников в компаниях на конец весны. Компании, которые полностью остановили свою деятельность, составили 7 %. Наибольшее влияние на закрытие бизнеса оказало резкое снижение покупательской способности населения, которое в последующем повлекло за собой снижение спроса [3].

Уровень безработицыв мае 2020 года достиг своего максимального значения за последние 8 лети составил 6,1%[6]. Превышение данного значения в последний раз было зафиксированов марте 2012 года. Число официально зарегистрированных безработных с марта 2012 года выросло более, чем в 4 раза. Однако к этим значениям надо отнестись с осторожностью, так как обследование рабочей силы в апреле 2020 года проводилось методом телефонного опроса респондентов. Это делает новые оценки несопоставимыми с теми, что были по-

лучены с использованием стандартных методов. К сожалению, мы не знаем, как выглядел новый инструментарий статистиков, каков был реальный охват респондентов и процент отказа от участия в опросе.

На рисунке 1. представлен график изменения уровня безработицы в России за последние 5 лет.

Рис. 1. Уровень безработицы в России за 2016-2020 гг.

На графике видно, что до 2020 года уровень безработицы постепенно снижался, но с наступлениемпандемииCOVID-19, наблюдается ее резкий рост. Во время действия карантинных мер в условиях пандемии, власти упростили процедуру получения статуса безработного, в результате чего, к концу 2020 года уровень безработных составил 5,9%. Стоит отметить, что в нашей стране уровень безработицы превышает теоретическую норму безработицы (≥4). Для того, чтобы приблизить значение безработицы к норме, необходимо разрабатывать и реализовывать мероприятия, которые будут способствовать минимизации числа незанятого населения и решению основных кризисных проблем.

По данным статистики Росстата, число безработных в стране за время коронакризиса превысило отметку в 4,5 миллиона человека и составило 4,581 миллиона человека [6].Стремительный рост числа безработного населения наблюдался на рынке труда с апреля по середину лета 2020года. Доля нерабо-

тающих возросла с 12% до 14% к июлю. На рисунке 2 представлен график изменения численности безработного населения за последние 5 лет.

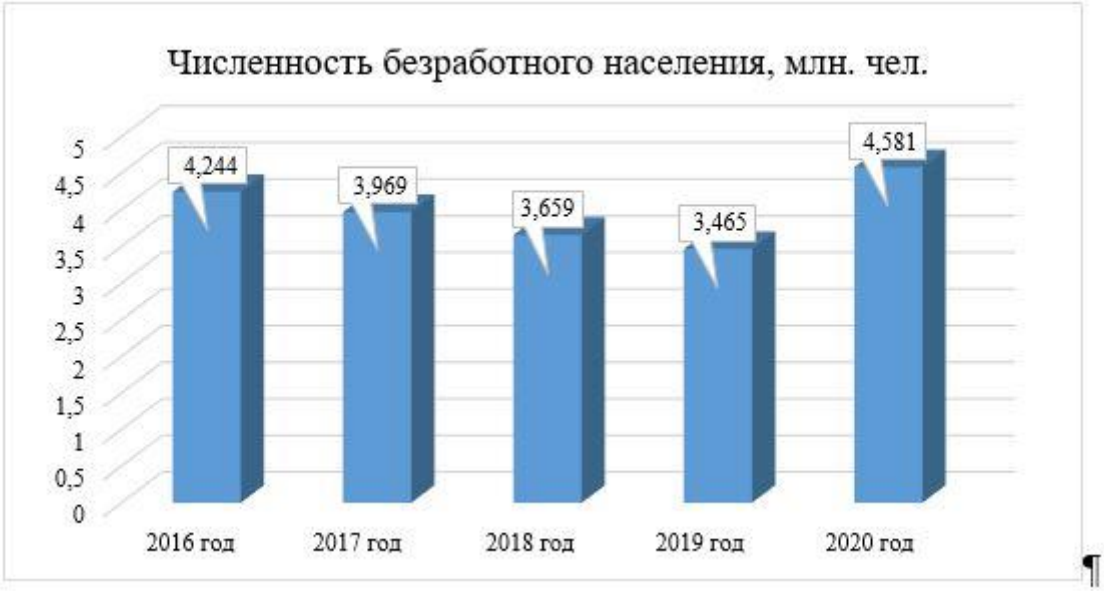


Рис. 2. Численность безработного населения в России 2016-2020 гг.

Наибольший рост численности безработного населения во время пандемии коронавируса был достигнут за счет банкротства малого и среднего бизнесов. Малый и средний предпринимательства осуществляют свою деятельность, как правило, в сферах торговли и предоставления услуг населению. В настоящий момент эти сферы имеют довольно низкую как инновационную, так и инвестиционную активности. Данное обстоятельство, а также высокая сложность процедур государственного урегулирования и высокая степень финансовой нагрузки, привели к абсолютной ликвидации предприятий, что в свою очередь лишило рабочих мест граждан и повысило уровень безработицы населения. За счет невозможности осуществления официальной деятельности, предприятия повысили показатели неформальной занятости в сфере малого и среднего бизнеса.

Наибольшее число безработных в России в первом квартале 2020 года пришлось на сферу оптовой и розничной торговли,в указанной сфере безработными числились свыше 581 тысячи человек. Среди лидирующих по этому по-

казателю отраслей оказались «обрабатывающие производства» (434 тысячи человек), «строительство» (282 тысячи), «сельское, лесное хозяйство, рыболовство и рыбоводство» (275 тысяч), а также «транспортировка и хранение» (216 тысяч). Меньше всего безработных среди сотрудников сферы водоснабжения, водоотведения, организации сбора и утилизации отходов – 24 тысячи человек.На рисунке 3. представленадиаграмма доли безработного населения по секторам экономики за 2020 год.

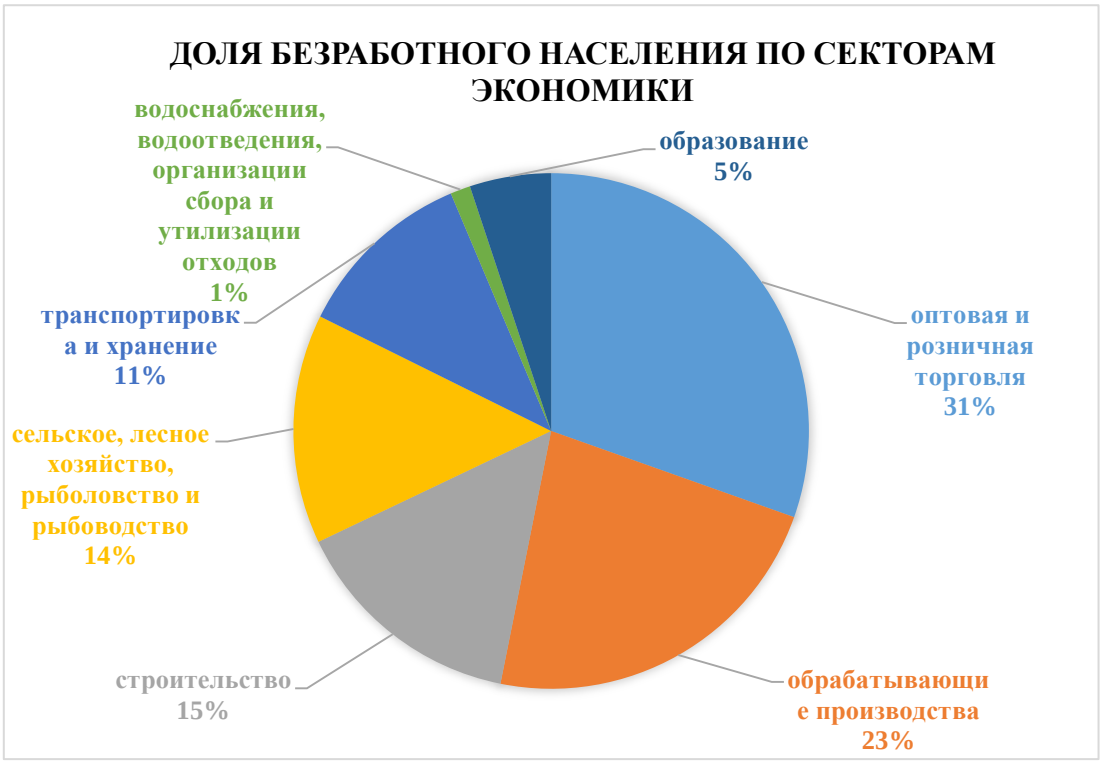


Рис. 3. Доля безработного населения по секторам экономики за 2020 год

Введение ограничительных мер оказало разрушительное влияние на жизнедеятельность производств,половина рабочих мест была подвержена увольнению, сокращению или задержке зарплаты. Таким образом, около 35 миллионов человек оказались в зоне риска.Тяжелая ситуация на рынке труда характеризовалась не только увольнениями, но и сокращением рабочего дня, а такжеотправкой сотрудников в неоплачиваемый отпуск.

Пандемия коронавируса нанесла серьезный удар по доходам населения. Исходя из опроса, проводимого экспертами компании Online Market Intelligence (OMI) и Центра социального проектирования «Платформа», был сделан вывод,

что 49% работающих россиян из-за пандемии коронавирусной инфекции отчетливо ощутили на себе падение доходов своихсемей [5]. А 46% граждан обеспокоены, что им вообще не на что будет покупать даже продукты питания.

В опросе участвовало около 1 тыс. человек. 8% опрошенных остались полностью без работы, 14% ушли в неоплачиваемые отпуска, а 13% сотрудников перевели на неполный рабочий день. По данным опроса ЦСР «Социально-экономические эффекты от «шоковых» событий начала 2020г.» выявилось, что около 33% компаний принудили своих сотрудников взять отпуск за свой счет.

На сегодняшний день одной из целей «спасения» экономики России остается снижение безработицы. Для осуществления данной цели, во время действия пандемии государство создаломеры поддержки малого и среднего бизнеса, а также меры поддержки безработного населения. В перечне мер по поддержки малого и среднего бизнеса оказалось снижение страховых взносов с 30% до 15%, реструктуризация кредитов, действующая до конца 1 квартала 2021 года, а также исключительно для малого бизнеса, – освобождение от плановых проверок.Важнейшим стал проект беспроцентного кредитования малого и среднего бизнеса, разработанныйкрупнейшими банками совместно с Правительством РФ и Центральным банком. Кредиты выдаются компаниям для уплаты заработной платы работникам. Сумма кредита исходит из общего числа сотрудников, умножается на МРОТ и на шесть.

Со стороны государства также действовали меры поддержки безработного населения. К ним относятся пособия по безработице в размере 12 130 рублей, дополнительны пособия безработным, имеющим несовершеннолетних детей, в размере 3 000 рублей на каждого ребенка, кредитные каникулы и дистанционная постановка на биржу труда.

Таким образом, чтобы компенсировать негативные последствия и эффекты пандемии COVID-19, государству необходимо регулярно принимать комплексные меры, включая налоговую, административную, банковскую и финан-

совую поддержку малых и средних предприятий.В целом к мерам по сокращению уровня безработицы относятся:

− возрождение отечественного производства, создание новых рабочих мест для населения страны во всех сферах хозяйственной деятельности;

− цифровизация сбора информации от работодателей и передача ее населению;

− устранение факторов, которые оказывают негативные влияние на мобильность рабочей силы;

− введение программ переквалификации и профессионального переобучения;

− создание условий для роста спроса на товары и услуги;

− создание программ поддержки малого бизнеса;

− улучшение программ поддержки молодых работников;

− усиление контроля за неплатежами заработной платы, повышение гарантий в сфере оплаты труда. [2]

Принятые меры помогут минимизировать убытки от пандемии не только для самих предприятий, но и для государства, для его граждан, а значит – поддержать лояльность населения и значимость страны на мировой экономической арене.Важнейшим уточнением является то, что все меры должны реализовываться комплексно, в противном случае, их применение не сможет нейтрализовать негативные последствия пандемииCOVID-19.

Подводя итог статьи, мы приходим к выводу, что деятельность государства по социальной защите населения имеет огромное значение в условиях развивающейся безработицы, а особенно в такие сложные периоды, как пандемия. В это непростое время люди как никогда нуждаются в поддержке и помощи. По нашему мнению, уровень безработицы пойдет на спад только в том случае, если меры по поддержке населения и сфер экономики будут реализовываться комплексно и единовременно. На данный момент сложно говорить об улучшении докризисного состояния уровня безработицы, так как для этого необходимо

восстановление всех процессов экономики страны в короткий промежуток времени, что является невозможным. Но достижение докризисного уровня безработицы, по нашему мнению, вполне реально при выполнении государством комплексных мер по поддержке населения, а также среднего и малого бизнеса.

СПИСОК ЛИТЕРАТУРЫ

1. Колосова Р.П., Меликьян Г.Г. Экономика труда и социальнотрудовые отношения. – М.: МГУ, 2018. – 239 с.
2. Королёв А.А. Безработица в России и методы борьбы с ней // Современные научные исследования и инновации. – 2017. – №4. – С. 295-300.
3. Паздникова Н.П., Глазкова Н.Г., Буреш Д.С. COVID-19: влияние
нового типа коронавирусной инфекции на национальную экономику. - М.: Аналитика Родис, 2020. – 181 с.
4. Селимова С.А. Проблемы рынка труда в Российской Федерации и направления их решения // Научное сообщество студентов: материалы IX Международной студенческой НПК, Чебоксары, 2016. – С. 229-233.
5. РБК [Электронный ресурс]: официальный сайт. Режим доступа: https://www.rbc.ru/ (дата обращения 12.08.2021).
6. Федеральная служба государственной статистики [Электронный ресурс]: официальный сайт. Режим доступа: https://rosstat.gov.ru/ (дата обращения 12.08.2021).

УДК 331.1

А. В. ТРИФОНОВА
aljo1588@gmail.com
Науч. руководв. – канд. пед. наук, доц. А. Ю. ФАРРАХОВА

Уфимский государственный авиационный технический университет

ВЛИЯНИЕ МОТИВАЦИИ НА СОКРАЩЕНИЕ ТЕКУЧЕСТИ ПЕРСОНАЛА

Аннотация. В статье представлен теоретический анализ понятия «мотивация» различными учеными, рассмотрены основные теории мотивации и их взаимосвязь с управлением персонала, эффективностью деятельности предприятия в целом. Актуальность данной статьи заключается в определении взаимосвязи мотивации и снижения текучести персонала. На примере компанииАО «Уфанет» представлены рекомендации по разработке системы мотивации персонала с целью предупреждения текучести кадров.
***Ключевые слова*:** мотивация; мотив; мотивационные модели; теории мотивации; мотивационный менеджмент; текучесть кадров; управление персоналом.

Мотивация играет большую роль в системе управления персоналом, является базовой функцией менеджмента. Что движет людьми, пришедшими в организацию? Какие цели они преследуют? Как побуждать работников к деятельности с пользой для себя и одновременно в интересах организации? Этими и подобными вопросами занимается мотивационный менеджмент.

Процесс мотивации базируется на потребностях человека, которые и считаются главным объектом влияния с целью побуждения человека к действию.

В современной литературе по психологии, управлению организацией, персоналом понятие «мотивация» представлено разными авторами. Некоторые из существующих определений представлены в таблице 1.

Таблица 1

Определение понятия «мотивация»

Автор	Определение
Маслоу А.	Мотивация – побуждение к действиям, направленным на последовательное удовлетворение существующих у человека потребностей, начиная с первичных.
Тейлор Ф.	Мотивация – процесс побуждения себя и других к определенной деятельности, направленной на достижение личных целей или целей организации.
Виханский О.С.	Мотивация – совокупность сил, побуждающих человека осуществлять деятельность с затратой определенных усилий, на определенном уровне страдания и добросовестности, с определенной степенью настойчивости в направлении достижения определенного результата.

Таким образом, мотивация – это совокупность внутренних и внешних движущих сил, которые побуждают человека к деятельности, задают границы и формы деятельности и придают этой деятельности направленность, ориентированную на достижение определенных целей [2].

Успешное функционирование любой организации зависит от множества внешних и внутренних факторов, которые оказывают влияние на ключевые процессы ее деятельности, поэтому менеджерам организации необходимо адаптировать свой стиль управления к меняющемуся контексту управленческой деятельности. Теории и подходы, еще сегодня казавшиеся вполне актуальными и действенными, уже завтра могут показать свою полную несостоятельность и бессилие в решении новых задач и проблем.

Мотивационные теории делятся на три вида:

1) биологические (теория XYZ, теория атрибуции);

2) содержательные (теория иерархии потребностей А. Маслоу, теория двух факторов Ф. Герцберга, теория ERG К. Альдерфера, теория приобретенных потребностей Д. Макклеланда);

3) процессуальные (теория ожиданий (В. Врум, Портер Лоулер), теория равенства С. Адамса, теория постановки целей Э. Локе, модификация поведения, теория подкрепления мотивов, теория партисипативного управления).

Отсутствие условий для реализации идей, чувства причастности к компании, возможностей для развития, изменений в статусе работника монотония и другое, может стать причиной ухода сотрудников из организации.

Текучесть кадров влияет как на внутренние факторы организации, так и на внешние, поэтому HR-менеджерам крайне важно следить за этимипоказателями, стараясь стабилизировать текучесть, снизить ее уровень. Рассмотрим понятие текучести кадров в таблице 2.

Таблица 2

Определение понятия «текучесть кадров»

Автор	Определение
Джуэлл Линд	Текучесть кадров – изменения в составе членов организации, в ходе которых одни сотрудники увольняются, а их должности занимают новые люди.
Кибанов А.Я.	1) Текучесть кадров – движение рабочей силы, обусловленное неудовлетворенностью работника рабочим местом (условиями труда, быта) и неудовлетворенностью организации данным работником (его недисциплинированностью, систематическим невыполнением обязанностей без уважительных причин). 2) Текучесть кадров – увольнение по собственному желанию, так и увольнение по инициативе администрации в связи с прогулами работников, систематическими нарушениями трудовой дисциплины.

Влияние текучести кадров на предприятие можно рассмотреть в двух аспектах – количественный и качественный.

Количественный аспект в свою очередь можно разделить на естественный и повышенный уровень текучести: естественный уровень в российской производственной сфере оптимальной считается текучесть около 10%. В активно растущем бизнесе, особенно на стадии массового найма, уровень текучести может составлять чуть более 20%.

Высокая текучесть снижает укомплектованность рабочих мест исполнителями, отвлекает от работы высококвалифицированных специалистов, которые вынуждены помогать новичкам, ухудшает морально-психологический климат в коллективе, что препятствует созданию команды [5].

Рассмотрим наглядный пример системы мотивации на основе данных компании АО «Уфанет».

Были определены характеристики групп, из которых происходит убывание персонала, а именно возраст, отдел работников (подразделение) и другое. Обеспеченность организации кадрами определяется сравнением количества рабочих по категориям (табл. 3).

Таблица 3

Анализ структуры персонала

Наименование	2016 г.	2017 г.	2018 г.	Изменения 2016-2017 гг.	Изменения 2017-2018 гг.
Руководители	114	120	128	6	8
Специалисты	705	858	938	153	80
Рабочие	612	603	588	-9	-15
Служащие	730	719	699	-11	-20
Всего	2 161	2 300	2 353	139	53

Исходя из таблицы видно, что наблюдается тенденция увеличения руководителей, специалистов и всего персонала, в то время как происходит уменьшение рабочих и служащих.

Рассмотрим структуру трудовых ресурсов предприятия по возрастному составу (табл. 4).

Таблица 4

Возрастная структура кадрового состава предприятия (в % к численности)

Возраст	2017 г.	2018 г.	2019 г.
Моложе 21 года	210	184	235
До 25 лет	336	345	282
До 30 лет	736	851	941
До 40 лет	526	598	635
До 50 лет	231	230	612
Старше 50 лет	63	92	47

Анализируя данную таблицу, можно сказать, что старшее поколение меньше заинтересовано в работе или же уходят на пенсию. Больше всего преобладает работников в возрасте от 25 до 30 лет и от 30-40 лет.

Наиболее существенным этапом в анализе обеспеченности предприятия рабочей силой – изучение ее движения и динамики, поскольку стабильность состава кадров на предприятии – предпосылка роста производительности труда и эффективности производства в целом. Для этого проведем анализ движения и постоянства кадров (табл. 5).

Таблица 5

Анализ движения персонала

Показатели	2016 г.	2017 г.	2018 г.
Списочный состав работников на начало года, чел.	2 004	2 161	2 300
Принято, чел.	437	490	535
Выбыло, чел., в т.ч. по:	280	353	482
Собственному желанию, чел	180	240	325
За нарушение трудовой дисциплины, чел.	21	18	23
Другие причины, чел.	79	96	134
Среднесписочный состав работников на конец года, чел.	2 161	2 300	2 353
Текучесть кадров, %	12,96	15,35	20,48
Коэффициент оборота персонала по приему	0,2	0,21	0,23
Коэффициент оборота персонала по выбытию	0,1	0,14	0,18

Из данной таблицы видно, что списочный состав увеличился за 2 года; за нарушение трудовой дисциплины количество уволенных относительно постоянно, что свидетельствует о том, что в данной организации хорошо работает внутренний распорядок, корпоративная этика, охрана труда и другое.

Следующий этап анализа мотивационного менеджмента в компании АО«Уфанет» – определение причин текучести кадров.

Независимо от того, на какую теорию мотивации опирается руководитель, и какие практические методы он использует, ему не следует игнорировать простые практические правила управления мотивацией:

1) положительная оценка деятельности сотрудника эффективнее и конструктивнее отрицательной;

2) неожиданные вознаграждения и поощрения мотивируют и стимулируют эффективнее ожидаемых;

3) временной разрыв между поощряемым действием сотрудника и вознаграждением должно быть минимальным;

4) вознаграждайте часто, умеренно и многих.

Разработка и реализация системы мотивации осуществляется в три этапа:

1) определение характера мотивационной среды организации;

2) построение мотивирующей системы;

3) мониторинг и коррекция системы мотивации.

Для правильного построения мотивации можно использовать карту мотиваторов, предложенную Ивановой С.В., экспертом в области HR, бизнес-тренером, кандидатом психологических наук.

Анализ карты мотиваторов сотрудника позволяет не только решить, подходит ли вам этот сотрудник, но и понять, как управлять им в процессе работы (табл. 6).

Таблица 6

Карта мотиваторов (некоторые из них)

Мотивы	Выводы
Деньги, признание, оценка, самореализация	Для человека значимо как содержание работы, так и внешнее признание. При управлении таким сотрудником нужно помнить, что ему необходимо некоторое внешнее положительное подкрепление (но не чрезмерное). Основная задача – уточнить, что именно стоит за самореализацией.
Удовлетворенность работой, деньги, результат, соответствие ожиданиям – своих и других сотрудников	Мотивация такого рода достаточно характерна для профессионала высокого класса или руководителя среднего звена. У сотрудников, занимающих низшие исполнительские должности, такая мотивация может привести к быстрому разочарованию, или нам придется затратить слишком много усилий на то, чтобы их мотивировать, т.к. совокупность факторов «удовлетворенность работой», «результат» и «соответствие ожиданиям» требует значительной работы от руководителя.
Безопасность/стабильность, карьерный рост, чувство стабильности	Стоит обратить внимание на отсутствие материального фактора. Это может объясняться тем, что сотрудник уверен в своем профессионализме и рассчитывает на довольно высокую оплату своего труда, и тем, что у него уже имеется хороший доход из других источников. Есть некоторый риск того, что материально мотивировать такого сотрудника будет довольно сложно. Поэтому рост вознаграждения следует преподносить как карьерный рост и показатель того, что компания его ценит (стабильность).

Можно сделать вывод, что в любой организации необходима разработка и внедрение системы мотивации труда персонала, для того что бы предприятие работало эффективнее и отдача от сотрудников была выше, а не несло убытки, связанные с оттоком неудовлетворенных специалистов.

В заключение необходимо отметить, что мотивационные стимулы действуют только в случае систематического применения как внешних, так и внут-

ренних мотиваторов, их взаимосвязи и учета индивидуальных особенностей и потребностей персонала.

СПИСОК ЛИТЕРАТУРЫ

1. Иванова С. В. Мотивация на 100%: А где же у него кнопка? / С.В. Иванова. — М.: Альпина Бизнес Букс, 2005 — 288 с. — (Серия «Бизнес на 100%»). [Электронный ресурс] URL: https://static.my-shop.ru/product/pdf/207/2061850.pdf.
2. Кондакова А. А. Текучесть кадров: подходы и классификация понятий // Концепт. 2017. №S1. [Электронный ресурс] URL: https://cyberleninka.ru/article/n/tekuchest-kadrov-podhody-i-klassifikatsiya-ponyatiy (дата обращения: 05.04.2021).
3. Костенко Е. П. История менеджмента: учебное пособие / Е. П. Костенко, Е. В. Михалкина; Южный федеральный университет. - Ростов-на- Дону: Издательство Южного федерального университета, 2014. 606 с.
4. Нотченко В. В., Жукова М. В. Исследование проблемы высокой текучести кадров на промышленных предприятиях // Вестник Псковского государственного университета. Серия: Экономика. Право. Управление. 2013. №2. URL: https://cyberleninka.ru/article/n/issledovanie-problemy-vysokoy-tekuchesti-kadrov-na-promyshlennyh-predpriyatiyah(дата обращения: 10.04.2021).
5. Титченко Ю.А. Влияние мотивации персонала на сокращение текучести кадров [Электронный ресурс] URL: https://nauchkor.ru/uploads/documents/5b8ed7f77966e1073081be44.pdf (дата обращения: -7.04.2021).
6. Шамратова Л. В., Лемец К. Д. Влияние мотивации персонала на сокращение текучести кадров на предприятии // Экономика и бизнес: теория и практика. 2019. №1. [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/vliyanie-motivatsii-personala-na-sokraschenie-tekuchesti-kadrov-na-predpriyatii(дата обращения: 05.04.2021).

УДК 336.77

Г. И. ФАТКУЛЛИНА
gulnaz.fatkullina.02@mail.ru
Науч. руководит. – канд. филос. наук, ст. преп. А. Р. ФАРЕСОВА

Уфимский государственный авиационный технический университет

ИПОТЕЧНАЯ ЗАКРЕДИТОВАННОСТЬ НАСЕЛЕНИЯ КАК УГРОЗА ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ

Аннотация. В данной статье рассмотрена ипотечная закредитованность населения как угроза экономической безопасности. Были проанализированы статистические данные Центрального Банка России и выяснено, что на экономическую безопасность негативно влияет не только пандемия коронавируса, но и резкое понижение процентной ставки, снижение доходов россиян, безработица и, как следствие, их ипотечная закредитованность.
Ключевые слова: экономическая безопасность; ипотечные каникулы; ипотечная закредитованность населения; процентная ставка; угроза экономической безопасности; ипотечное жилищное кредитование.

Пандемия коронавируса, низкие процентные ставки по ипотечному кредитованию, рост цен на недвижимость отрицательно отражаются на закредитованности населения и, как следствие, на экономической безопасности государства. В то же время количество задолженностей по ипотечному кредитованию непрерывно растет вместе с уровнем бедности, что сказывается на снижении уровня жизни населения и, соответственно, представляет угрозу экономической безопасности государства.

Согласно данным Центрального Банка Российской Федерации в период с 1 января 2019 по 1 июля 2019 года просроченнаязадолженность по ипотечному жилищному кредитованию составила 442 840 млн. рублей. А в 2020 и 2021 годах за тот же период простроченная задолженность по ипотеке составила 458 708 млн. руб. и 493 591 млн. рублей соответственно.

Таким образом, сумма задолженностей по ипотечному жилищному кредитованию с каждым годом возрастает [1].

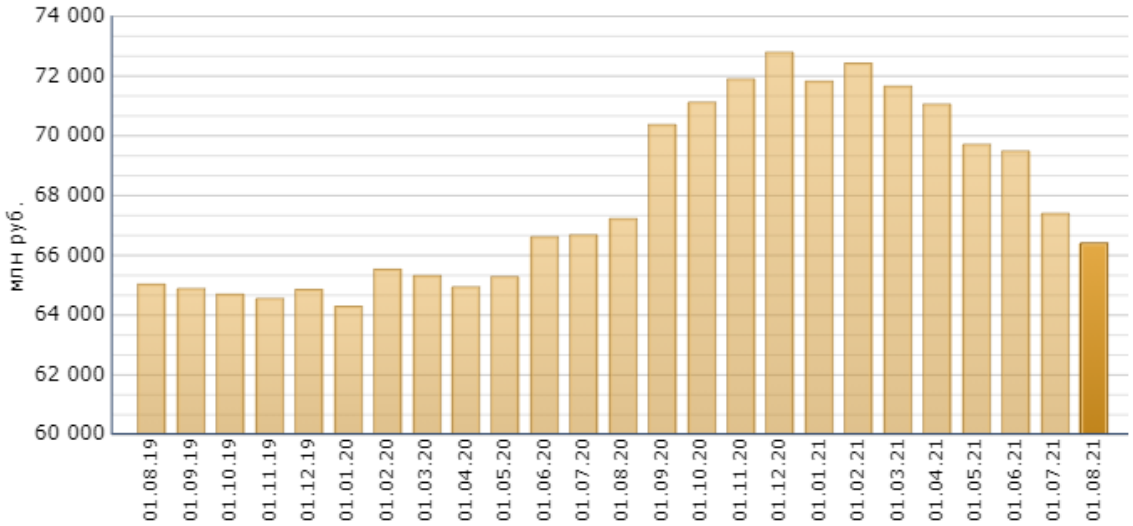


Рис. 1. Просроченная задолженность по ипотечному жилищному кредитованию

Для того чтобы избежать кризисной ситуации, государство приняло решение об утверждении Федерального закона «О праве на ипотечные каникулы», который подразумевает под собой отсрочку по ипотеке на шесть месяцев для тех граждан, кто оказался в трудной жизненной ситуации и потерял работу [2].

Стоит отметить, что в начале 2019 года процентная ставка по ипотечному кредитованию составила 9,66% и в конце первого полугодия 2019 года достигла 10,56%[1].

На новое строящееся жилье в 2020 году действовала программа с пониженной ставкойльготной ипотеки.Поэтому предел выдачи ипотечных кредитов населению был преодолен.

Так, в начале 2020 года процентная ставка снизилась и составила 9,05%, а в начале 2021 года произошло очередное снижение процентной ставки до 7,36%, в июле она уже составляла 7, 07%.

На что может повлиять понижение процентной ипотечной ставки?

Понижение процентной ставки по ипотеке, конечно же, стимулирует экономический рост. Физические лица охотнее начинают брать жилищные кредиты и, соответственно, в экономику государства поступает больше денежных средств. То есть с повышением спроса на недвижимость увеличивается не

только прибыль предприятий, но и расширяется строительство и, как следствие, появляются новые рабочие места.

С одной стороны, все это положительно отражается на экономике государства, а с другой осуществляется таргетирование экономики, с целью ее стабильности. Однако низкая процентная ставка приводит к росту цен и инфляционным процессам.

Необходимо также отметить, что низкая процентная ставка отражается и на увеличении числа закредитованных лиц. И если не будет вовремя повышена процентная ставка, то это может привести к чрезмерному расширению денежной массы за счет массового кредитования, что в свою очередь отражается на инфляции.

За последние два с половиной года было предоставлено кредитов:

– 2019год – 1,312млн. рублей;

– 2020год – 1,725млн рублей;

– полугодие 2021года – 1,148млн. рублей.

При этом за полугодие 2019 годабыло выдано 742 тысячи кредитов, за полугодие 2020 года – 806тысяч [1].

Количество выданных кредитов с каждым годом увеличивается, так как на рынке банковских услуг появляются более выгодные условия, которые становятся привлекательными для населения.

Банк устанавливает переплату по ипотеке исходя из расходов: банк платит 0,4% взносов Агентству по страхованию вкладов (АСВ) от портфеля пассивов физических лиц, также учитываются операционные расходы (аренда офиса, реклама, зарплата сотрудников, оформление и обслуживание), риск невозврата. При дальнейшем понижении процентной ставки может произойти рост государственных расходов на поддержку кредитных организаций, что также может повлечь за собой инфляцию.

Поэтому Центральный Банк России контролирует спрос, уровень развития производства и закредитованности населения, а также показатели доходов

населения, безработицы, вносит коррективы, то понижая процентную ставку, то повышая ее.

Большая разница между стоимостью жилья и доходами населения приводит к повышенным рискам невозврата денежных средств и, соответственно, к их закредитованности.

Таким образом, ужесточение требований Центрального Банка России, комплекс своевременных мер, направленных на снижение показателей закредитованности населения, а также на предотвращение инфляционных процессов в стране позволяют контролировать экономическую ситуацию в сфере ипотечного кредитования.При оформлении кредита банки должны рассчитывать коэффициент отношения ежемесячных платежей граждан по всем кредитам к их среднему ежемесячному доходу за последний год. Этот шаг позволит обеспечить стабильное социально-экономическое положение населения, обезопасить от невозврата сумм по ипотечным жилищным кредитам и предотвратить закредитованность населения как основную угрозу экономической безопасности общества.

СПИСОК ЛИТЕРАТУРЫ

1. Банк России. Показатели рынка жилищного (ипотечного жилищного) кредитования (в целом по Российской Федерации). Консультант плюс [Электронный ресурс]. URL: https://cbr.ru/statistics/bank_sector/mortgage/
2. Федеральный закон № 76–ФЗ от 01.05.2019 «О праве на ипотечные каникулы» Консультант плюс [Электронный ресурс]. URL:http://www.consultant.ru/document/cons_doc_LAW_323793/

УДК 330.354

А. А. ХАМАТЬЯРОВ, Д. Р. ХАКИМОВА, Р. Р. АКМАЛОВ
aydar.hamatyarov.00@mail.ru
Науч. руководит. – канд. экон. наук, доц. А. Н. ШЕРЫШЕВА

Уфимский государственный авиационный технический университет

ЗЕЛЕНАЯ ЭКОНОМИКА КАК ПРИОРИТЕТ РЕГИОНАЛЬНОГО РАЗВИТИЯ

Аннотация. В данной работе был рассмотрен уровень экологической безопасности регионов и РФ в целом, а также были предложены шаги для внедрения «зеленой» экономики.
Ключевые слова: зеленная экономика; устойчивый экономический рост; экологическая безопасность.

Вопросы экологической безопасности сегодня стоят на повестке дня всех государств мира. Наша страна в этом плане не является исключением, поскольку экологические проблемы угрожают как здоровью граждан России, так и ее экономике. Поэтому вопросы «зеленой» экономики стали все чаще подниматься на различных экономических форумах.

Главными чертами, которыми можно описать зеленую экономику – это низкоуглеродистая, ресурсосберегающая и социально вовлеченная экономика. В «зеленой» экономике все направлено на то, чтобы истощающиеся ресурсы использовались максимально рационально.

К перспективам зеленой экономики можно отнести уменьшение загрязнений воды, воздуха и почвы, повышение темпов роста ВВП, сокращение мировых катастроф, вызванных климатическими изменениями (парниковый эффект, озоновые дыры, глобальное потепление). Переход к экономике замкнутого цикла направлен на внедрение ресурсоэффективных и более чистых производственных систем, которые позволят компаниям повысить свою конкурентоспособность, одновременно защищая окружающую среду [1].

Сегменты рынка зеленых технологий представлены в таблице 1.

Таблица 1

Сегменты рынка «зеленый» технологий, млрд. евро [2]

Сегменты рынка «зеленых» технологий	2016 г.	2025 г.
«Циклическая» экономика	110	210
Экологическое устойчивое управление водными ресурсами	667	1001
Экологически устойчивый транспорт и мобильность	412	998
Эффективное использование сырья и материалов	521	1048
Экологически чистое производство	667	1164

Обратим внимание на данные Росстата (табл. 2): к началу 2021 г. промышленных и бытовых отходов было образовано на 37,46% больше, чем в 2015 г., тогда как утилизация и обезвреживание отходов возросли на 27,7%.

Таблица 2

Образование, утилизация и размещение отходов в РФ, млн. тонн [3]

Год	Образование отходов производства и потребления – всего	Утилизация и обезвреживание отходов производства и потребления	Размещение отходов производства и потребления на объектах, принадлежащих предприятию - всего
2015	5060,2	2685,1	2333,1
2016	5441,3	3243,7	2620,8
2017	6220,6	3264,6	3204,5
2018	7266,1	3818,4	3575,4
2019	7750,9	3881,9	3800,8
2020	6955,7	3429,0	3706,4

Порядка 90% отходов приходится на долю различных производств, в основном добывающих (рис. 1).

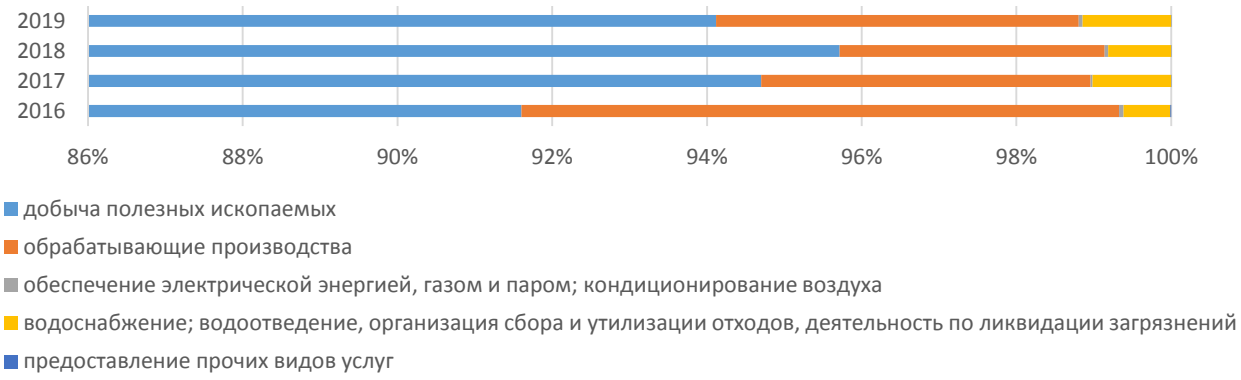


Рис. 1. Утилизация и обезвреживание отходов по видам экономической деятельности по Российской Федерации

В отрасли добычи полезных ископаемых максимальную долю дает производство угля (77,4% за 2019 г.), при том, что в мире идет отказ от углеводородов и переход на альтернативные источники энергоресурсов.

Рассмотренные статистические данные отражают ситуацию в целом по стране. Далее перейдем к анализу статистических данных по Приволжскому ФО, в котором наблюдается неоднородный, но в большей степени негативный характер образования отходов производства.

Таблица 3

Индекс промышленного производства в 2020 году [4]

	Индекс промышленного производства, агрегированный по видам деятельности	Водоснабжение; водоотведение, организация сбора и утилизации отходов, деятельность по ликвидации загрязнений
Российская Федерация	97,1	96,2
Приволжский федеральный округ	96,6	100,6
Республика Башкортостан	98,0	112,3
Республика Марий Эл	93,6	117,7
Республика Мордовия	102,4	71,8
Республика Татарстан	96,4	98,4
Удмуртская Республика	92,7	127,1
Чувашская Республика	97,6	87,0
Пермский край	97,0	106,4
Кировская область	100,1	104,1
Нижегородская область	93,4	99,9
Оренбургская область	96,0	124,3
Пензенская область	107,3	112,8
Самарская область	95,5	81,4
Саратовская область	102,8	109,3
Ульяновская область	96,9	105,4

В Приволжском ФО общий объем отходов увеличился на 55,6% в 2017 году относительно 2010 года.

Если рассмотреть индекс производства в 2020 году, который охарактеризовался общим снижением производства в связи с эпидемией, то можно увидеть, что на фоне падения индекса промышленного производства агрегированный по совокупности всех видов деятельности на 2%, наблюдается рост водоснабжения; водоотведения, организации сбора и утилизации отходов, деятельности по ликвидации загрязнений на 12,3%.

Инвестиции в основной капитал, направленные на охрану окружающей среды и рациональное использование природных ресурсов в 2020 г. составили 195962 миллиона рублей, за последние 6 лет увеличение финансирования составило 29,1 %. В республике Башкортостан на государственную программу «Экология и природные ресурсы РБ» 575 145,3 тыс. руб. на 2021 год, из них на региональный проект «Комплексная система обращения с твердыми коммунальными отходами» выделяется 1 196,4 тыс. руб.

Целью проекта «Комплексная система обращения с твердыми коммунальными отходами» является комплекс мероприятий, которые направленны на создание объектов по обработке и утилизации отходов в целях снижения негативного воздействия на окружающую среду путем снижения объема захоранираемых отходов. В качестве основных результатов федерального проекта на 2021 год (справочно из паспорта федерального проекта) можно выделить введение в промышленную эксплуатацию мощности по обращению с ТКО, в том числе: по обработке (сортировке), нарастающим итогом – 46,55 млн. руб., по утилизации и переработке ТКО, нарастающим итогом и внебюджетные источники – 13,81 млн. руб.

Таким образом анализ данных показывает, что объемы государственного финансирования не достаточны для решения проблем и не позволят перейти к модели «зеленой» экономики. Основным источником финансирования перехода к «зеленой» экономике должны ресурсы бизнеса, и задачей государства должно быть регулирование, когда при помощи специальных инструментов бизнесу создаются благоприятные условия для внедрения и развития «зеленых» технологий. Цель подобных действий – изменить направление движения капитала, который будет перенаправлен из экономических секторов, негативно влияющих на окружающую среду, в секторы, обеспечивающие на национальном уровне более устойчивое производство и потребление.

Основные причины, сдерживающие развитие «зеленых» технологий, вытекающие из сырьевой модель национальной экономики:

– значительный уровень износа основных производственных фондов, влекущий за собой риск техногенных аварий;

– низкая доля (менее 5%) инвестиций природоохранного значения;

– возрастающее количество выбросов от стационарных источников, в связи с низким уровнем диверсификации региональной экономики;

– недостаточный объем государственного финансирования природоохранных мероприятий [5].

В любом случае необходимо внедрять «зеленую» экономику, поскольку это инновация, которая позволит достичь больших преимуществ в части производства, экономии как следствие экономической безопасности. А для этого необходимы определенные действия:

– сокращение государственных инвестиций и увеличение налоговых тарифов для экологически вредных отраслей промышленности;

– увеличение инвестирования в отрасли «зеленой» экономики: сельское хозяйство, переработка вторсырья, возобновляемые источники энергии;

– постепенное внедрение эффективных технологии в «коричневую» экономику, введение новых природоохранные законы.

В итоге можно сделать вывод: несмотря на то, что как отдельного документа «Стратегии финансирования устойчивого развития и “зеленой” экономики» не существует, целый ряд документов содержит ее элементы, которые, если собрать их воедино, формируют неполную по охвату секторов экономики и территории страны, но фрагментарную стратегию финансирования устойчивого развития, что позволит повысить уровень экологической и экономической безопасности регионов и РФ в целом.

СПИСОК ЛИТЕРАТУРЫ

1. Боркова Е.А., Изусова М.Р., Гематдинова К.А. «Зеленые» инвестиции как фактор устойчивого развития экономики стран мира // Креативная экономика. – 2019. – Том 13. – № 12. – С. 2315-2326. doi: 10.18334/ce.13.12.41522.
2. Сегменты рынка «зеленый» технологий. URL: https://renen.ru/the-global-market-of-green-technologies-will-grow-to-eur-5-9-trillion-by-2025/ (дата обращения 19.07.2021).
3. Обращение с отходами производства и потребления. Минприроды России. URL: http://mnr.gov.ru/upload/medialibrary/259-330.pdf (дата обращения: 20.07.2021).
4. Индексы промышленного производства по субъектам Российской Федерации, Росстат. URL: https://rosstat.gov.ru/storage/mediabank/XsVlesp0/ind-sub_okved2.xls (дата обращения: 24.07.2021).
5. Паспорт Национального проекта «Экология». Минприроды России. URL: https://www.mnr.gov.ru/upload/medialibrary/ba5/NP_Ekologiya.pdf (дата обращения: 27.07.2021).