УФИМСКИЙ УНИВЕРСИТЕТ

приоритет2030^
лидерами становятся

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ ОБЕСПЕЧЕНИЯ КОМПЛЕКСНОЙ БЕЗОПАСНОСТИ В ЦИФРОВОМ ОБЩЕСТВЕ

Сборник материалов
VII Всероссийской молодежной научно-практической конференции с международным участием
(г. Уфа, 24 – 25 мая 2024 г.)

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ
УФИМСКИЙ УНИВЕРСИТЕТ НАУКИ И ТЕХНОЛОГИЙ

ИНСТИТУТ ИНФОРМАТИКИ, МАТЕМАТИКИ
И РОБОТОТЕХНИКИ

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ ОБЕСПЕЧЕНИЯ КОМПЛЕКСНОЙ БЕЗОПАСНОСТИ В ЦИФРОВОМ ОБЩЕСТВЕ

Сборник материалов
VII Всероссийской молодежной научно-практической конференции с международным участием
(г. Уфа, 24 – 25 мая 2024 г.)

Научное электронное издание сетевого доступа

Уфа
РИЦ УУНиТ
2024

УДК 004.9
ББК 32.973-0812
И74

Печатается по решению кафедры управления информационной безопасностью УУНиТ.
Протокол № 10 от 08.05.2024 г.

И74 **Информационные технологии обеспечения комплексной безопасности в цифровом обществе:** сборник материалов VII Всероссийской молодежной научно-практической конференции с международным участием (г. Уфа, 24 – 25 мая 2024 г.) / отв. ред. Д.С. Юнусова. [Электронный ресурс] / Уфимск. ун-т науки и технологий. – Уфа: РИЦ УУНиТ, 2024. – 314 с. – URL: https://uust.ru/digital-publications/2024/131.pdf – Загл. с титула экрана.
ISBN 978-5-7477-5932-9

В сборнике материалов представлены статьи, подготовленные в рамках основных направлений работы конференции: математические модели и методы защиты, преобразования и передачи информации; организационно-правовые аспекты защиты информации; концепция и методы инженерно-технического обеспечения безопасности; обеспечение безопасности и развития детей в информационном пространстве; цифровая экономика: вызовы, угрозы, перспективы; обеспечение национальной безопасности в условиях информационных войн.

Сборник представляет интерес для преподавателей, аспирантов, студентов и всех, кто интересуется актуальными исследованиями в сфере проблем информационной безопасности современного общества.

УДК 004.9
ББК 32.973-0812

ISBN 978-5-7477-5932-9

СОДЕРЖАНИЕ

ПЛЕНАРНЫЕ ДОКЛАДЫ И ВЫСТУПЛЕНИЯ ЭКСПЕРТОВ

Байрушин Ф.Т. Открытая информация в России и иностранные разведывательные спецслужбы 10

Белова Е.П. Анализ данных с использованием доверенных платформ искусственного интеллекта 14

Валеев С.С., Султанов Р.Р., Макаримов Т.И. Применение принципа нулевого доверия в автоматизированных системах управления технологическими процессами предприятия 21

Вульфин А.М., Кириллова А.Д. Автоматизация моделирования сценариев реализации атак информационной безопасности 25

Кушубакова Б.К. Информационная безопасность хозяйствующих субъектов в условиях обязательной публичности отчетности об их деятельности 28

Лушников Н.Д. Извлечение биометрических характеристик при распознавании пользователей компьютерной информационной системы по голосу и по изображению лица 33

Марцинкевич В.А., Романюк М.В., Марков А.Н. Импортозамещение сетевого оборудования и программного обеспечения в разрезе информационной безопасности внутренней инфраструктуры организации 38

Миронова Н.Г. Распознавание фейковости изображений и нейросетевого контента 42

Салов И.В. Переход на российские операционные системы 46

Фатхелисламов А.Ф. Беспроводная сеть как уязвимое место в периметре защиты 52

Яппаров Р.М. К вопросу о безопасности объектов критической информационной инфраструктуры 55

СЕКЦИЯ 1. МАТЕМАТИЧЕСКИЕ МОДЕЛИ И МЕТОДЫ ЗАЩИТЫ, ПРЕОБРАЗОВАНИЯ И ПЕРЕДАЧИ ИНФОРМАЦИИ

Бильданов С.З. Анализ стеганографических инструментов для соревнований формата CTF и используемых в них методов сокрытия информации 59

Вахитова Э.М. Средства проведения MITM-атаки на уровне операционной системы 62

Волков Н.А. Использование сверточных нейронных сетей для оценки защищенности речевой акустической информации 64

Габитов А.Э. Сравнительный обзор методов защиты гетерогенной среды 69

Гаврилова А.А. Генерация пакетов трафика для моделирования сетевых атак 72

Гулякин Н.В., Денисов И.Ю. Корпоративный мессенджер с применением криптографического метода шифрования 75

Гумерова А.И., Назарова А.Д. Тестирование сайтов на фишинг методом нейросетевого анализа 77

Давлетшин Б.М., Клыгин В.О. Определение фишинговых веб-страниц с помощью машинного обучения 81

Коробко Т.П. Запрещенный текстовый контент в сети Интернет и его выявление при помощи искусственного интеллекта 84

Кунавина О.А., Забара К.С. Технология перехвата и анализа трафика в беспроводных сетях 87

Лычагин Е.А. Разработка приложения устойчивого к перехвату 90

Молчанов Д.И. Обзор подходов к обеспечению информационной безопасности с использованием методов квантовой криптографии 93

Назаров М.В., Акмырадов Д.М., Насибуллин Р.М. Анализ различных типов подключений на безопасность с помощью программы Wireshark 96

Султанов Д.Ж. Использование нейросетей для распознавания фишинговых URL 99

Файзуллина А.С. Угрозы открытых сетей беспроводной передачи данных 103

СЕКЦИЯ 2. СОВРЕМЕННЫЕ ВЫЗОВЫ В ОБЛАСТИ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

Абрамов К.И., Сафронова А.В., Щанькин К.Д. Квантовые компьютеры и будущее криптографии: вызовы и возможности 107

Азнабаев Ю.С. Анализ инструментов моделирования угроз безопасности информации 111

Асанбаева А.С., Ахметов У.Р. Применение искусственного интеллекта с целью повышения безопасности в образовательных учреждениях . 114

Асанов Р.Ш. Уязвимости НС-моделей и атаки на НС-системы 118

Ахмадуллин И.И. Защита персональных данных в эпоху нейронных сетей 121

Ахмедьянов Д.М. Использование искусственного интеллекта в обеспечении информационной безопасности: возможности вызовы и перспективы 124

Ворсина А.С. Проблемы безопасности использования файлов cookies……..... 127

Галеев Р.Т. Модель машинного обучения в облачных технологиях .. 130

Галяува М.И. Защита данных пользователя в мессенджерах 133

Гвоздева Е.И. Информационная безопасность при организации удаленной работы 136

Давлетова Д.Р. Акутальные проблемы обеспечения безопасности критической информационной инфраструктуры в современных условиях 139

Ерушев Б.А. Анализ атак на облачные сервисы 143

Зайнуллин Б.И. Проблемы информационной безопасности при решении задачи миграции ИС организации на отечественные платформы 146

Зарипова А.И. Специфика создания специализированной организации для хранения конфиденциальных документов и носителей, конфиденциальной информации 149

Зыков А.И. Кибертерроризм как угроза основам конституционного строя российской федерации 153

Карлышева К.О., Корноухова Т.В. Методы искусственного интеллекта для корреляции событий информационной безопасности..... 156

Летяев В.А., Рожков М.А., Бухнер А.А. Эволюционирующая угроза вредоносного программного обеспечения: от вирусов до автономного кибероружия 160

Масальский Н.В. Обеспечение защиты персональных данных с использованием технологий искусственного интеллекта: актуальные проблемы 163

Махмутов А.Р. Моделирование сети промышленного интернета вещей с помощью технологий виртуализации 167

Набиев Д.Т. Сетевая безопасность: эволюция кибератак 170

Неттов А.С. Современные проблемы в области кибербезопасности..173

Полышева А.К. Анализ современных технических каналов утечки информации 176

Сабиров Б.Ф. Совершенствование систем защиты информации в сфере недвижимости 180

Садыкова А.В. Применение биометрических данных для идентификации сотрудников 183

Сальникова А.А. Интегрированный цикл управления информационной документацией: от хранения до переработки 187

Сахибгареев И.Р. Система управления ловушками и приманками 190

Сержанин М.Е. Анализ потенциально-опасного контента в «Telegram» 194

Тазетдинов Д.И. Безопасность в облаке: современные вызовы и стратегии защиты данных 198

Фарвазов Т.У. Обеспечение безопасности биометрических персональных даных 201

Хаерова Э.И., Гатауллин Б.И. Виртуальный тренажёр по обработке конфиденциальной информации на физических носителях 204

Хаматнуров Н.А. Анализ обеспечения информационной безопасности мобильных устройств 208

Цагалов А.Р. Проблемы безопасности технологий NFC 211

Чахалян К.Ш., Ихсанова А.А. Влияние развития искусственного интеллекта на информационную безопасность 215

Шамсутдинов Б.С. Методы защиты информации от нежелательных почтовых рассылок, спам-звонков и сообщений 218

Шарипова Э.Ф. Муниципальные информационные системы и вопросы защиты информации 222

СЕКЦИЯ 3. ОРГАНИЗАЦИОННО-ПРАВОВЫЕ АСПЕКТЫ ЗАЩИТЫ ИНФОРМАЦИИ

Антипова В.М. Содержание информации о деятельности организаций, составляющих коммерческую тайну и способы обеспечения её защиты……226

Ахмадиева Вилена Ф., Ахмадиева Виола Ф. Ответственность за распространение персональных данных, содержащихся в базах поисковых ботов и способы скрытия личной информации 230

Ахмадиева Вилена Ф., Ахмадиева Виола Ф. Лицензирование деятельности по технической защите конфиденциальной информации……...233

Зыков А.И. Анализ правовых норм России и зарубежных стран в области защиты персональных данных 236

Клияненко Д.А. Укрепление защиты информации в законодательстве Российской Федерации в эпоху цифровизации общества 240

Нуриев Р.С., Садыкова А.В. Проблемы моделирования угроз информационной безопасности 242

Поляков Е.В., Ивлева Т.Д. Внутренний контроль за обеспечением информационной безопасности организаций 246

Сагилова Э.К. О выявлении критических процессов у организаций, являющихся субъектами КИИ 249

Фаизов А.А. Персональные данные как категория сведений конфиденциального характера 253

Хаматова Г.Ф. О защите IT-инфраструктуры учреждений здравоохранения 255

Хусаинова А.Р. Разработка методов и форм работы с персоналом организации, допущенным к конфиденциальной информации 258

СЕКЦИЯ 4. КОНЦЕПЦИЯ И МЕТОДЫ ИНЖЕНЕРНО-ТЕХНИЧЕСКОГО ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Дмитриева Д.Д. Передача и защита данных в информационных системах 261

Кашапов Т.И., Хаертдинов А.Х. Разработка программного обеспечения по обнаружению угроз SQL инъекций в исходном коде 264

Макаримов Т.И. Организация защищенного обмена данными в автоматизированных системах управления 267

Насертдинова А.Н. Защита электронного документооборота в организации 270

Султанов Р.Р. Применение принципа нулевого доверия на примере учебных заведений 273

Федосеев Н.А. Обзор решений аппаратных криптошлюзов для построения защищенных корпоративных сетей 276

Хорольская Е.Д. Пост-клик оптимизация в обеспечении безопасности посещений веб-страниц 280

СЕКЦИЯ 5. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ И РАЗВИТИЯ ДЕТЕЙ В ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ

Вагабов И.М., Моисеева К.А. Основные угрозы информационной безопасности для детей при использовании государственных сервисов 284

Стенькина Р.В. Защита детей в цифровом пространстве 287

СЕКЦИЯ 6. ОБЕСПЕЧЕНИЕ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ ИНФОРМАЦИОННЫХ ВОЙН

Гаврилов Д.Ю. Искусственное занижение категории значимости объектов критической информационной инфраструктуры – угроза информационной безопасности страны 291

Кириллов В.С. О стратегиях противодействия РФ информационной войне 294

Лисина Т.Е. Реализация мандатного разграничения доступа в корпоративной сети на базе защищенной операционной системы Astra Linux Special Edition 298

Нигматуллин М.А. Импортозамещение в сфере информационной безопасности: современное состояние и перспективы 302

Козорез Д.А., Смирнов И.А. Суверенитет платежной системы на основе цифрового рубля и его значение в обеспечение национальной безопасности России 305

Хайруллина Г.Ф. Некоторые актуальные направления противодействия войнам в информационной сфере 309

Якупова И.Р. О системности борьбы с информационными войнами.. 311

ПЛЕНАРНЫЕ ДОКЛАДЫ И ВЫСТУПЛЕНИЯ ЭКСПЕРТОВ

УДК 004

Ф.Т. Байрушин
Уфимский университет
науки и технологий, Уфа, Россия

ОТКРЫТАЯ ИНФОРМАЦИЯ В РОССИИ И ИНОСТРАННЫЕ РАЗВЕДЫВАТЕЛЬНЫЕ СПЕЦСУЖБЫ
OPEN INFORMATION IN RUSSIA AND FOREIGN INTELLIGENCE SPECIAL SERVICES

Аннотация: В данной статье рассмотрены вопросы сбора и использования открытой информации иностранными спецслужбами, которая после аналитической обработки превращается в разведывательную. Описано явление сбора открытой информации из периодических и прочих научных изданий представителями иностранных дипмиссий, которая после проведения аналитическими отделами определенных манипуляций превращалась в разведывательную. Рассмотрены примеры работы аналитических отделов иностранных разведок, в результате которой вырабатывался образ военного потенциала СССР.

Abstract: This article discusses the collection and use of open information by foreign intelligence agencies, which, after analytical processing, turns into intelligence. The phenomenon of collecting open information from periodicals and other scientific publications by representatives of foreign diplomatic missions, which, after certain manipulations by analytical departments, turned into intelligence, is described. Examples of the work of analytical departments of foreign intelligence services, as a result of which an image of the military potential of the USSR was developed, are considered.

Ключевые слова: Открытая информация, информационный ресурс, спецслужбы, секретная информация, журналист, аналитический отдел, журналистское интервью.

Keywords: Open information, information resource, special services, classified information, journalist, analytical department, journalistic interview.

Часто информационный контент, на первый взгляд не несущий секретной информации и публикуемый в печатных изданиях, таких как газеты, журналы научных изданиях, описывающих различные новшества в области технологий, изобретений, научных разработок и других новинок в различных областях хозяйственной деятельности, транслируемый по телевизионным каналам в сводках

новостей, научных передачах, журналистских интервью и обзорах, где показываются новаторские решения наших военных в зоне соприкосновения, разработчиков средств индикации и поражения технических средств, используемых неприятелем, является ценным информационным ресурсом для разведки противника, которая в результате анализа и выработки контрмер сводит на «нет» полученные преимущества над противоположной стороной.

Так на недавнем процессе по шпионажу, обвиняемый в сотрудничестве с иностранной разведкой не признал своей вины, заявив, что передавал сведения, собранные из открытых источников, и что, таким образом, любого гражданина, использующего эти источники, можно обвинить в сборе информации и шпионаже.

Обратимся к событиям прошлого века, именно к началу 60-х годов, когда Советский Союз находился в зените научно - технического развития. Так был отмечен нездоровый интерес представителей дипломатического корпуса США, а также представителей таких стран, как Япония и ФРГ, к научным и научно-популярным изданиям таких издательств как: «Наука», «Мысль», «Связь», «Машиностроение», «Атомиздат» и так далее, которые активно скупались в таких специализированных магазинах, как «Академкнига», «Техническая литература». Не трудно было догадаться, что в подобного рода книгах содержалась информация в свободном доступе о изобретениях, научных исследованиях и разработках в различных областях науки, например физики элементарных частиц, аэро- и гидродинамики, химии и физики полупроводников и микроэлектроники.

Японцы буквально перелопачивали в библиотеках связки периодически издаваемых научных и научно популярных журналов: «Природа», «Радио», «Техника молодёжи», «Юный техник», (где была даже рублика: «Патенты не выдавать»), Квант», «Моделист конструктор», где публиковались всевозможные разработки наших умельцев с сопутствующими подробными чертежами мини-автомобилей, аэросаней, станков, летательных аппаратов - автожиров с расчётами, журнал «Рационализатор и изобретатель», который несомненно являлся «кладезью» идей и всевозможных разработок. К этому можно добавить, что, несмотря на отсутствие мирного договора между Японией и СССР, в 60-х годах началось активное сотрудничество в области научных изысканий, где в результате обмена научной информацией началось вынужденное вливание научных достижений в науку Японии, особенно этому способствовало подписание в 1956 году декларации о научном сотрудничестве. Всё это, несомненно, сыграло положительную роль в преодолении Японией послевоенного промышленного и, соответственно, экономического кризиса, сэкономив колоссальное количество средств, минуя разработки и научные исследования, занимаясь только доработкой

украденного. А сколько за этот период выиграла Америка, сэкономив на разработках и исследованиях в различных стратегических областях, можно только догадываться.

Рисунок 1 – Та самая злосчастная фотография пульта Свердловского центрального диспетчерского пункта Уральской электроэнергетической системы, опубликованная в журнале «Огонёк»

Так, в 1958 году всего лишь на первый взгляд по «безобидной» фотографии главного пульта управления подачей электроэнергии в уральском регионе, напечатанной в одной из статей журнала «Огонёк», в результате тщательного анализа информации, изображённой на этом фото (рисунок 1), о распределяемой электроэнергии и потребляемых мощностях предприятиях, работающих по ядерной программе, было выявлено количество произведенных на этих предприятиях атомных боеприпасов. Этому способствовал один момент – оказалось, что в энергетике США используются идентичные пульты управления, что значительно облегчило работу аналитического отдела американской разведки.

Конечно, этому способствовали и другие формы разведки, такие как запуск воздушных шаров с фотографическим оборудованием в обозначенную сторону, пролёты над уральским регионом разведовательных, высотных самолётов U-2, наземная разведка с посещением определённых мест сотрудниками ЦРУ, но всё же основной задел этого процесса был произведён на основе информации, выложенной на фотографии из журнала «Огонек».

Вернёмся в наше непростое время. Ещё до начала СВО на телевидении в качестве рекламного ролика демонстрировали, и достаточно подробно, устройства, касающиеся военной техники, а именно макеты высокого давления подвижных средств вооружения, вплоть до средств стратегического удара, изготовленные с потрясающей точностью одной из

российских фирм, которые могли использоваться в перспективе, как отвлекающие ложные цели для артиллерии и авиации неприятеля. По понятиям информационной безопасности такое, уж если не засекречено, то должно быть запрещено на предмет демонстрации на ТВ.

Периодически производится видеодемонстрация средств РЭБ, «ружей» по борьбе с беспилотниками с сопутствующими пояснениями работы данных видов вооружения. А ведь давно известно, что по виду только внешнего корпуса прибора даже среднего уровня инженер-электронщик без особого труда воссоздаст внутреннее «убранство» этого средства! Даже во время написания этой статьи по телевидению во время своего интервью эвакуируемый, получивший ранение в ногу журналист, скользнул видеокамерой по кнопочной панели управления, расположенной на «ружье» РЭБ с беспилотниками, находящегося в руках рядом сидящего участника СВО. Такие явления в репортёрской практике в условиях боевых действий однозначно преступны! Даже показ индикаторов электромагнитного поля по СМИ, что наблюдается неоднократно по телевидению, оповещающих российских солдат о нахождении по близости БПЛА, недопустимо. Показ всевозможных приспособлений и устройств, обеспечивающих дополнительную защиту подвижного парка бронетехники, транспортных средств, средств артиллерии - как подвижной, так и стационарной, должно быть под строжайшим запретом, чтобы не оснащать оперативным материалом военных аналитиков НАТО, способствующим определению уязвимых точек для удара беспилотников. Достаточно вспомнить обучающие фильмы для советских летчиков, где демонстрировались уязвимые места и методы уничтожения самолётов «LUFTWAFFE».

Исходя из вышесказанного, возникает необходимость создании свода нормативных документов СМИ, определяющих правила ведения репортажей, касающихся боевых средств вооружения, с целью предотвращения утечки информации, входящей в зону интересов иностранных разведок.

Список использованных источников:

1. Куприянов А.И. Радиоэлектронная борьба / А.И. Куприянов. – Москва: «Вузовская книга», 2013, 182 с.

2. Байрушин, Ф.Т. Информационная безопасность как фактор обеспечения социальной стабильности в российском обществе / Ф.Т. Байрушин, И.В. Салов, И.Р. Абрамов // Евразийский юридический журнал. № 8(183). 2023. С.427-429.

3. Байрушин, Ф.Т. Информационная безопасность в современном многополярном укладе общественного устройства / Ф.Т. Байрушин, И.В. Салов, И.Р. Абрамов // Евразийский юридический журнал. № 8(183). 2023. С. 416-417.

4. Золотая пора научно-популярной публицистики – URL: https://habr.com/ru/companies/vk/articles/380375/ (Дата обращения: 15.04.2024)

УДК 004

Е.П. Белова
Уфимский университет
науки и технологий, Уфа, Россия

АНАЛИЗ ДАННЫХ С ИСПОЛЬЗОВАНИЕМ ДОВЕРЕННЫХ ПЛАТФОРМ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА
DATA ANALYSIS USING TRUSTED ARTIFICIAL INTELLIGENCE PLATFORMS

Аннотация: В данной статье говорится об анализе данных, акцент делается на анализе больших данных. Приводятся этапы анализа данных и работы с большими данными. Даётся определение доверенных платформ и доверенных платформ искусственного интеллекта. Предлагаются примеры доверенных платформ и доверенных платформ искусственного интеллекта. Рассматриваются проблемы, с которыми сталкиваются платформы искусственного интеллекта.

Abstract: This article talks about data analysis, with an emphasis on big data analysis. The stages of data analysis and working with big data are given. A definition of trusted platforms and trusted artificial intelligence platforms is given. Examples of trusted platforms and trusted artificial intelligence platforms are provided. The problems faced by artificial intelligence platforms are considered.

Ключевые слова: Анализ данных, большие данные, доверенные платформы, доверительные вычисления, доверенные платформы искусственного интеллекта, искусственный интеллект, проблемы систем искусственного интеллекта.

Keywords: Data analysis, big data, trusted platforms, trusted computing, trusted artificial intelligence platforms, artificial intelligence, problems of artificial intelligence systems.

Анализ данных — это процесс переработки исходных данных в требуемую информацию.

Согласно [1] анализ данных состоит из следующих этапов:

1. сбора;
2. классификации;
3. фильтрации;

4. интерпретации.

Например, для того, чтобы метеоцентру осуществить прогнозирование погодных условий, необходимо получить данные за определённый временной период и измерить текущие показатели погодных условий, после чего данные проходят процедуру классификации, в ходе которой между ними устанавливаются взаимосвязи, затем данные подвергаются фильтрации, то есть значения, выходящие за пределы разброса, удаляются, в конце осуществляется интерпретация, на основе которой составляется прогноз погоды на заданный промежуток времени.

Как правило, под использованием доверенных платформ искусственного интеллекта для анализа данных подразумевается их применение для анализа больших данных.

Большие данные — это данные, характеризующиеся 3-мя основными свойствами: внушительным объёмом, исчисляемым десятками терабайт, высокой скоростью обработки, разнообразием типов предоставляемой информации [2].

Работа с большими данными состоит из 3-х этапов:

1. интеграции;
2. управления;
3. анализа.

На этапе интеграции компания задействует различные способы сбора информации.

Этап управления ознаменует собой распределение и хранение полученных данных.

Анализ позволяет интерпретировать большие данные в необходимую информацию.

На рис. 1 представлены примеры использования больших данных.

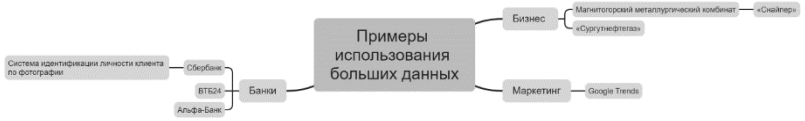

Рисунок 1 – Примеры использования больших данных

Первопроходцем использования больших данных в Российской банковской сфере стал Сбербанк. Они оперировали массивами данных большого объёма для системы аутентификации пользователей по фотографии с 2014 года. На сегодняшний день Сбербанк активно применяет большие данные в виде данных о клиентах, счетах и поведении

системы для повышения эффективности своей деятельности и защите от рисков.

Чуть позже к Сбербанку присоединились ВТБ24 и Альфа-Банк.

В качестве использования больших данных в бизнесе стоит отметить пример Магнитогорского металлургического комбината и их сервис «Снайпер», направленный на экономию сырья.

Также применяет массивы данных большого объёма для отслеживания бизнес-процессов «Сургутнефтегаз».

В маркетинге примером их использования является Google Trends, позволяющий повысить эффективность продаж.

Прежде чем говорить о доверенных платформах искусственного интеллекта необходимо определить, что понимается под доверенными платформами.

Доверенные платформы — это платформы, предоставляющие пользователям доступ к доверительным вычислениям.

Доверительные вычисления — это вычисления, производимые только посредством сертифицированного аппаратного и программного обеспечения [3].

В качестве примеров доверенных платформ стоит отметить продукты Российских компаний «Доломант» и ООО "АльтЭль", «Эльбрус» от ЗАО «МЦСТ» и Ассоциацию «Доверенная платформа» [4].

Ассоциация «Доверенная платформа» создана для построения цифрового пространства Интернета вещей. В неё входит много известных компаний (рис. 2).

Рисунок 2 – Перечень компаний, входящих в ассоциацию «Доверенная платформа»

Применение искусственного интеллекта для анализа данных включает:

- автоматизацию повторяющихся задач;
- выявление закономерностей и тенденций;
- поддержку прогностической аналитики;
- развёртывание и мониторинг моделей;
- исследование и визуализацию данных.

Доверенными платформами искусственного интеллекта называются платформы, результатам работы которых можно доверять [3].

Согласно анализу, представленному в работе [3], главным свойством, определяющим доверенную систему искусственного интеллекта, является устойчивость.

Под устойчивостью понимается неизменность поведения системы в процессе эксплуатации от заявленного в процессе обучения и тестирования.

Выделяют следующие этапы функционирования платформы искусственного интеллекта:

1. сбор обучающих данных;
2. создание обучающей выборки;
3. обучение модели;
4. тестирование модели;
5. эксплуатация модели.

На пути становления платформы искусственного интеллекта в качестве доверенной существуют следующие проблемы:

1. несоответствие обучающих данных тем, с которыми система работает;
2. отравление данных;
3. модификация данных;
4. обучение на состязательных (опровергающих) примерах;
5. атаки на системы машинного обучения;
6. изменение параметров.

Рис. 3 показывает, какие проблемы характерны для каждого этапа функционирования платформы искусственного интеллекта.

Рисунок 3 – Проблемы, характерные для каждого
этапа функционирования платформы искусственного интеллекта

Как правило, большинство доверенных платформ искусственного интеллекта построены на основе глубокого обучения.

В таб. 1 приведены примеры атак на системы глубокого обучения, представленные в [5].

Таблица 1 – Примеры атак на системы глубокого обучения

Атака	Место атаки	Затрагиваемые параметры	Методы противодействия
Adversarial Attack	Использование	Входные данные	Gradient Masking, Pre-Processing Filters, Adversarial Retraining
Backdoor Attack	Тренировка	Параметры сети	Pruning, Fine Tuning
Data poisoning	Тренировка, использование	Входные данные	Encryption, Local Training
IP stealing	Использование	Отклик системы	Obfuscation, Encryption
Neural-level trojan	Тренировка	Отклик системы	Data filtering
Side-channel Attack	Использование	Отклик системы	Randomness

Согласно проекту IBM Trusted AI надёжный искусственный интеллект обладает следующими составляющими:

– тестированием ИИ;

– состязательной устойчивостью и сохранением конфиденциальности;
– объяснимостью;
– чувствительностью к изменениям;
– справедливостью, подотчётностью, прозрачностью;
– надёжной и доверенной генерацией;
– количественной оценкой неопределённости [6].

На рис. 4 приведены известные доверенные платформы искусственного интеллекта.

Однако, так как требования к доверенным платформам искусственного интеллекта только формируются, назвать их доверенными можно лишь с явной натяжкой.

Искусственный интеллект является феноменом нашего времени. Он позволяет оптимизировать множество задач. Особенно это актуально для анализа больших данных.

Но существуют проблемы на сегодняшний день не позволяющие создать доверенную платформу искусственного интеллекта. Хотя многие производители называют свои продукты доверенными, работы над стандартизацией доверенных ИИ еще ведутся [3]. Проблема выражена и тем, что работая с большими данными, пользователь получает лишь результат, он не знает, как именно система искусственного интеллекта обрабатывает данные. Поэтому, чтобы сделать платформы ИИ доверенными, необходимо сделать их полностью прозрачными для пользователя.

Таким образом, для анализа больших данных предполагается использовать доверенные платформы искусственного интеллекта. Главным критерием того, что систему искусственного интеллекта можно назвать доверенной, является её устойчивость. На сегодняшний день, в соответствии с данным критерием, множество платформ искусственного интеллекта относят к доверенным. Но не всё так однозначно. Работы над стандартизацией доверенных платформ искусственного интеллекта ещё ведутся. Системы на основе искусственного интеллекта подвержены различным проблемам, требующим решения.

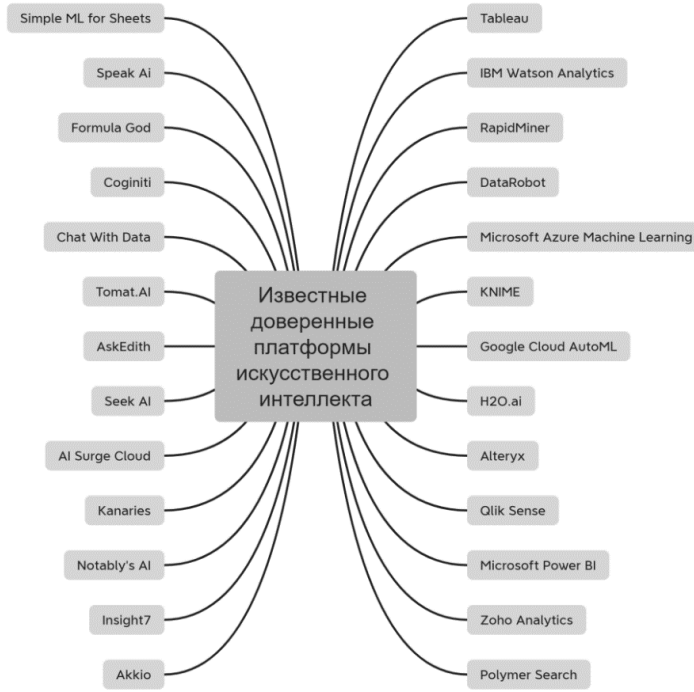

Рисунок 4 – Известные доверенные платформы искусственного интеллекта

Список использованных источников:

1. 10 Best AI Tools For Data Analysis [2024] // geeksforgeeks.org/. URL: https://www.geeksforgeeks.org/best-ai-tools-for-data-analysis/ (дата обращения: 12.04.2024).

2. Абрамов Р. Что такое «Big Data»? // habr.com. URL: https://habr.com/ru/companies/productstar/articles/503580/ (дата обращения: 12.04.2024).

3. Намиот Д.Е., Ильюшин Е.А., Пилипенко О.Г. Доверенные платформы искусственного интеллекта // International Journal of Open Information Technologies. 2022. №7. URL: https://cyberleninka.ru/article/n/doverennye-platformy-iskusstvennogo-intellekta (дата обращения: 12.04.2024).

4. Демешин С.В. Создание российской доверенной платформы для Интернета вещей // Информационное право в обществе. URL: https://dzen.ru/a/XPalnSegYACv_S7h (дата обращения: 12.04.2024).

5. Намиот Д.Е., Ильюшин Е.А., Чижов И.В. Текущие академические и индустриальные проекты, посвящённые устойчивому машинному обучению // International Journal of Open Information Technologies. 2021. № 10. URL: https://cyberleninka.ru/article/n/tekuschie-akademicheskie-i-industrialnye-proekty-posvyaschennye-ustoychivomu-mashinnomu-obucheniyu (дата обращения: 12.04.2024).

6. Trusted AI // URL: https://research.ibm.com/teams/trusted-ai (дата обращения: 12.04.2024).

УДК 004

С.С. Валеев, Р.Р. Султанов, Т.И. Макаримов
Уфимский университет
науки и технологий, Уфа, Россия

ПРИМЕНЕНИЕ ПРИНЦИПА НУЛЕВОГО ДОВЕРИЯ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИМИ ПРОЦЕССАМИ ПРЕДПРИЯТИЯ
APPLICATION OF THE ZERO TRUST PRINCIPLE IN AUTOMATED PROCESS CONTROL SYSTEMS OF ENTERPRISE

Аннотация: Обсуждаются особенности принципа нулевого доверия, решения необходимые для его реализации в системах управления промышленным предприятием. Рассматривается обобщенная схема реализации принципа нулевого доверия на основе алгоритмической защиты данных, с помощью встраиваемых средств защиты данных на исполнительном уровне системы управления.

Abstract: The features of the zero trust principle and the solutions necessary for its implementation in industrial enterprise management systems are discussed. We consider a generalized scheme for implementing the zero trust principle based on algorithmic data protection, using built-in data protection tools at the executive level of the control system.

Ключевые слова: Принцип нулевого доверия, архитектура нулевого доверия, промышленная система управления, защита данных, PLC.

Key words: Zero trust principle, zero trust architecture, industrial control system, data protection, PLC.

В настоящее время защита данных от несанкционированного доступа, с целью их модификации становится одной из первостепенных задач в различных областях, включая организационно-технические системы (ОТС) [1]. Автоматизированные системы управления технологическими процессами (АСУ ТП) относятся к классу ОТС и играют ключевую роль в современном промышленном производстве, обеспечивая эффективное управление и контроль различными производственными процессами.

Однако, в условиях возникновения новых киберугроз, традиционные методы защиты данных требуют совершенствования. Принцип нулевого доверия (ПНД) является одним их перспективных решений обеспечения безопасности обмена и передачи данных в АСУ ТП [2].

Как известно, АСУ ТП решают важные задачи управления в различных отраслях промышленности. Они включают в себя различные типы программируемых логических контроллеров (ПЛК), сенсоры, исполнительные устройства, SCADA-системы, которые взаимодействуют друг с другом по информационным каналам для обеспечения непрерывного и безопасного функционирования различных производственных процессов. Сложность и важность этих систем требует совершенствования методов защиты информации [3].

ПЛК являются важным элементом автоматизированных систем управления технологическими процессами. Они отвечают за анализ и контроль параметров производственного процесса, взаимодействуют с датчиками и исполнительными механизмами. Одной из задач ПЛК является обеспечение надежности и безопасности передачи данных между компонентами системы управления.

В АСУ ТП, особенно тех, которые функционируют десятилетиями, традиционные протоколы передачи и обмена данными, такие как Modbus, все еще широко используются. Эти протоколы были разработаны без учета современных требований к кибербезопасности, что делает их уязвимыми к некоторым видам атак. Внедрение принципа нулевого доверия позволяет повысить уровень защиты данных, передаваемых через такие протоколы.

Традиционные методы защиты обмена данными на основе защищенного периметра, уже не могут обеспечить достаточный уровень безопасности. В таких системах доступ предоставляется устройствам и пользователям, которые находятся внутри защищенной ЛВС предприятия.

Однако, с учетом современных угроз, включая внутренние угрозы и атаки, использующие уязвимости в легитимных приложениях, этот подход не всегда обеспечивает эффективное решение задачи защиты информации [4].

ПНД базируется на иной парадигме: никакое устройство или пользователь, даже если они находятся внутри сети, не должны автоматически получать доступ к запрашиваемым сервисам и активам.

Каждое действие, каждое подключение должно быть проверено и подтверждено. Это включает обязательную аутентификацию, авторизацию и алгоритмическую защиту данных, минимизацию привилегий и микросегментацию ЛВС предприятия.

Как отмечалось ранее, ПНД основывается, на том, что никакое устройство или пользователь не должны автоматически получать статус доверия в внутренней сети при обращении к ее активам.

Основные подходы, позволяющие, реализовать это следующие:

– использование методов аутентификации и авторизации на каждом шаге, т.е. каждое устройство и каждый пользователь должны быть идентифицированы и аутентифицированы перед получением доступа к активам системе, что позволяет предотвратить несанкционированный доступ даже в случае компрометации учетных данных;

– реализация динамической микросегментации сети, т.е. сеть должна быть разделена на небольшие сегменты, доступ к которым предоставляется только при подтверждении необходимости доступа к активам пользователями и устройствами, что помогает предотвратить распространение возможных атак внутри сети предприятия;

– применение алгоритмической защиты данных, т.е. все данные, передаваемые по сети, должны быть алгоритмически защищены от перехвата и утечки, что является необходимым для защиты конфиденциальной информации, передаваемой между различными подсистемами и компонентами АСУ ТП;

– использование разумной минимизации привилегий для пользователей и устройств, т.е. пользователи и устройства должны получать доступ только к тем ресурсам, которые необходимы для выполнения их задач, что приводит к снижению риска от потенциальных атак и возможных утечек информации.

Для реализации ПНД в АСУ ТП могут быть использованы различные известные технологические платформы. Одним из примеров является система ViPNet SIES, предназначенная для встраивания в АСУТП и обеспечивающая криптографическую защиту данных.

ViPNet SIES включает в себя алгоритмические модули защиты данных, которые могут быть встроены в ПЛК и другие компоненты системы управления технологическими процессами.

Эти модули обеспечивают защиту данных на уровне устройств, что позволяет защитить данные, передаваемые по различным каналам передачи данных.

Рассматриваемая подсистема включает рабочие места инженеров и операторов, SCADA сервер и базу данных, которые составляют пункт управления. Программный комплекс ViPNet SIES Unit обеспечивает шифрование данных в пункте управления.

Модули защиты данных ViPNet SIES Core, встроенные в ПЛК, выполняют обработку данных, переданных с пункта управления.

Использование ПНД в различных АСУТП позволит решить следующие задачи:

– повысить уровень безопасности с требованиями политики безопасности на предприятии, т.к. повсеместная аутентификация, микросегментация и защита данных снижают риски реализации угроз злоумышленниками;

– обеспечить соответствие заданным нормативным требованиям при аудите, т.е. применение рассматриваемого принципа способствует выполнению законодательных требований по защите данных и помогает избежать штрафов;

– повысить уровень управления доступом, т.к. администраторы сети получают возможность точечно контролировать доступ к ресурсам, что минимизирует риски возможных внутренних угроз;

– обеспечить защиту критически важных данных, т.к. конфиденциальные данные, передаваемые в АСУТП, в данном случае надежно защищены от несанкционированного доступа, что способствует устойчивой работе предприятия.

–

Список использованных источников:

1. Концепция Zero Trust: не доверяй - всегда проверяй URL: https:// www.kaspersky.ru/ blog/zero-trust-security/28780/?ysclid=lvqexsu7y0477804 184 (дата обращения: 28.04.2024).
2. Интегрированные системы проектирования и управления. SCADA: учебное пособие / Х.Н. Музипов, О.Н. Кузяков, С.А. Хохрин [и др.]. – Санкт-Петербург: Лань, 2022. – 408 с.
3. С.С. Валеев, Н.В. Кондратьева, М.Б. Гузаиров, А.В. Мельников. Этапы реинжиниринга информационной системы предприятия в рамках технологии нулевого доверия. [Электронный ресурс]: vestnik-rosnou.ru – 2023 – URL: https://vestnik-rosnou.ru/sites/default/files/136_Сложные%20 системы%20№%203%20ПРОСМОТРОВЫЙ.pdf (дата обращения: 28.04.2024).
4. С.С. Валеев, Н.В. Кондратьева. Особенности проектирования систем безопасности на базе архитектуры нулевого доверия. [Электронный ресурс]: ivdon.ru– 2023 – URL: http://www.ivdon.ru/uploads/article/pdf/IVD _68__8_valeev_kondratyeva_v2.pdf_72458b243f.pdf. (дата обращения: 28.04.2024).

УДК 004.056.5

А.М. Вульфин, А.Д. Кириллова
Уфимский университет
науки и технологий, Уфа, Россия

АВТОМАТИЗАЦИЯ МОДЕЛИРОВАНИЯ СЦЕНАРИЕВ РЕАЛИЗАЦИИ АТАК ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
AUTOMATION OF SIMULATION OF INFORMATION SECURITY ATTACK SCENARIOS

Аннотация: Рассматривается проблема обеспечения информационной безопасности автоматизированных систем управления технологическими процессами промышленных объектов. Разработана архитектура интеллектуальной системы поддержки принятия решений и программная реализация средств автоматизации моделирования сценариев проведения атак и оценки рисков информационной безопасности автоматизированных систем управления технологическими процессами, применение которых позволяет повысить эффективность выбора контрмер на этапах проектирования и внедрения комплексных систем защиты информации.

Abstract: The problem of ensuring information security of industrial control systems of industrial facilities is considered. The architecture of an intelligent decision support system and software implementation of automation tools for modeling attack scenarios and assessing the information security risks of industrial control systems have been developed, the use of which makes it possible to increase the efficiency of choosing countermeasures at the stages of designing and implementing complex information protection systems.

Ключевые слова: Информационная безопасность, оценка рисков, система поддержки принятия решений, автоматизированная система управления технологическими процессами, сценарий атаки.

Keywords: Information security, risk assessment, decision support system, industrial control system, attack scenario.

Современные промышленные системы автоматизации претерпевают цифровую трансформацию, что существенно обостряет проблему обеспечения информационной безопасности (ИБ) автоматизированных систем управления технологическими процессами (АСУ ТП) промышленных объектов. Текущий ландшафт угроз АСУ ТП промышленных объектов требует разработки и использования моделей и методов количественной оценки рисков ИБ АСУ ТП, применение которых позволит повысить оперативность и достоверность принимаемых управленческих решений [1, 2].

В [3] разработана методика количественной оценки рисков ИБ АСУ ТП на основе иерархии моделей и алгоритма построения сценариев проведения атак, отличающаяся нечетким когнитивным моделированием сценариев проведения атак в выделенных зонах промышленного объекта, что позволяет выполнить оценку рисков ИБ и оптимальное распределение затрат на реализацию, внедрение и сопровождение контрмер с учетом их функциональных ограничений. Автоматизация моделирования сценариев проведения атак позволяет извлечь информацию о слабых местах инфраструктуры, наиболее опасных уязвимостях и потенциальных слабостях компонент системы, выявить наиболее успешные сценарии реализации атак и оценить их последствия для промышленного предприятия.

Предлагается разработать инструментальные средства автоматизации моделирования сценариев проведения атак на АСУ ТП в составе интеллектуальной системы поддержки принятия решений (ИСППР) на этапе оценки рисков ИБ АСУ ТП промышленных объектов.

Описаны возможности практического применения инструментального средства автоматизации, включающие анализ уязвимостей объекта и моделирование сценариев реализации атак на основе открытых баз компьютерных атак, построение и визуализацию нечетких когнитивных карт (НКК), а также интеллектуальную оптимизацию весовых коэффициентов НКК.

На рисунке 1 представлен фрагмент логической модели данных, описывающей структуру и взаимосвязь основных сущностей предметной области, используемой для создания хранилища данных об угрозах, уязвимостях и сценариях их реализации.

Разработанное ПО обеспечивает:

– поддержку принятия решений при работе с открытыми базами угроз, уязвимостей и шаблонов атак, что позволяет специалистам, зная конкретные уязвимости объекта, получить наглядную графовую модель реализации атаки [4, 5];

– анализ сценариев атак с требуемым уровнем детализации и оптимизации весовых коэффициентов НКК при помощи методов машинного обучения для распределения ресурсов контрмер.

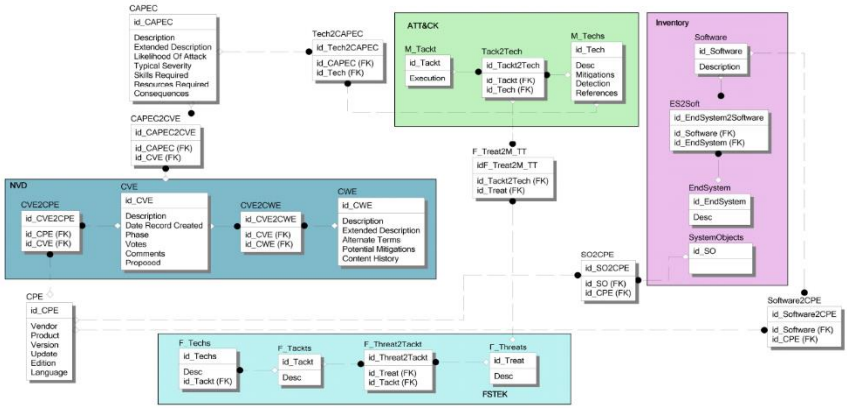

Рисунок 1 – Логическая модель данных

На рисунке 2 представлена фрагмент архитектуры ИСППР в нотации диаграммы компонентов UML с реализацией паттерна MVC.

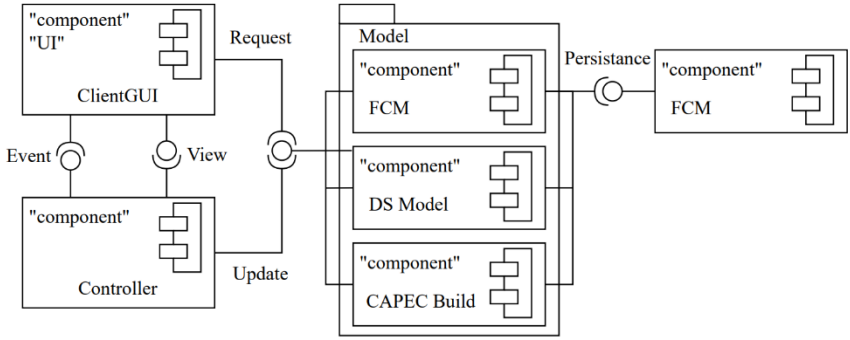

Рисунок 2 – Фрагмент архитектуры ИСППР
(диаграмма компонентов UML)

Разработанные инструментальные средства автоматизации моделирования сценариев проведения атак в составе ИСППР позволяют повысить достоверность и обоснованность качественных и количественных оценок рисков ИБ АСУ ТП с учетом воздействия факторов неопределенности. Применение программной реализации оценки рисков ИБ для конкретной АСУ ТП позволило после оптимизации распределения ресурсов, выделенных на контрмеры, уменьшить на 70-80 % как разброс, так и центральные значения экспертных оценок, а также повысить уровень ИБ АСУ ТП до допустимого и снизить оценку стоимости эксплуатации контрмер. Проведенные эксперименты показали, что на этапах проектирования и внедрения контрмер временные затраты на

моделирование сценариев реализации атак сократились более чем в 1,5 раза.

Список использованных источников:

1. Зегжда Д.П. и др. Кибербезопасность прогрессивных производственных технологий в эпоху цифровой трансформации // Вопросы кибербезопасности. 2018. Т. 2(26). С. 2–14.

2. Alshamrani A. et al. A survey on advanced persistent threats: Techniques, solutions, challenges, and research opportunities // IEEE Communications Surveys & Tutorials. 2019. Т. 2(21). С.1851–1877.

3. Васильев В.И., Вульфин А.М., Кириллова А.Д., Кучкарова Н.В. Методика оценки актуальных угроз и уязвимостей на основе технологий когнитивного моделирования и Text Mining // Системы управления, связи и безопасности. 2021. Т. 3. С. 110–134. DOI: 10.24412/2410-9916-2021-3-110-134.

4. Bakhtavar E. et al. Fuzzy cognitive maps in systems risk analysis: a comprehensive review // Complex & Intelligent Systems. 2021. Т. 7(2). С. 621–637.

5. Amirkhani A., Nasiriyan-Rad H., Papageorgiou E.I. A novel fuzzy inference approach: neuro-fuzzy cognitive map // International Journal of Fuzzy Systems. 2020. Т. 22(3). С. 859–872.

УДК 657.633.5

Б.К. Кушубакова
Уфимский университет
науки и технологий, Уфа, Россия

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ХОЗЯЙСТВУЮЩИХ СУБЪЕКТОВ В УСЛОВИЯХ ОБЯЗАТЕЛЬНОЙ ПУБЛИЧНОСТИ ОТЧЕТНОСТИ ОБ ИХ ДЕЯТЕЛЬНОСТИ
INFORMATION SECURITY OF ECONOMIC ENTITIES IN CONDITIONS OF MANDATORY PUBLIC REPORTING ON THEIR ACTIVITIES

Аннотация: В статье показано значение публичности информации, отраженной в бухгалтерской отчетности, для функционирования рынка и противоречие, возникающее между открытостью информации и необходимостью обеспечения ее защиты. Также рассмотрены тенденции изменений правил составления отчетности и пути их совершенствования

Abstract: The article shows the significance of publicity of information reflected in financial statements for the market, and the contradiction that arises between the transparency of information and the necessity to ensure its security.

The author also considers trends in changes in reporting rules and ways to improve them.

Ключевые слова: Информационная безопасность, бухгалтерская отчетность, публичность, эффективность рынка

Key words: Information security, financial statement, publicity, market efficiency

Системная и наиболее полная информация о деятельности организации формируется в бухгалтерской (финансовой) отчетности. Отчетность о деятельности организации является бухгалтерской по форме и финансовой по содержанию. Это и отражается в обозначении характеристики отчетности, как бухгалтерской, фиксируя внутри скобки финансовый характер ее содержания.

Информация о деятельности организации, отраженная в отчетности выступает готовой продукцией, которая создается в результате поэтапного, последовательного обобщения информации о каждом факте хозяйственной жизни, отражаемой на уровне первичного бухгалтерского учета.

Уникальность бухгалтерской (финансовой) отчетности состоит в том, что в ней сочетается статическая и динамическая информация о деятельности организации, которая обобщает результаты всех проведенных хозяйственных и финансово-экономических операций. Это свойство отчетности обусловлено методологией и методами построения системы бухгалтерского учета, основанной на базовых принципах двойной записи, полноты, достоверности, объективности и временной определенности.

Информация, отраженная в отчетности, будучи обязательно публичной, носит универсальный характер, так как, она одинаково полезна широкому кругу разнородных потребителей, выступающих ее пользователями.

Универсальность информации, отражаемой в отчетности, определяет цементирующее значение бухгалтерского учета и отчетности для функционирования рыночной системы. Каждая единица информации в отчетности это сигнал, прежде всего для инвесторов, который создает условия для информационной эффективности рынка, без которого рынок не работает.

Бухгалтерская отчетность выступает основным унифицированным институтом, периодически воспроизводящим ключевую информацию о деятельности организации, которые, по Дж. Акерлофу, как сигналы, снижают уровень асимметрии информации на рынке [6]. Снижение асимметрии информации приближает цены на качественные товары к их объективному уровню, создавая преграду развалу рынка.

Вместе с тем, уровень адресной полезности информации, отраженной в отчетности зависит от модели учета, на основе которой построена система национальных стандартов бухгалтерского учета и степени раскрытия информации. Как наиболее распространенные в мировой практике, можно выделить две модели. Первая модель бухгалтерского учета при формировании информации предполагает соблюдение приоритета интереса собственника, как пользователя информации. Вторая модель устанавливает приоритет государства, как пользователя информации о деятельности организации, для которого организация, прежде всего, субъект налоговых отношений. Установленный приоритет предопределяет порядок раскрытия информации.

Приведенные выше две модели различаются и по подходам к регулированию системы бухгалтерского учета. Первая модель функционирует на основе правил ведения учета и составления отчетности, разработанных и установленных профессиональным сообществом, в лице ассоциаций, комитетов и других объединений бухгалтеров и аудиторов. При второй модели регулирование порядка ведения учета и составления отчетности осуществляется государством.

Систему бухгалтерского учета, сформированную в России с большей уверенностью можно отнести ко второй модели, так как информация в учете и отчетности ориентирована на интересы государства и порядок ведения учета регулируется государством. Кроме того, в России применяется автономный налоговый учет, сопряженный с бухгалтерским учетом.

Налоговый учет был закреплен на законодательном уровне введением в действие с 1 января 2002 г. второй части Налогового Кодекса РФ, где статьи 313-333 гл. 25 отражают положения, регулирующие порядок ведения налогового учета объектов, связанных с определением налогооблагаемой базы по налогу на прибыль. Присвоением налоговому учету статуса обязательного завершилось формирование модели бухгалтерского учета, где приоритетным пользователем информации выступает государство.

Таким образом, с одной стороны публичность информации, отраженной в отчетности, нивелирует асимметрию информации о деятельности каждого хозяйствующего субъекта, повышая тем самым информационную эффективность и создавая условия для функционирования рынка.

С другой стороны, доступность информации, в зависимости от состава, объемов и уровня раскрытия информации в отчетности может влиять негативно на результаты деятельности хозяйствующего субъекта, создавая угрозу потери его конкурентоспособности не только на внутреннем, а и на внешнем рынке. Особенно важен этот момент для

участников международной деятельности. И определяющее значение имеет тот факт, что негативное влияние излишеств в раскрытии информации о деятельности хозяйствующих субъектов непосредственно влияет на национальную экономическую безопасность.

Следовательно, для обеспечения национальной экономической безопасности необходимо информацию в отчетности формировать по принципу оптимального соотношения между публичностью информации о деятельности хозяйствующих субъектов и допустимым уровнем ее раскрытия.

Практика становления бухгалтерского учета, отвечающего потребностям рыночной экономики, в России, в 1990-е годы далека от оптимального соотношения между публичностью информации о деятельности хозяйствующих субъектов и защищенностью информации. В стремлении приблизиться к международным стандартам бухгалтерской отчетности (МСФО) в отчетности отражалась избыточно детализированная по составу, структуре и содержанию информация, соответствующая установленным положениям, регулирующим бухгалтерский учет и порядок составления отчетности в России. Это, безусловно, противоречило интересам и отдельных хозяйствующих субъектов и национальной экономики в целом.

Неоправданно высокий уровень публичной детализации статей баланса был установлен Приказом Минфина России № 4-н от 13.01.2000 года, который был принят в рамках федерального закона от 21.11.1996 г. № 129-ФЗ "О бухгалтерском учете", и ПБУ 4/99 "Бухгалтерская отчетность организации", утвержденного Приказом Минфина России от 6.07.1999 г. № 43н.

В соответствии с данным документом например, статья «Запасы» должна была отражать величину запасов раздельно по всем их конкретным видам, в том числе запасы сырья и материалов, затраты в незавершенном производстве, запасы готовой продукции и товаров отгруженных и т.д. Еще более важная статья «Дебиторская задолженность» отражалась не только по срокам погашения (ожидаемые к погашению в течение 12 месяцев после отчетной даты и более 12 месяцев после отчетной даты). Отдельными строками в балансе показывались долги покупателей и заказчиков, векселей к получению, долги дочерних и зависимых обществ, учредителей по взносам в уставной капитал.

Учитывая логическую взаимосвязь статей «Запасы» и «Дебиторская задолженность», отражающих движение капитала по стадиям его трансформации, и соответственно возникающие проблемы в его кругообороте, такая информация могла быть использована конкурентами на внутреннем рынке для недобросовестной борьбы. На национальном уровне, зная состояние и характер неплатежей по экономике России,

можно было применить формы финансового давления на решение политических вопросов. Практически такой подход к формированию отчетности способствовал существенному снижению экономического суверенитета.

В определенной мере приведенный выше подход был преодолен Приказом Минфина России № 66н от 2.07.2010 года, согласно которому вышеназванная статья баланса «Запасы» отражалась одной строкой, и также статья «Дебиторская задолженность» стала отражаться свернуто, одной строкой. Можно сказать, что формами, рекомендованными для формирования отчетности согласно названному выше приказу, было обеспечены сужение состава информации, более высокий уровень обобщенности информации без детализации и соответственно более высокий уровень защищенности информации о деятельности хозяйствующих субъектов.

В современных условиях возникли новые вызовы в сфере обеспечения защиты информации, связанные с санкциями и разрывом хозяйственных и финансовых связей с большинством западных контрагентов, с построением новых логистических маршрутов.

Учитывая эти вызовы, государство дифференцировало доступ в Государственный информационный ресурс бухгалтерской (финансовой) отчетности (ГИРБО), которую формирует и ведет ФНС России. Так, согласно Постановлению Правительства РФ от 16.09.2022 № 1624 с 1 января 2023 года введены ограничения и установлены условия возобновления доступа к информации, отраженной в бухгалтерской отчетности организаций оборонно-промышленного комплекса, предприятий и организаций, отнесенных к стратегическим.

Регулирование доступа следует продолжить относительно отдельных категорий пользователей информации в финансовой отчетности. Для обеспечения защиты информации уровень доступа собственника и потенциального инвестора, регулятора финансового рынка и рейтингового агентства не должны быть одинаковыми.

Список использованных источников:

1. Налоговый кодекс Российской Федерации. Часть 2 от 5.08. 2000 г. № 117-ФЗ. [Электронный ресурс]. – URL: https://www.consultant.ru/document/cons (дата обращения: 20.04.2024).

2. Федеральный закон «О бухгалтерском учете» от 06.12.2011года № 402-ФЗ Электронный ресурс. URL: https://www.consultant.ru/document/cons (дата обращения: 20.04.2024).

3. Постановление Правительства РФ от 16.09.2022 г. № 1624 «О порядке ограничения и возобновления доступа к информации…

в ГИРБО….» [Электронный ресурс]. – URL: https://www.consultant.ru/document/cons (дата обращения: 20.04.2024)

4. Приказ Минфина России № 43н от 6/07. 1999 г. «Об утверждении положения по бухгалтерскому учету «Бухгалтерская отчетность организации» (ПБУ 4/99). [Электронный ресурс]. – URL: https://www.consultant.ru/document/cons_doc_LAW_18609/ (дата обращения: 20.04.2024).

5. Приказ Минфина России № 66н от 2 июля 2010 г. «О формах бухгалтерской отчетности организаций» Электронный ресурс. URL: https://www.consultant.ru/document/cons _doc_LAW_103394/ (дата обращения: 20.04.2024).

6. Акерлоф Дж. Рынок лимонов: неопределенность качества и рыночный механизм. / Ж. THESIS, 1994, вып. 5. С. 91-104.

УДК 004.032.26

Н.Д. Лушников
Уфимский университет
науки и технологий, Уфа, Россия

ИЗВЛЕЧЕНИЕ БИОМЕТРИЧЕСКИХ ХАРАКТЕРИСТИК ПРИ РАСПОЗНАВАНИИ ПОЛЬЗОВАТЕЛЕЙ КОМПЬЮТЕРНОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПО ГОЛОСУ И ПО ИЗОБРАЖЕНИЮ ЛИЦА
EXTRACTION OF BIOMETRIC CHARACTERISTICS IN RECOGNITION OF COMPUTER INFORMATION SYSTEM USERS BY VOICE AND FACIAL IMAGE

Аннотация. В данной статье описаны особенности верификации пользователей компьютерной информационной системы. Биометрическая система аутентификации состоит из подсистем, основанных на извлеченных признаках речи и изображений лица.

Abstract: This paper describes the features of user verification of a computer information system. Biometric authentication system consists of subsystems based on extracted features of speech and facial images.

Ключевые слова: Распознавание пользователей, биометрия, изображение лица, голос.

Keywords: User recognition, biometrics, facial image, voice.

В настоящее время наиболее актуальным вопросом является проблема защищенности устройства от несанкционированного доступа. Каждый из нас, используя персональное устройство, надеется на

минимальные риски и угрозы извне. Любой пользователь имеет полное право быть защищенным в той информационной среде, которая его окружает.

Время довольно быстро убегает вперед, изобилуя инновационными разработками и прогрессивными идеями в области информационных технологий. В перспективе, в автоматизированных системах предприятий начнут появляться новые квантовые компьютеры с высокой производительностью и высокоскоростной обработкой данных. Для таких устройств пользователю необходимы такие же инновационные программные продукты, которые будут защищать устройство от несанкционированного доступа и кибератак.

Процедуры аутентификации и авторизации субъектов являются важнейшим механизмом защиты, от качества которого зависит безопасность информационной системы. Средства аутентификации, авторизации и администрирования являются одними из классических средств по управлению информационной безопасностью компьютерными системами предприятия, и включают в себя такие процессы, как определение, создание, изменение, удаление и аудит пользовательских учетных записей [2]. Современные биометрические системы являются очень удобными для пользователей. В отличие от паролей и носителей информации, которые могут быть потеряны, украдены, скопированы, биометрические системы основаны на человеческих параметрах, которые всегда находятся вместе с ними, и проблема их сохранности не возникает.

Согласно имеющимся показателей современного рынка биометрических технологий, при распознавании пользователей чаще всего применяют такие биометрические параметры, как изображение лица, вены ладоней и голос [5]. Это, в первую очередь, связано с имеющимися показателями качества и точности распознавания пользователей.

В ходе исследования были разработаны программные модули распознавания пользователей компьютерной информационной системы по изображению лица и по голосу.

При распознавании пользователей компьютерной информационной системы по изображению лица используются такие процессы, как предварительная обработка изображений и морфологическое преобразование на основе фильтра Калмана. Данный метод предназначен для шумоподавления цифрового шума исходных изображений пользователей информационной системы (Рис. 1).

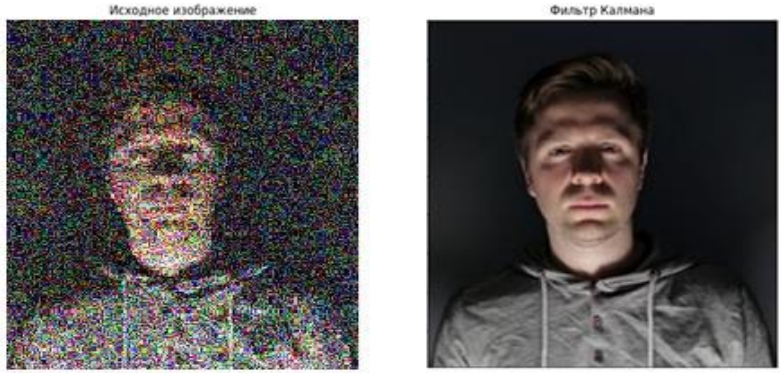

Рисунок 1 – Вывод работы программного обеспечения фильтрации помех изображения на основе фильтра Калмана

Произведя факторизацию спектральной плотности, найдем передаточную функцию формирующего фильтра для задающего воздействия.

Следует обозначить порождающий белый шум, из которого фильтр с передаточной функцией формирует случайное задающее воздействие со спектральной плотностью. Далее необходимо составить стохастическое дифференциальное уравнение для случайного задающего воздействия со спектральной плотностью. Используя векторно-матричные обозначения для совокупностей переменных и коэффициентов, уравнение состояния будет представлено в виде одного матричного уравнения первого порядка. На вход синтезируемого фильтра поступает m-мерная совокупность наблюдаемых величин, имеющая смысл многомерного входного воздействия. Как доказывается в теории оптимальной фильтрации, оптимальная оценка $y(t)$ процесса $x(t)$ удовлетворяет матричному дифференциальному уравнению (уравнение оценки).

В рамках исследования реализуется обработка сигнала с видеопотоком в режиме онлайн. Для противодействия несанкционированному доступу разработан программный модуль, который определяет настоящего искомого пользователя информационной системы от объекта, который его олицетворяет (муляж) (Рис. 2) [3].

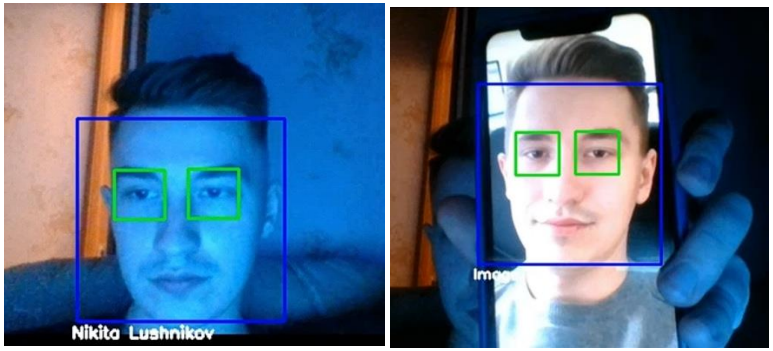

Рисунок 2 – Распознавание пользователя информационной системы по изображению лица

Также в данном исследовании были получены дополнительные биометрические характеристики при распознавании пользователей компьютерной информационной системы на основе алгоритмов машинного обучения с применением библиотек языка программирования Python (Рис. 3) [4]. Данный софт реализован на языке программирования Python 3.8 с применением таких библиотек, как tensorflow, keras, librosa, opencv, numpy и pandas. Разработаны и реализованы архитектуры нейронных сетей на основе различных наборов обучающих выборок (датасетов). В рамках обучения задействовано 512 нейронов и 100 эпох обучения.

Для повышения точности и качества обработки биометрических характеристик следует обратить внимание на имеющиеся разработки в данной области, которые сводятся к минимизации ошибок первого и второго рода.

Таким образом, для решения данной проблемы рекомендуется разработать комбинированные мультимодальные биометрические системы – системы, которые используют несколько различных биометрических модальностей (например, распознавание по лицу и голосу). Мультимодальные биометрические системы способны устранить такие недостатки одномодальных систем, как шум в полученных данных, неадаптивность, восприимчивость к спуфинговым атакам и большие внутриклассовые вариации. Использование правильной методологии объединения данных может значительно улучшить производительность сопоставления. Наличие нескольких источников также увеличивает пространство признаков, тем самым увеличивая количество людей, которых можно надежно различать.

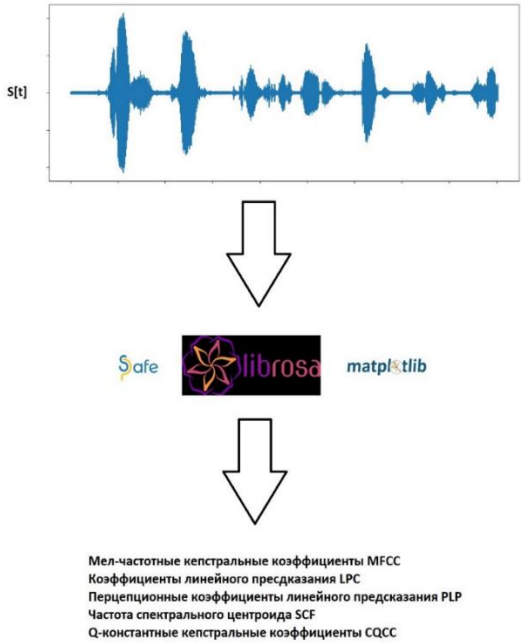

Рисунок 3 – Алгоритм биометрической системы аутентификации пользователей компьютерной информационной системы при извлечении акустических признаков

Однако биометрические характеристики человека обычно являются биологическими особенностями, которые могут быть либо генетически, возможно, экологически измененными, либо приобретенными или приобретенными со временем характеристиками, которые могут быть использованы для распознавания или идентификации человека [1].

Список использованных источников:

1. ГОСТ Р 54411-2018 Информационные технологии. Биометрия. Мультимодальные и другие мультибиометрические технологии. URL: https://docs.cntd.ru/document/1200098737 (дата обращения 05.05.2024).

2. ГОСТ Р 58833-2020 Защита информации. Идентификация и аутентификация. Общие положения. URL: https://docs.cntd.ru/document/1200172576 (дата обращения 05.05.2024).

3. Свидетельство о государственной регистрации программы для ЭВМ № 2021614672 Российская Федерация. Аутентификация учетных записей пользователей с помощью биометрических технологий: №

2021613387: заявл. 15.03.2021: опубл. 29.03.2021 / Н.Д. Лушников, А.С. Исмагилова; заявитель федеральное государственное бюджетное образовательное учреждение высшего образования «Башкирский государственный университет».

4. Исмагилова А.С. Программная реализация защиты от несанкционированного доступа / А.С. Исмагилова, Н.Д. Лушников // Безопасность информационных технологий. – 2023. – Т. 30, № 1. – С. 81-91.

5. Пчеловодова Н. Российский биометрический рынок в 2019–2022 годах. Результаты масштабного исследования J'son & Partners Consulting // Системы безопасности. 2019, № 2. С. 88–91.

УДК 004.71:004.4:339.5

В.А. Марцинкевич, М.В. Романюк, А.Н. Марков
Белорусский государственный университет информатики
и радиоэлектроники, Минск, Беларусь

ИМПОРТОЗАМЕЩЕНИЕ СЕТЕВОГО ОБОРУДОВАНИЯ И ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ В РАЗРЕЗЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ВНУТРЕННЕЙ ИНФРАСТРУКТУРЫ ОРГАНИЗАЦИИ
IMPORT SUBSTITUTION OF NETWORK HARDWARE AND SOFTWARE IN THE CONTEXT OF INFORMATION SECURITY OF THE ORGANIZATION'S INTERNAL INFRASTRUCTURE

Аннотация: В статье рассмотрены принципы и подходы по импортозамещению сетевого оборудования и программного обеспечения для виртуализации в разрезе информационной инфраструктуры организации. Отмечены ключевые компании поставщики и производители, а также продукты, сертифицированные для использования в Республике Беларусь.

Abstract: The article discusses the principles and approaches to import substitution of network equipment and software for virtualization in the context of the organization's information infrastructure. Key suppliers and manufacturers are noted, as well as products certified for use in the Republic of Belarus.

Ключевые слова: Импортозамещение, сетевое оборудование, межсетевые экраны, средства виртуализации, среда виртуализации.

Keywords: Import substitution, network equipment, firewalls, virtualization, virtualization environment.

В эпоху мировых трансформаций экономики приобретает все большую популярность импортозамещение телекоммуникационного оборудования и программного обеспечения. Импортозамещение как фактор является актуальной темой в сфере информационных технологий. Исторически сложилось, что западные вендоры телекоммуникационного оборудования (Cisco, Huawei, Dell, HP) доминировали на рынке Республики Беларусь. На фоне изменившейся обстановки в мире и Республике Беларусь, в частности, многие иностранные компании после 2022 года заявили о частичной или полной приостановке деятельности и полном уходе с рынка стран СНГ. При том, потребности в технике и программном обеспечении не уменьшились, что автоматически сделало возродило импортозамещение ИТ-оборудования и программных продуктов.

Так из декабрьского отчета Strategy Partners «Стратегическое исследование российского рынка ПО и автоматизации бизнес-процессов для финансового сектора» следует, что в 2022 г. в общей структуре российского ИТ-рынка 60% приходилось на ИТ-оборудование, 27% – на ИТ-услуги и 13% – на программное обеспечение [1]. Импортозамещение телекоммуникационных компаний на рынке Республики Беларусь затрагивает все аспекты функционирования экономики.

В контексте импортозамещения в направлении сетевого оборудования: коммутаторов, маршрутизаторов и решений для беспроводных сетей, стоит отметить, что Cisco, HP и Dell, ушедшие с рынка Беларуси, занимают лидирующие мировые позиции в этой области, а также обладают многолетним опытом и многомиллионными контрактами. Они предлагают широкий спектр продуктов и решений, которые используются во многих странах.

В рамках импортозамещения по вышеописанному направлению наиболее широкий выбор продуктов на рынке Республики Беларусь действуют как Российские, так и Китайские партнеры. (Российские компании – Zelax, Eltex и QTECH. Китайские компании – Maipu, Ruijie и BDCOM.) Они производят множество различных коммутаторов, маршрутизаторов и решений для беспроводных сетей Wi-Fi, что делает их широко представленными на рынке. Компании постоянно обновляют свои продукты и внедряют новые технологии, чтобы оставаться конкурентоспособными и удовлетворять потребности клиентов.

Однако, необходимо учесть, что в некоторых случаях предлагаемое оборудование может не полностью соответствовать требованиям и стандартам, которые предъявляются к продуктам международных брендов, поэтому перед принятием решения о замене оборудования

необходимо провести тщательное тестирование и возможности интеграции в существующую инфраструктуру.

В контексте импортозамещения межсетевых экранов, включая экраны типа NGFW, российские и китайские компании представляют собой важные альтернативы импортным решениям. Продукты многих иностранных производителей, включая Fortinet и Cisco, больше официально не представлены на рынке Беларуси, несмотря на это возможен их ввоз с использованием параллельного импорта и сертификация, однако использование таких продуктов в критически важной инфраструктуре сопряжено с множеством рисков как для компаний-дилеров и поставщиков, так и для покупателей.

Среди межсетевых экранов, официально представленных в Республике Беларусь можно выделить следующие продукты:

1. Continent – Комплекс безопасности «Континент» версии 4 сертифицирован Оперативно-аналитическим центром при Президенте Республики Беларусь (далее – ОАЦ) для серийного производства.
2. UserGate – Включает в себя брандмауэры, веб-фильтры, системы управления доступом к интернет-ресурсам и другие решения для обеспечения безопасности сетей. Программно-аппаратные и программные комплексы сертифицированы ОАЦ в Республики Беларусь для серийного производства.
3. Ideco – Ассортимент включает брандмауэры, системы мониторинга и анализа трафика, а также решения для защиты данных в облачных средах. Продукты Ideco сертифицированы в Беларуси отдельными партиями: 200 шт. в 2022 году, 100 шт. в 2023.
4. Sangfor – На рынке Республики Беларусь представлен межсетевыми экранами различных серий. Однако, устройства сертифицируются и ввозятся небольшими партиями: с 2023 года сертифицировано ОАЦ всего 10 устройств.

Еще одним важным направлением импортозамещения в Республике Беларусь является виртуализация. На замену продуктам виртуализации пришли вендоры из Российской Федерации и Китая, а также разработки компаний из Республики Беларусь:

5. ZVirt Max – На момент написания статьи покрытие функционала vSphere не полное, отсутствует, например, автоматизация процесса обновления инфраструктуры, поддержка репликации на уровне СХД и управление конфигурациями хостов. В некоторых статьях отмечается неудобный интерфейс и плохая документация на продукт [2]. Сертифицирована ОАЦ в Республике Беларусь партия продукции из 100 комплексов.
6. ROSA Virtualization – ROSA Virtualization создавалась с прицелом на отказоустойчивость, что достигается благодаря режиму

гиперконвергентной инсталляции с использованием распределенной файловой системы GlusterFS в конфигурации от трёх узлов и от двух узлов в кластере в конфигурации с СХД. В ОАЦ сертифицирована партия продукции 200 шт.

7. ZStack – Платформа является довольно зрелой с технической точки зрения и покрывает фактически весь функционал vSphere, дополняя его собственными наработками, например, cross-cluster HA, поддержкой ceph, а также собственным аналогом VMware NSX и др. Сертифицированы в ОАЦ несколько партий продукции в суммарном количестве 400 шт.

8. itPVE – Платформа не имеет аналога VMware vSAN, VMware NSX, собственных разработок и дополнений к функционалу не заявлено. Нет гарантированной совместимости с различными системами резервного копирования, т.к. в них не заявлена официальная поддержка данной платформы. Имеется сертификат ОАЦ на серийное производство.

Нельзя не отметить, что все еще возможен ввоз оборудования и ПО с использованием параллельного импорта и сертификация в регулирующих органах продукции иностранных компаний, ушедших с рынка Республики Беларусь, однако необходимо понимать, что использование такой продукции может быть сопряжено с невозможностью обращения напрямую в техподдержку, увеличением сроков гарантийной замены и ремонта товаров, а также с рисками удаленной блокировки устройств, доступа к обновлениям ПО и сигнатур безопасности и другим облачным функциям, требующим подключение к серверам производителей.

Список использованных источников:

1. Импортозамещение «софта» и «железа» вступает в новую фазу [Электронный ресурс]. – URL: https://www.novostiitkanala.ru/news/detail.php?ID=174771 (дата обращения: 20.04.2024).

2. Тестируем отечественную виртуализацию: итоги и выводы [Электронный ресурс]. – URL: https://habr.com/ru/articles/800039/ (дата доступа: 21.04.2024).

УДК 004.932.2

Н.Г. Миронова
Уфимский университет
науки и технологий, Уфа, Россия

РАСПОЗНАВАНИЕ ФЕЙКОВОСТИ ИЗОБРАЖЕНИЙ И НЕЙРОСЕТЕВОГО КОНТЕНТА
RECOGNITION OF FAKE IMAGES AND NEURAL NETWORK CONTENT

Аннотация: В статье выполнен анализ подходов к распознанию фейкового визуального контента.

Abstract: The article analyzes approaches to recognizing fake visual content.

Ключевые слова: Форензика, фейки, нейросети, дезинформация.

Keywords: Forensics, fakes, neural networks, information warfare.

В условиях информационной войны технология дипфейков позволяет быстро генерировать и распространять обман, создавая нужную массовую реакцию и ошибки в принятии решений ЛПР. Как отличать фейковый мультимедиа контент от образа реального процесса или объекта?

1. Предупредительные меры:

1.1. Правовые меры воздействия на создателей фейков – принятие законов об ответственности граждан и юрлиц за размещение фейков, несущих общественную угрозу. В РФ, например, действует ФЗ № 31 от 18.03.2019 г. «О внесении изменений в статью 15.3 ФЗ (о блокировке фейковой информации), поправки в КоАП РФ (например, ст. 13.15 «Злоупотребления СМИ» и т.п.). Но эффект от таких мер в условиях информационного противоборства стран невелик, фейковый контент активно используют ресурсы за пределами России.

1.2. Запреты стоковых сервисов изображений (например, Adobe Stock [1]) публиковать определенные категории сгенерированного нейросетями контента (например, созданного с использованием запросов об конкретных людях, местах, объектах собственности и т.п.) и рекомендация авторам сгенерированных НС и отредактированных изображений указывать это в описании к файлу. Мера малоэффективна в глобальном интернете, т.к. источником фейков служат не только стоковые хранилища; большинство СМИ и людей сами генерируют фейки с помощью многочисленных НС-сервисов, не храня их в стоках).

1.3. Способы защиты контента от подмены и редактирования кем-либо в будущем. Например, с помощью сервисов можно добавить на

публично размещаемые фото невидимые шумы (от каждого типа «атак» на изображение – свои шумы); техническое ограничение внесения изменений в скопированное с сайта фото (оно будет отображаться в искаженном виде после копирования или добавить элементы на защищенные фотографии у злоумышленников не получится). Также для сайтов применяется запрет на копирование изображений с помощью CSS свойств, HTML, функции JavaScript, наложения поверх изображения на сайте второго, прозрачного пустого слоя для защиты от копирования [2], но этот метод защиты от подтасовки изображения малоэффективен. Еще одна технология защиты достоверности фото – использование производителями цифровых камер наложения цифровых EXIF- меток в файл фото и видео в момент съемки (аналог сертификата цифровой подписи или сертификата доверенного сервера); впрочем, EXIF-данные легко редактировать (программами типа EXIF Pilot), да и другие выше перечисленные методы ограниченно эффективны.

1.3. «Честное предупреждение». Более эффективен в борьбе с фейками метод принуждения разработчиков сервисов генерации нейросетевого контента в обязательном порядке снабжать синтетический продукт спец. метками типа «сделано нейросетью» и т.п., желательно, легко заметными, - подобно тому, как ставится водяной знак для защиты изображений от несанкционированного использования и подделки (вотермарку помогают проставлять на фото программы типа Photoshop, Lightroom и др.). Для сгенерированного контента метод принудительной пометки применяется мало (некоторыми сервисами генерации музыки и графики), как правило, метки незаметны, изредка проставляются в метаданных файла (далеко не всегда), поэтому никак не мешают создателям НС-фейков обманывать людей. Например, Adobe с Nikon, BBC, Microsoft и Truepic договорились [3] снабжать меткой CR (Content Credentials) изображения, созданные или исправленные с помощью нейросетей (данные об источнике изображения добавляются в метаданные документа, видеозаписи либо могли бы вставляться цифровой камерой в файл). DeepMind от Google выпустил инструмент для создания и обнаружения водяных знаков SynthID (невидимые изменения в пикселях изображений, распознаваемые алгоритмами, указывают на искусственное происхождение изображения), а разработчик нейросетевого генератора изображений Vertex AI [4] дает возможность вставлять в созданные этой НС изображения цифровой «водяной знак» SID (к слову, поисковик Google при поиске изображений может по метаданным изображения указать, что оно сгенерировано нейросетью, для чего изображение должно быть изначально размечено НС-сервисом согласно стандарту IPTC).

В целях безопасности технология использования меток авторства должна быть схожа с использованием сертификата электронной подписи в

последней редакции документа, чтобы подписи всех редактирующих файл людей и сервисов принудительно сохранялась в метаданных файла, - что, однако, требует наличия буквально у каждого пользователя универсального идентификатора, поддерживаемого в любом средстве создания и редактирования фото и видео. (примерно так, как в системах электронного документооборота хранится вся история обработки документа). Сервисы генеративных НС также следовало бы обеспечить поддержкой меток авторства для всей продукции ГНС, что предполагает следование всех разработчиков «творческих» сервисов единому стандарту верификации. Понятно, что это пока нереально, т.к. вызвало бы сопротивление разработчиков и пользователей НС-сервисов. Но честно было бы ставить хотя бы видимый невооруженным глазом «водяной знак» «сгенерировано/скорректировано нейросетью» на синтетический контент. В реальности для повышения доверия к изображениям в общественных облачных хранилищах рекомендуется верифицировать изображения по некоторым стандартам (C2PA и т.п.), но пока эта мера лишь локально и добровольно применяемая – она малополезна в борьбе с фейками. Также для защиты изображений от подделки в будущем могли бы быть полезны криптоалгоритмы.

2. Методы распознания созданных фейков.

2.1. Визуальный анализ на основе опыта («насмотренности»). Для продукции нейросетей характерны некоторые признаки, отличающие их от реальных фото и видео: неестественная регулярность объектов, клонирование (дублирование) элементов изображения – слишком много чего либо (деревьев, людей, пальцев на руке), лица, позы, предметы, иные элементы на одном изображении однотипны; нарушена перспектива; нарочитая «красивость» или «трагедийность» сюжетов; гладкость или аномальность структуры поверхностей, чрезмерная детализация и четкость всех элементов изображения – или расфокусированность тех деталей, которые должны быть в фокусе; стереотипность ракурсов; неестественность освещения; размытость фона; отсутствие в зрачке сгенерированного лица отражения, или отражение в разных глазах различается. При анализе фейк-видео, сгенерированного или исправленного нейросетью, подмена видна по движению глаз, частоте моргания, расхождении темпа речи с движением губ, странному направлению взгляда, неестественным движениям тела при дыхании и т.д. Впрочем, создатели нейросетей постоянно дообучают их; наложение цифровой маски на реальное видео в реальном режиме времени делает фейки более реалистичными и хуже распознаваемыми визуально, а если фото или виде вручную отредактирует специалист, то и «насмотренность» не поможет распознать фейк. Сомнительную новость или изображение можно поискать по нескольким авторитетным источникам, чтобы понять,

имело ли место событие реально и когда, т.к. фейки нередко выдают старую информацию за остроактуальную (поиск аналогов - сервисы images.google.com, tineye.com и т.п.).

2.2. Анализ мета-данных мультимедиа-файлов для обнаружения подделки. Есть сервисы анализа метаданных изображений по характеристикам сжатия JPEG (типа https://www.fakeimagedetector.com), но сгенерированные нейросетью изображения они плохо различаются этими сервисами от реальных фото. Для анализа фейковости видео проводят покадровый анализ; например, появление размытости на отдельных кадрах намекает на наличие редактирования, фейка и т.п.

2.3. Применение нейросетей для распознания фейков, для различения естественных и сгенерированных/измененных изображений. Усилия в этом направлении предпринимаются почти 10 лет (проект «Media Forensics» от DARPA (2016) [5], исследования Дартмутского и Политехнического университетов (2018) [6], технология Video Authenticator (от Microsoft), 2020) и Project Angora (от Gfycat, 2019) и др.) и привели к созданию ряда сервисов (например, сервис hivemoderation.com/ai-generated-content-detection довольно хорошо определяет сгенерированное нейросетью, а другие сервисы (contentatscale.ai/ai-image-detector, huggingface.co/spaces/umm-maybe/AI-image-detector, huggingface.co/spaces/umm-maybe/AI-image-detector и т.п.) - плохо отличает НС-контент от реального фото. Недостаток современных НС-инструментов распознания фейков – их ограниченная эффективность (обученные под один сервис, детекторы ИИ-контента плохо справляются с другими, универсального инструмента анализа дипфейков пока нет). Можно ожидать, что состязательные нейросети могли бы быть обучены совместно с генеративными сетями на обнаружение фейкового контента, но потребовался бы доступ к моделям (кто ж предоставит доступ к своей коммерческой тайне) - или массивам больших массивов обучающих образцов. Еще один метод детектирования НС-фейков - использовать специфичные для разных НС-инструментов «отпечатки», которые оставляют в сгенерированных изображениях НС-модели, прогнав изображение через фильтры анализаторов изображения. Настоящие фотографии имеют высокий уровень и однородность шума, а вставки, сделанные редактором, почти не имеют шума, а для нейросетевых изображения шумы изображения могут иметь необычную форму. Анализ изображений м.б. выполнен сервисами вроде 29a.ch/photo-forensics; есть программа Ghiro для обнаружения в цифровых изображениях следов монтажа и подделки; сервис и программа Deepware для обнаружения дипфейковых видео scanner.deepware.ai/; корейское приложения анализа фейков kaicatch.com/ и т.д.

В целом можно сказать, что эффективность отдельных существующих средств и мер борьбы с фейками невелика, но при применении всего комплекса мер повышается.

Список использованных источников:

1. Руководство пользователя для авторов AdobeStock. – URL: https://helpx.adobe.com/ru/stock/contributor/help/titles-and-keyword.html (Дата обращения: 12.01.2024)
2. Как защитить изображения на сайте от копирования (Дата публикации: 23.02.2023) – URL: https://mchost.ru/articles/kak-zashtitit-izobrazheniya-na-sajte-ot-kopirovaniya
3. Parsons A. Adobe MAX 2023: Milestone wave of Content Credentials adoption with industry partners Microsoft, Leica Camera, Nikon, Publicis Groupe, and more / blog.adobe.com – URL: https://blog.adobe.com/en/publish/2023/10/10/new-content-credentials-icon-transparency (Дата публикации: 10 октября 2023)
4. Gowal S., Pushmeet Kohli, Identifying AI-generated images with SynthID. – URL: https://deepmind.google/discover/blog/identifying-ai-generated-images-with-synthid/ (Дата публикации: 29 августа 2023)
5. Hatmaker T. DARPA is funding new tech that can identify manipulated videos and «deepfakes» // TechCrunch. 2018. 30.04. – https://techcrunch.com/2018/04/30/deepfakes-fake-videos-darpa-sri-international-media-forensics
6. Chesney R., Citron D. Deepfakes and the New Disinformation War: The Coming Age of Post-Truth Geopolitics // Foreign Affairs. 2019. – С. 152

УДК 004.451.9

И.В. Салов
Уфимский университет
науки и технологий, Уфа, Россия

ПЕРЕХОД НА РОССИЙСКИЕ ОПЕРАЦИОННЫЕ СИСТЕМЫ
TRANSITION TO RUSSIAN OPERATING SYSTEMS

Аннотация: В статье описаны этапы перехода организации на российские операционные системы и раскрыты основные проблемы, возникающие при таком переходе.

Abstract: The article describes the stages of an organization’s transition to Russian operating systems and reveals the main problems that arise during such a transition.

Ключевые слова: Операционная система, российская операционная система, программное обеспечение, импортозамещение, этапы перехода, перечень российского программного обеспечения.

Keywords: Operating system, Russian operating system, software, import substitution, stages of transition, list of Russian software.

Переход на российское программное обеспечение является насущной необходимостью. Это осознает и государство, и бизнес. Руководством страны принят ряд нормативно-правовых актов в сфере импортозамещения. С 1 января 2016 г. вступило в силу Постановление Правительства РФ от 16.11.2015 № 1236 «Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд» [1], определяющее курс на импортозамещение всего используемого в Российской Федерации программного обеспечения до конца 2024 года. Согласно нему, все государственные и муниципальные бюджетные органы власти, осуществляющие государственные закупки в соответствии с требованиями закона №44-ФЗ, обязаны соблюдать запрет на допуск к конкурсам и тендерам иностранного программного обеспечения. В сфере средств защиты информации действует Указ Президента РФ от 1 мая 2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» [3]. Однако, не только нормативно-правовые акты требуют скорейшей замены программного обеспечения на российские аналоги. Отключение лицензий используемого зарубежного программного обеспечения свершившиеся факты. И, конечно, если мы переходим на импортозамещение в программном обеспечении, то, начинать необходимо с операционной системы [4].

Для перехода на российские операционные системы в организации, как правило, создается рабочая группа, курирует, или возглавляет которую, заместитель руководителя по вопросам использования IT. При переходе на российскую операционную систему, если речь не идет о создании информационной системы с нуля, любой организации предстоит пройти ряд обязательных этапов.

1. Определение перечня используемого и необходимого программного обеспечения и периферийных устройств.

2. Сравнительный анализ имеющихся на рынке российских операционных систем, с учетом поддерживаемого ими программного обеспечения и периферийных устройств.

3. Определение перечня, отсутствующего в репозиториях анализируемых операционных систем необходимого программного

обеспечения и драйверов периферийных устройств, необходимых по функциям или по иным причинам.

4. Оценка стоимости и сложности реализации возможных решений по отсутствующему программного обеспечению и драйверов для периферийных устройств.
5. Подготовка плана перехода на российские операционные системы.
6. Процесс миграции.
7. Тестовая эксплуатация с выявлением всех проблемных моментов.
8. Решение всех возникших вопросов.
9. Ввод модернизированной информационной системы в эксплуатацию.

Первый этап не представляет из себя особой трудности, так как, обычно, все программное обеспечение и периферийные устройства инвентаризированы. Возможно, если инвентаризация проводилась только в рамках бухгалтерского учета, придется вносить в перечень используемое свободное или бесплатное программное обеспечение. Однако, в список используемого ПО и периферии придется вносить метку о том, необходимы ли функциональные или точные аналоги. Например, использование уникального программного комплекса и/или уникальной же периферии. При учете периферии необходимо отметить наличие драйверов для различных операционных систем как в комплекте поставки, так и наличие их в сети Интернет.

Второй этап, заключающийся в сравнительном анализе имеющихся на рынке российских операционных систем, казалось бы, более трудозатратен. Однако, несмотря на то, что в перечне российского программного обеспечения [5] на данный момент к категории «Операционные системы общего назначения» относится 13 записей, выбор не так уж велик.

Согласно материалам, размещенному на сайте интернет-обзоров iaassaaspaas.ru [6], топ-3 российских операционных систем по итогам четырех месяцев 2024 года заняли более 97% рынка. Так что рассматривать, фактически, придется Astra Linux (71,7%, ГК Астра), Ред ОС (15,6%, компания РЕД СОФТ) и Альт Linux (10,1%, компания Базальт СПО). Кроме того, если в информационной системе предполагается обрабатывать гостайну, то выбор сужается до Astra Linux или Альт Linux. Именно они сертифицированы ФСБ для данных работ. Если же такой необходимости нет, то можно рассмотреть и РЭД ОС. Кроме указанного интернет-обзора, имеется и большое количество иных обзоров в различных источниках, которые, в целом, подтверждают данный вывод. Например, обзор ixbt.com, по итогам 2023 год оценки рынка российских операционных систем [7]. Кроме того, правительство РФ, например, в лице

Минцифры, активно подталкивает к выбору именно одной из трех указанных ОС [8].

Третий этап заключается в подготовке списка отсутствия для каждой из выбранных операционных систем необходимого программного обеспечения и драйверов периферийного оборудования. Должно учитываться отсутствие как в репозитории конкретной операционной системы, так и на сайте разработчиков. В списке же должны ставиться пометки о том, возможен ли переход на другое программное обеспечение и оборудование. Следует отметить, что если первый этап, как правило, проводится сотрудниками подразделения, использующего средства вычислительной техники, с помощью сотрудников бухгалтерии, то третий и четвертый этапы могут выполнить только наиболее сотрудники службы поддержки средств вычислительной техники или администраторы информационных систем.

При проведении четвертого этапа, после определения перечня необходимого, но отсутствующего программного обеспечения, следует принять решение, возможен ли переход на функционально аналогичное программное обеспечение или периферию, или придется решать вопрос иным методом. Четвертый этап достаточно сложен, так как предполагает оценку (как финансовых издержек, технической сложности реализации, так и временных затрат) нескольких возможных вариантов решения. Возможно, например, применение технологии виртуализации. Вероятно, придется провести и ряд некоторых исследований по возможности применения нестандартных вариантов решения, таких, например, как применение программных продуктов NDISwrapper или NDISulator. Не исключена вероятность того, что придется разрабатывать свое программное обеспечение для взаимодействия с уникальным периферийным оборудованием, например, получения передаваемых периферией данных на низком уровне и записи их в специальный файл.

Именно на этом этапе возможно принятие решения о использовании, в некоторых случаях, разных российских операционных систем. Хотя, необходимо учитывать, что однообразие применяемых операционных систем намного облегчает обслуживание и сопровождение операционных систем. Кроме того, разнообразие используемых операционных систем осложняет и процесс обучения сотрудников организации, работающих в информационных системах.

Пятый этап перехода на российские операционные системы очень важен. При подготовке к переходу на российские операционные системы конкретной информационной системой необходимо тщательно спланировать и зафиксировать порядок действий. Необходимо определить порядок, сроки, ответственных за проведение конкретного действия, средства, применяемые на данном этапе. Например, при проведении

архивного копирования информации с компьютера, определяется ответственный, срок проведения копирования, время, необходимое для этого, на какой носитель производится копирование (с учетом необходимых объемов информации), где будет храниться копия и кто отвечает за ее сохранность, и каким образом будет проводиться восстановление информации в новой системе. На все процедуры необходимо планировать некоторый запас времени, сил и средств.

При этом необходимо учитывать не только вопрос перехода на отдельно взятом компьютере, но и сети/сетей в целом. Решение необходимо будет принимать исходя из операционной системы будущих серверов и рабочих станций. Существует множество альтернатив для Active Directory. Например, кроссплатформенная Avanpost Directory Service (от компании Аванпост) или ALD Pro (от ГК Астра). Существует большое количество и бесплатных, но более специализированных продуктов, чаще всего использующих в своей основе протокол LDAP. В зависимости от размеров организации, некоторое время в организации параллельно будут существовать информационные системы основанные на разных принципах управления пользователями, сервисами и ресурсами. Рекомендуется, по возможности, заблокировать на переходный период внесение изменения в Active Directory. Или, при невозможности такого решения, фиксировать все изменения, которые будет необходимо внести, например, в Avanpost Directory Service.

Шестой этап, то есть процесс миграции, требует огромного внимания, тщательного выполнения всех запланированных этапов и готовности к быстрому реагированию на возникновение нештатных ситуацию. Именно в процессе миграции проявляются все ошибки, допущенные на этапе планирования. Именно в этих случаях положительную роль может сыграть запас времени, сил и средств, заложенный на этапе планирования. Имеющийся опыт показывает, что возможен и желателен предварительный переход некоторых сервисов организации на российское программное обеспечение. Например, почтового сервиса, систем управления базами данных и т.п.

Седьмой (тестовой эксплуатации) и восьмой (решения возникших проблем) этапы, в соответствии с циклом PDCA, скорее всего, придется проводить не один раз. Данные этапы занимают достаточно много времени и заканчивается, когда некоторое, достаточно продолжительное время не возникает новых критических ошибок, не связанных с ошибками эксплуатации. При анализе ошибки должен учитываться ее характер, обстоятельства возникновения, вероятность ее дальнейшего появления. При подготовке плана по устранению должен указываться ответственный за выполнение каждого пункта, необходимое время, задействованные силы и средства. Если возможно несколько путей решения данной проблемы, то

просчитываются затраты (как финансовые, так и временные) для каждого варианта. Решение по данному вопросу принимает руководитель организации.

Решение о переходе к девятому этапу принимает первое лицо организации по представлению рабочей группы, организующей переход на российские операционные системы.

Список использованных источников:

1. Постановление Правительства РФ от 16.11.2015 № 1236 «Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд» (с изм. и доп.) [Электронный ресурс]. – URL: http:www.garant.ru (дата обращения: 18.04.2024).

2. Федеральный закон "О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд" от 05.04.2013 № 44-ФЗ (с изм. и доп.) [Электронный ресурс]. – URL: https://www.consultant.ru (дата обращения: 18.04.2024).

3. Указ Президента РФ от 1 мая 2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» [Электронный ресурс]. – URL: http:www.garant.ru (дата обращения: 18.04.2024).

4. Андреев, М.Ф. Обработка сетевых пакетов в ядре Linux для противодействия атакам типа «отказ в обслуживании» / М.Ф. Андреев, А.С. Исмагилова // Информационные технологии обеспечения комплексной безопасности в цифровом обществе: сборник материалов VI Всероссийской молодежной научно-практической конференции с международным участием, Уфа, 19–20 мая 2023 года. – Уфа: Уфимский университет науки и технологий, 2023. – С. 9-14.

5. Единый реестр российских программ для электронных вычислительных машин и баз данных [Электронный ресурс]. – URL: https://reestr.digital.gov.ru/ (дата обращения: 18.04.2024).

6. Российские операционные системы. Обзор рынка 2024 / Iaassaaspaas.ru обзоры облачных исследований [Электронный ресурс]. – URL: https://iaassaaspaas.ru/rating/russian-os (дата обращения: 18.04.2024).

7. Российские операционные системы набирают обороты. Рынок таких ОС в прошлом году вырос на 57% / МРАК [Электронный ресурс]. – URL: / https://www.ixbt.com/news/2024/04/02/rossijskie-operacionnye-sistemy-nabirajut-oboroty-rynok-takih-os-v-proshlom-godu-vyros-na-57.html (дата обращения: 18.04.2024).

8. Минцифры потребует предустанавливать российские операционные системы на ноутбуки и ПК / Олег Капранов [Электронный

ресурс]. – URL: / https://rg.ru/2023/04/25/mincifry-potrebuet-predustanavlivat-rossijskie-operacionnye-sistemy-na-noutbuki-i-pk.html (дата обращения: 18.04.2024).

УДК 004

А.Ф. Фатхелисламов
Уфимский университет
науки и технологий, Уфа, Россия

БЕСПРОВОДНАЯ СЕТЬ КАК УЯЗВИМОЕ МЕСТО В ПЕРИМЕТРЕ ЗАЩИТЫ
WIRELESS NETWORK AS A VULNERABILITY IN THE SECURITY PERIMETER

Аннотация: В статье рассматриваются вопросы безопасности применения беспроводных сетей и рекомендации для улучшения их защиты.

Abstract: The article discusses the security issues of using wireless networks and recommendations for improving their protection.

Ключевые слова: Беспроводная сеть, аудит безопасности, шифрование, контроль доступа, информационная безопасность.

Keywords: Wireless network, security audit, encryption, access control, information security.

Много работ посвящено изучению беспроводных сетей и вопросу их безопасного использования со стороны обычных пользователей и компаний, которые занимаются обработкой персональных данных [1-3]. Также в техническом плане существуют множество технологий, которые применять радиоканал, как среду для передачи данных. Разнообразие беспроводных технологий и гаджетов позволяют создавать быстро разворачиваемые и масштабируемые сети для обмена данными, и позволяют без существенных материальных затрат настроить и подключить новых клиентов. Но в погоне за удобством и минимизации затрат, не нужно забывать про аспекты информационной безопасности. Они могут стать уязвимым местом в защите сетевой инфраструктуры и открыть дать возможность для реализации атак. Так как с развитием технологий следуют также растет число угроз и атак на эти сети. Беспроводные сети могут представлять с потенциальную уязвимость в периметре защиты атакуемой сети.

Атака также может проводится на пользователей сети с помощью «зеркальных» точек, созданных по подобию компрометируемой точки для захвата данных пользователей и проведения фишинговых атак.

Для повышения безопасности беспроводных сетей можно применить различные методы защиты. Вот основные из них:

1. Использование последних алгоритмов шифрования. Применение WPA3 для шифрования трафика, поскольку это последний и наиболее безопасный стандарт.

Избегание устаревших и менее безопасных методов, таких как WEP и WPA2.

2. Сегментация сети. Создание отдельных SSID для гостевых пользователей и устройств IoT, чтобы ограничить доступ к корпоративной сети. Создание виртуальных локальных сетей (VLAN) для дополнительной изоляции трафика.

3. Управление доступом. Применение сильных паролей и периодическое их обновление. Использование аутентификации с использованием радиус-серверов или других более надежных методов аутентификации. Проведите настройку аутентификации через серверы, такие как RADIUS или TACACS, для управления доступом на основе пользовательских учетных записей.

4. Физическая безопасность. Ограничение физического доступа к оборудованию беспроводной сети.

Применение методов обнаружения несанкционированного доступа к сетевым устройствам.

5. Мониторинг и управление. Регулярный мониторинг сетевого трафика и автоматическое обнаружение аномалий. Можно установить программы для защиты от сетевых атак, а также в ручном режиме мониторить подозрительный траффик с помощью программ-анализаторов. Введение системы управления беспроводными доступными точками для централизованного управления и мониторинга.

6. Обновление ПО. Регулярное обновление программного обеспечения точек доступа и клиентских устройств для защиты от известных уязвимостей. Обеспечивайте регулярное обновление фирменной прошивки и программного обеспечения сетевых устройств для защиты от известных уязвимостей.

7. Ограничение мощности сигнала. Настройка мощности передатчиков таким образом, чтобы сигнал не выходил далеко за пределы необходимой территории.

Сочетание этих мер поможет создать более безопасную беспроводную сетевую инфраструктуру и значительно снизить риск потенциальных угроз, но не гарантирует полную безопасность. Чтобы выявить риски использования беспроводной сети необходимо провести

ряд тестирований на безопасность, связанная с проникновением в сетевой периметр из вне и контролируемую атаку на точку [4]. Итогом которого будет анализ эффективности применяемых методов для защиты. По мере необходимости оптимизируйте настройки для улучшения производительности и безопасности.

Также как базовое правило использования беспроводных сетей, их нужно отделить от корпоративной сети и сделать отдельный сегмент. Настройте различные SSID для каждой сегментированной группы пользователей. Это позволит легко управлять политиками безопасности и доступом. Назначьте каждому SSID отдельный VLAN. Это изолирует трафик каждой группы на уровне сети, предотвращая возможное пересечение данных между сегментами. Настройте маршрутизаторы и коммутаторы на поддержку VLAN тегирования (802.1Q). Создайте различные политики безопасности для каждого VLAN, основываясь на уровне чувствительности данных и требований к доступу. Примените меры контроля доступа, такие как Списки Контроля Доступа (ACL) и аутентификация через радиус-серверы или другие системы аутентификации.

Рассмотренные меры значительно повысят уровень безопасности беспроводной сети, обеспечив надежную защиту данных и устройств внутри сети.

Список использованных источников:

1. Исследование влияния атак на беспроводные сети Wi-Fi 6e / М.М. Ковцур, С.А. Винников, В.И. Трезоров, А.Ю. Киструга // Экономика и качество систем связи. – 2023. – № 2(28). – С. 87-92.

2. Особенности организации доступа к сети интернет в общественных Wi-Fi сетях / С.Ю. Бодриков, А.В. Лукьянчиков, Д.С. Иванченко, Е.Я. Закурдаева // Современные проблемы радиоэлектроники и телекоммуникаций. – 2023. – № 6. – С. 69.

3. Анализ атак на WI-FI сети / Е.Г. Ткачева, В.С. Калашников // Научный аспект. – 2024. – Т. 38, № 1. – С. 4977-4983.

4. Моделирование сетевых атак в условиях учебной лаборатории / Э.М. Вахитова // Информационные технологии обеспечения комплексной безопасности в цифровом обществе: Сборник материалов VI Всероссийской молодежной научно-практической конференции с международным участием, Уфа, 19–20 мая 2023 года. – Уфа: Уфимский университет науки и технологий, 2023. – С. 71-73.

УДК 004.056

Р.М. Яппаров
Уфимский университет
науки и технологий, Уфа, Россия

К ВОПРОСУ О БЕЗОПАСНОСТИ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ
ON THE ISSUE OF SECURITY OF CRITICAL INFORMATION INFRASTRUCTURE FACILITIES

Аннотация: В данной статье рассматриваются актуальные вопросы, связанные с определением значимости критических процессов на объектах критической информационной инфраструктуры. Автором проводится анализ содержания критических процессов в образовательной организации на примере действующей Единой государственной информационной системой учёта научно-исследовательских, опытно-конструкторских и технологических работ (ЕГИСУ «НИОКТР»), их составляющие и структура.

Abstract: This article discusses topical issues related to determining the importance of critical processes at critical information infrastructure facilities. The author analyzes the content of critical processes in an educational organization using the example of the current Unified State Information System for Accounting for Research, Development and Technological Works (EGISU "R&D"), their components and structure.

Ключевые слова: Критическая информационная инфраструктура, объект, критические процессы, информационная безопасность, информационная система, законодательство, угрозы, уязвимости, защиты информации.

Keywords: Critical information infrastructure, facility, critical processes, information security, information system, legislation, threats, vulnerabilities, information protection.

В современную цифровую эпоху необходимость обеспечения безопасности критически важных объектов информационной инфраструктуры невозможно переоценить. Эти объекты, в том числе электрические сети, транспортные системы, финансовые институты и государственные учреждения, необходимы для функционирования общества, и любое нарушение их работы может иметь серьезные последствия для государства и общества. Обеспечение безопасности объектов критической информационной инфраструктуры страны стало сегодня главным приоритетом в стратегии национальной безопасности государства.

В Российской Федерации обеспечение безопасности критической информационной инфраструктуры регламентируется Федеральным законом «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 № 187-ФЗ и другими подзаконными нормативными правовыми актами. Поэтому обеспечение информационной безопасности критического объекта информационной инфраструктуры является сложной и многогранной задачей, требующей скоординированных усилий всех заинтересованных сторон.

В работе любой организации существенное значение на результаты работы оказывают критические процессы, проходящие как внутри так и за пределами зоны ответственности. При этом не все проходящие внутри организации процессы являются критическими. Умение выделять их из общей массы всевозможных других, также нужных и необходимых, имеют большое значение в сфере информационного благополучия.

В соответствии с законом, под критическими понимаются процессы, нарушение и (или) прекращение которых может привести к негативным социальным, политическим, экономическим, экологическим последствиям, последствиям для обеспечения обороны страны, безопасности государства и правопорядка [1].

Определение содержания значимых критических процессов важная составляющая любой критической информационной инфраструктуры. При этом соответствующему анализу должна подвергаться повседневная деятельность организации. В условиях, когда нормативная база, определяющая порядок определения критически важных процессов оставляет желать лучшего организациям зачастую самим приходится его выбирать. Так, например, в образовательных организациях эту процедуру следует начинать с установления степени критичности имеющихся научно-образовательных процессов. Для убедительности можно проанализировать пять таких возможных критических процессов:

1. Сбор данных (технологический процесс);
2. Контроль выполнения проектных работ (управленческий процесс);
3. Обработка, анализ и обобщение информации (технологический процесс);
4. Контроль правильности результатов (технологический процесс);
5. Формирование заявок в РосПатент (иные).

Отметим, что работоспособность вышеназванных критических процессов обеспечивается Единой государственной информационной системой учёта научно-исследовательских, опытно-конструкторских и технологических работ (далее – ЕГИСУ «НИОКТР»). Для выполнения поставленных задач автоматизированные рабочие места (АРМ) ЕГИСУ «НИОКТР» должны быть объединены в единую корпоративную

локальную ИВС с выходом в информационно-телекоммуникационную сеть общего пользования (Интернет). Наличие выхода в сеть «Интернет» - обязательный элемент использования информационной системы [2].

Основным назначением ЕГИСУ «НИОКТР» является автоматизация управленческих процессов, связанных с проведением научно-исследовательских, опытно-конструкторских и технологических работ, и поэтому система должна обеспечивать функционирование указанных выше критических процессов. Содержанием ЕГИСУ «НИОКТР» охватывается актуализация и систематизация всех научно-исследовательских, опытно-конструкторских и технологических работ, их выбор и обоснование. При этом пользователям системы предоставляется ограниченный правами администратора доступ к информации о ходе, проводимых исследований, полученным отчётам и результатам. В целом система обрабатывает научную информацию, поступающую от всех участвующих и зарегистрированных в ней субъектов образовательной организации, и поэтому является учётно-аналитической.

Сбор информации в ЕГИСУ «НИОКТР» позволяет ее систематизировать и объединить в единую базу научно-исследовательских, опытно-конструкторских и технологических знаний, которая позволит произвести расчёт затрат на разработку новых и проведение дополнительных научных исследований, а также использовать результаты интеллектуальной деятельности в различных бизнес-проектах, стартапах и т.д.

В ЕГИСУ «НИОКТР» образовательной организации могут быть сосредоточены следующие виды документов, подверженные угрозам нарушения их целостности, доступности, конфиденциальности: отчёты, договоры, заявки, проекты, заключения, диссертации, справки, техническая документация [3]. И если все угрозы ЕГИСУ «НИОКТР» образовательной организации объединить в группы по принципу их возникновения и использования, то можно системно получить следующую картину:

1. Организационные угрозы. К ним можно отнести отсутствие соответствующих инструкций по конфиденциальному делопроизводству, режимных ограничений, в том числе установления допусков сотрудникам и режима доступа в защищаемые помещения, обучения персонала правилам работы со сведениями, ограниченного доступа, разработанных в соответствии с требованиями нормативных актов должностных обязанностей.

2. Физические угрозы. Они могут проявляться в том, что СКУД находится вне пределов контролируемой зоны и внутриобъектовый режим организации не обеспечивает надежную охрану периметра защищаемой территории от проникновения злоумышленника.

3. Программно-аппаратные угрозы. К ним можно отнести модификацию BIOS, разграничение прав доступа и установление привилегий отдельным пользователям, уязвимости в межсетевом взаимодействии, отсутствие СКЗИ, средств межсетевого экранирования, сертифицированных средств защиты информации, в том числе от НСД, использование устаревших версий программных продуктов, в том числе средств антивирусной защиты, старого оборудования [4].

Правильное определение угроз безопасности, своевременный и надлежащий анализ уязвимостей ЕГИСУ «НИОКТР» образовательной организации позволят вовремя обнаружить проникновение в информационную систему и заблаговременно принять меры по противодействию правонарушению.

Список использованных источников:

1. Галатенко, В.А. Стандарты информационной безопасности: учебник / В.А. Галатенко. – М.: Изд-во «Интернет-университет информационных технологий ИНТУИТ.ру», 2019. – 287 с.

2. Малюк, А.А. Введение в защиту информации в автоматизированных системах / А.А. Малюк, С.В. Пазизин, Н.С. Погожин. – М.: Горячая линия – Телеком, 2019. – 147 с.

3. Методика оценки угроз безопасности информации [Электронный ресурс] // Режим доступа: / URL: fstec.ru/dokumenty/vse-dokumenty/spetsialnye- normativnye-dokumenty/metodicheskij-dokument-ot-5-fevralya-2021-g. (дата обращения 18.05.2024).

4. Яппаров, Р.М. Роль и значение автоматизированных информационных систем в правоохранительной деятельности / Р.М. Яппаров // Информационные технологии обеспечения комплексной безопасности в цифровом обществе: сборник материалов V Всероссийской молодежной научно-практической конференции, Уфа, 20–21 мая 2022 года. – Уфа: Башкирский государственный университет, 2022. – С. 48-53. – DOI 10.33184/itokbco-2022-05-20.12.

СЕКЦИЯ 1. МАТЕМАТИЧЕСКИЕ МОДЕЛИ И МЕТОДЫ ЗАЩИТЫ, ПРЕОБРАЗОВАНИЯ И ПЕРЕДАЧИ ИНФОРМАЦИИ

УДК 004

С.З. Бильданов
Поволжский государственный университет
телекоммуникаций и информатики, Самара, Россия

Научный руководитель:
М.В. Шакурский
Поволжский государственный университет
телекоммуникаций и информатики, Самара, Россия

АНАЛИЗ СТЕГАНОГРАФИЧЕСКИХ ИНСТРУМЕНТОВ ДЛЯ СОРЕВНОВАНИЙ ФОРМАТА CTF И ИСПОЛЬЗУЕМЫХ В НИХ МЕТОДОВ СОКРЫТИЯ ИНФОРМАЦИИ
ANALYSIS OF STEGANOGRAPHIC TOOLS FOR CTF FORMAT COMPETITIONS AND INFORMATION HIDING METHODS USED IN THEM

Аннотация: В настоящей работе представлен анализ популярных стеганографических инструментов, используемых в соревнованиях формата CTF. В настоящей работе рассмотрены алгоритмы сокрытия информации, используемые в представленных инструментах. Рассмотренные алгоритмы сокрытия информации были исследованы на предмет используемых теоретических методов сокрытия информации.

Abstract: In the given paper we present an analysis of popular steganographic tools used in CTF format competitions. In the given paper we examined information hiding algorithms used in presented steganographic tools. Information hiding algorithms were analyzed for used theoretical information hiding methods.

Ключевые слова: Методы сокрытия информации, стеганография.

Keywords: Information hiding methods, steganography.

Обеспечение информационной безопасности неразрывно связано с такими методами защиты информации, как криптография и стеганография. Данные методы используются совместно: криптография позволяет скрыть смысл сообщения, а стеганография – сам факт передачи.

В наше время одним из самых популярных форматов соревнований в области информационной безопасности является формат Capture the Flag(CTF), в котором команды пытаются получить у противника уникальную последовательность символов, называемую флагом, решая различные прикладные задачи, связанные со многими областями Информационной безопасности, в том числе, и со стеганографией. Список инструментов, используемый на таких соревнованиях в области стеганографии, известен, так что я считаю актуальным выявить, какие теоретические методы стеганографии в них использованы, для более успешного погружения в формат CTF.

Целью своей работы я ставлю рассмотрение известных приложений в области стеганографии с точки зрения используемых в них стеганографических методов защиты информации. Для этого необходимо описать основные методы стеганографии, привести список приложений для сокрытия информации и рассмотреть методы, используемые в них.

Приложения, используемые в соревнованиях формата CTF предусматривают сокрытие информации в изображениях и аудиозаписях.

Основным методом сокрытия информации в изображениях и аудиофайлах является метод встраивания в наименее значащий бит. Пиксель изображения содержит 3 байта информации о содержании в нем красного, зеленого и синего цветов соответственно. Среди каждого из этих байтов выбирается наименее значащий бит, значение которого меняют с целью встраивания секретной информации. [1]

Такой метод достаточно прост в реализации, практически не искажает изображение, что затрудняет обнаружение передачи невооруженным глазом, однако не безопасен при атаке на изображение с помощью статистических методов.

При сокрытии информации в аудиофайлах также используется метод фазового кодирования, основанный неразличимости человеческим слухом незначительных изменений фазы сигнала. Звуковая дорожка разбивается на некоторое количество сегментов по длине сообщения, после чего вычисляется разность фаз соседних сегментов, полученных с помощью дискретного преобразования Фурье. Секретное сообщение встраивается в фазу первого сегмента, после чего матрица фаз строится заново с учетом изменений. По завершению изменений, сигнал восстанавливается с помощью обратного дискретного преобразования Фурье. [1]

В соревнованиях формата CTF используются такие инструменты, как OpenStego, StegHide, MP3Stego.

OpenStego является удобным инструментом для сокрытия информации в изображениях с помощью таких методов, как сокрытие информации в наименее значащем бите, но также поддерживает DCT-преобразование, Быстрое преобразование Фурье и т.д. Данные методы

достаточно просто реализовать и обнаружить, что является хорошим качеством для соревнований CTF, заточенных для погружения участников в область Информационной безопасности.

StegHide является инструментом для сокрытия информации как в изображениях, так и в аудио-файлах. Утилита также использует внедрение информации в наименее значащие биты, поэтому подходит для использования в CTF, как было объяснено выше.

MP3Stego используется для сокрытия информации только в звуковых файлах расширения .wav при сжатии их в формат .mp3. Инструмент использует следующий алгоритм: данные сжимаются, шифруются, а затем скрываются в битовых потоках файла MP3. Причем сам процесс сокрытия данных осуществляется в процессе шифрования: внутренний цикл выполняет квантование информации до тех пор, пока количество бит не будет достаточным для кодирования информации или пока не будут достигнуты ограничения психо-акустической модели. Далее выполняется побитовое сложение по модулю 2 битов основной информации и битов кода Хафммана для последующего сокрытия информации в случайно выбранных битах результата на основе алгоритма SHA-1. [2]

Из этого следует, что выбранные программы используют основные методы сокрытия информации, которые обнаружимы. Это объяснимо тем, что современные методы стеганографии затрудняют обнаружение скрытой информации, что противоречит цели соревнований – погружение участников в область ИБ с помощью интересных прикладных задач.

Список использованных источников:

1. Нгуен Зуи Кыонг, ИССЛЕДОВАНИЕ И РАЗРАБОТКА УНИВЕРСАЛЬНОГО МЕТОДА СТЕГОАНАЛИЗА НА ОСНОВЕ ИСПОЛЬЗОВАНИЯ NIST-ТЕСТОВ [Текст]: дис. … канд. техн. наук, 05.13.19 – СПБГУТ, Санкт-Петербург, 2020 – 136 с.

2. MP3Stego: The information hiding homepage [Электронный ресурс] – URL: https://www.petitcolas.net/steganography/mp3stego/ (дата обращения 26.04.24).

УДК 004.056

Э.М. Вахитова
Уфимский университет
науки и технологий, Уфа, Россия

Научный руководитель:
А.Ф. Фатхелисламов
Уфимский университет
науки и технологий, Уфа, Россия

СРЕДСТВА ПРОВЕДЕНИЯ MITM-АТАКИ НА УРОВНЕ ОПЕРАЦИОННОЙ СИСТЕМЫ
METHODS OF CONDUCTING A MAN-IN-THE-MIDDLE ATTACK AT THE OPERATING SYSTEM LEVEL

Аннотация: В работе представлен обзор программных средств для моделирования сетевых атак на базе учебной лаборатории. Рассмотренные методы сетевых атак “man-in-the-middle” позволили разработать имитационную модель такой атаки. Было проведено ее моделирование в учебной сети с использованием инструментов на уровне операционной системы. Проанализировано влияние атаки на работу сетевого оборудования и конфиденциальность передаваемых данных.

Abstract: The paper presents an overview of software tools for modeling network attacks based on a training laboratory. The considered methods of man-in-the-middle network attacks made it possible to develop a simulation model of such an attack. It was modeled in the learning network using tools at the operating system level. The impact of the attack on the operation of network equipment and the confidentiality of transmitted data is analyzed.

Ключевые слова: Анализ трафика, сетевая инфраструктура, MITM, моделирование атак, система защиты, трафик, сетевые аномалии.

Keywords: Traffic analysis, network infrastructure, MITM, attack modeling, protection system, traffic, network anomalies.

Сетевая атака – одна из самых больших проблем при обеспечении безопасности информации предприятий и бесперебойной работы информационных систем. Обеспечение безопасности сетевой инфраструктуры играет важную роль при проектировании систем защиты [1]. Атаки типа «Человек посередине» (MITM), проводимые на уровне операционной системы, представляют угрозу безопасности информационных систем. В этой статье приводится обзор инструментов, используемых злоумышленниками для проведения MITM-атак [2], уделяя особое внимание Bettercap, Mitmproxy и Hetty в качестве наглядных примеров. MITM-атаки предполагают, что злоумышленник перехватывает

сетевой трафик между двумя или более узлами и манипулирует им, выдавая себя за доверенного посредника. Такие атаки могут привести к несанкционированному раскрытию конфиденциальной информации. MITM-атаки на уровне операционной системы получили широкое распространение благодаря их способности использовать уязвимости в различных сетевых протоколах.

В ходе исследований и экспериментальных атак с использованием Bettercap, Mitmproxy и Hetty мы выявили различные аномалии в перехваченном сетевом трафике и манипулировании им. Эти аномалии включали несанкционированный перехват и перенаправление трафика, внедрение вредоносного контента, изменение конфиденциальных данных и потенциальное нарушение конфиденциальности, целостности и неприкосновенности частной жизни пользователей.

В результате экспериментов с использованием Bettercap были обнаружены следующие аномалии в сетевом трафике:

ARP spoofing: Bettercap успешно перехватывал и перенаправлял сетевой трафик, что приводило к неправильной маршрутизации пакетов и возможному несанкционированному доступу к конфиденциальной информации.

DNS spoofing: Возможности DNS spoofing Bettercap позволяли манипулировать ответами DNS и перенаправлять пользователей на вредоносные веб-сайты, что создавало угрозу фишинговых атак и сбора конфиденциальных данных.

SSL stripping: С помощью функции SSL stripping в Bettercap можно было снизить защищенные соединения HTTPS до незашифрованного HTTP, что создавало уязвимости для перехвата и изменения конфиденциальной информации.

В результате экспериментов с использованием Mitmproxy были обнаружены следующие аномалии:

Манипуляция с HTTP трафиком: Mitmproxy перехватывал и изменял трафик HTTP, внедряя вредоносные сценарии или контент на веб-страницы, что нарушало целостность данных и могло угрожать конфиденциальной информации.

Перехват HTTPS: Mitmproxy имел возможность перехватывать и расшифровывать трафик HTTPS, что вызывало опасения относительно конфиденциальности и целостности обмена данными.

В результате экспериментов с использованием Hetty были выявлены следующие аномалии:

ARP spoofing: Hetty успешно выполнял ARP spoofing, что приводило к нарушению связи, возможному захвату сеансов и несанкционированному доступу к конфиденциальной информации.

DNS spoofing: Возможности DNS spoofing Hetty позволяли манипулировать ответами DNS и перенаправлять пользователей на вредоносные веб-сайты, что компрометировало безопасность и конфиденциальность пользователей.

Список использованных источников:

1. Вахитова, Э. М. Моделирование сетевых атак в условиях учебной лаборатории / Э.М. Вахитова // Информационные технологии обеспечения комплексной безопасности в цифровом обществе: сборник материалов VI Всероссийской молодежной научно-практической конференции с международным участием, Уфа, 19-20 мая 2023 года. – Уфа: Уфимский университет науки и технологий, 2023. – С. 71-73.

2. Казаков, М.Б. MITM-атаки и их предотвращение / М.Б. Казаков // Информационные технологии в деятельности органов внутренних дел: сборник научных статей Всероссийской научно-практической конференции, Москва, 20 апреля 2023 года. – Москва: Московский университет Министерства внутренних дел Российской Федерации им. В.Я. Кикотя, 2023. – С. 32-33.

3. Canteaut, A. Sieve-in-the-middle: Improved MITM attacks / A. Canteaut, M. Naya-Plasencia, B. Vayssière // Lecture Notes in Computer Science. – 2013. – Vol. 8042 LNCS, No. Part 1. – P. 222-240. – DOI 10.1007/978-3-642-40041-4_13.

УДК 004.056.53

Н.А. Волков
Самарский государственный
технический университет, Самара, Россия

Научный руководитель:
А.В. Иванов
Самарский государственный
технический университет, Самара, Россия

ИСПОЛЬЗОВАНИЕ СВЕРТОЧНЫХ НЕЙРОННЫХ СЕТЕЙ ДЛЯ ОЦЕНКИ ЗАЩИЩЕННОСТИ РЕЧЕВОЙ АКУСТИЧЕСКОЙ ИНФОРМАЦИИ

THE USE OF CONVOLUTIONAL NEURAL NETWORKS FOR ASSESSING THE SECURITY OF SPEECH ACOUSTIC INFORMATION

Аннотация: Работа посвящена рассмотрению существующих архитектур сверточных нейронных сетей и их применение в задачах разборчивости речи. Опробованы экспериментально три архитектуры –

типовая модель, AlexNet и ResNet. Для проверки был создан набор данных, состоящий из мел-частотных кепстральных коэффициентов зашумленных аудиозаписей речи от 20% до 80% разборчивости речи. Исследуемые архитектуры успешно прошли обучение, авторами выделяется архитектура ResNet, так как она достигла высокого процента точности распознавания при относительно низком коэффициенте потерь при обучении.

Ключевые слова: Сверточные нейронные сети, зашумленность аудиозаписи, разборчивость речи, мел-частотные кепстральные коэффициенты, защита речевой акустической информации.

Abstract: The article is devoted to the consideration of existing architectures of convolutional neural networks and their application in speech intelligibility problems. Three architectures have been experimentally tested – the typical model, AlexNet and ResNet. For verification, a data set was created consisting of MFCC of noisy audio recordings of speech from 20% to 80% of speech intelligibility. The studied architectures have been successfully trained, the authors highlight the ResNet architecture, as it has achieved a high percentage of recognition accuracy with a relatively low learning loss coefficient.

Keywords: Convolutional neural networks, audio recording noise, speech intelligibility, mel-frequency cepstral coefficients, protection of speech acoustic information.

Одной из основных задач в сфере обеспечения информационной безопасности является защита акустической речевой информации во время проведения конфиденциальных переговоров. Для развития автоматизации процесса оценки защищенности речевой акустической информации предлагается использовать нейронную сеть, которая работает с распознаванием звука и умеет определять степень зашумленности аудиозаписи.

Согласно последним исследованиям, именно сверточные нейронные сети демонстрируют высокую эффективность в различных задачах распознавания образов и изображений. Наиболее используемые исследователями архитектуры сверточных нейронных сетей являются AlexNet, VGGNet, GoogLeNet и ResNet [1,2,3,4].

Для проведения оценки возможности применения сверточных нейронных сетей в задачах оценки защищенности речевой акустической информации, был осуществлен эксперимент, для которого была собрана обучающая выборка, в которую входят мел-частотные кепстральные коэффициенты, широко применяемые для составления характеристик речевых сигналов [5].

Для исследования мы ограничились записью голоса одного диктора – мужчины со средним тембром голоса. Прежде чем проводить запись речи диктора определили следующие параметры получаемых аудиодорожек: формат аудиозаписи - WAV; частота дискретизации аудиозаписи - 19531 Гц; длительность аудиозаписи - 10 секунд. Необходимо отметить, что за 10 секунд диктор смог сказать 25 русских слов, что соответствует 100% разборчивости речи.

Набор данных состоит из мел-частотных кепстральных коэффициентов зашумленных аудиозаписей речи диктора. При помощи Adobe Audition сгенерировали 36 вариаций белого шума, получая разный уровень шума. Каждый вариант белого шума был наложен на аудиозапись речи диктора с таким отношением сигнал/шум, чтобы зашумленные аудиозаписи речи были равны от 20% до 80% разборчивости речи с шагом в 10%. Такой процент разборчивости речи был получен при помощи прослушивания аудиозаписей одним экспертом. Таким образом, было получено 252 зашумленных аудиозаписи. Для создания обучающей выборки ограничимся следующими параметрами изображений: формат полученного изображения - .PNG; размер изображения составляет 300x300 пикселей [6]. Для корректного обучения нейронной сети мы расширили набор данных путем «отзеркаливания» относительно временной оси полученные изображения. Итого получили 504 образца. Полученный набор данных был разделен на тренировочный набор данных (420 изображений) и тестовый набор данных (84 изображения). В качестве примера на рисунке 1 показаны мел-частотные кепстральные коэффициенты аудиозаписи речи диктора без наложения белого шума длительностью 10 секунд (слева) и мел-частотные кепстральные коэффициенты зашумленной аудиозаписи речи диктора с процентом разборчивости речи равное 50% и длительностью 10 секунд (справа).

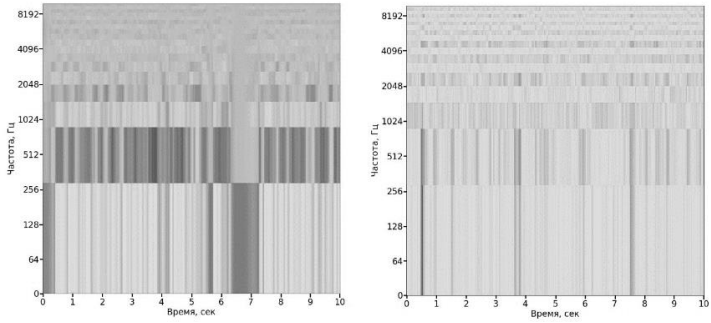

Рисунок 1 – Мел-частотные кепстральные коэффициенты аудиозаписи речи диктора без наложения белого шума (слева) и с наложением шума, равное 50% разборчивости речи (справа)

Так как мы имеем малый набор данных для обучения сверточной нейронной сети, то для проведения эксперимента были рассмотрены три архитектуры – AlexNet, ResNet и типовая модель сверточной нейронной сети, отличие которой заключается в том, что она состоит из трех сверточных слоев, двух полносвязных слоев и выходного слоя. В первом скрытом сверточном слое используется 96 фильтров размером 3x3, во втором - 256 фильтров размером 3x3, в третьем - 384 фильтра размером 3x3. Фильтры применяются с шагом в 2 пикселя. В каждой исследуемой архитектуре используется нелинейная функция активации и стохастический градиентный спуск в качестве оптимизационного алгоритма. Полносвязные слои имеют 64 нейрона каждый.

Параметром для выявления успешного обучения является процент точности распознавания нейронной сетью, который должен быть больше 90% [7,8]. Также будем опираться на количество эпох, затраченных на обучение нейронной сети, коэффициент потерь при обучении и время обучения. В таблице 1 показаны результаты обучения сверточных нейронных сетей.

Таблица 1 – Результаты обучения сверточных нейронных сетей

Архитектура сверточной нейронной сети	Процент точности распознавания нейронной сетью, %	Количество эпох, затраченных на обучение	Коэффициент потерь при обучении	Время обучения, минут
Типовая модель	90,23	11	0,3576	3 минуты 7 секунд
AlexNet	92,86	9	0,3169	1 минута 48 секунд
ResNet	97,61	8	0,1342	4 минуты 16 секунд

Опираясь на полученные результаты можно сказать, что сверточные нейронные сети успешно справляются с распознаванием процента разборчивости речи на мел-частотных кепстральных коэффициентах зашумленной аудиозаписи речи диктора. В данной работе стоит выделить архитектуру ResNet, так как процент точности распознавания нейронной сетью достиг 97,61, коэффициент потерь при обучении составил 0,1342. В данном случае такая архитектура уступает во времени обучения другим исследованным архитектурам, но превосходит по остальным исследуемым параметрам.

В дальнейшем предлагается расширить набор данных – записать речь дикторов с мужскими и женскими голосами разных тембров. Также для расширения набора данных необходимо добавить такой вид помехи

как розовый шум. Таким образом появится возможность исследовать такие архитектуры сверточной нейронной сети как VGGNet и GoogLeNet. Результаты данного исследования могут быть использованы для совершенствования процесса оценки защищенности речевой акустической информации.

Список использованных источников:

1. ImageNet classification with deep convolutional neural networks / A. Krizhevsky, I. Sutskever, G.E. Hinton // Communications of the ACM. – 2012. – № 60. – P.84 - 90.
2. Simonyan K. Very Deep Convolutional Networks for Large-Scale Image Recognition / K. Simonyan, A. Zisserman //3rd International Conference on Learning Representations (ICLR 2015), Computational and Biological Learning Society. – 2015. – P. 1–14
3. Going deeper with convolutions / Szegedy C., [et al.] // 2015 IEEE Conference on Computer Vision and Pattern Recognition (CVPR), Boston, MA, USA, 2015. - P. 1-9.
4. Deep Residual Learning for Image Recognition [Электронный ресурс] URL: https://arxiv.org/pdf/1512.03385.pdf (Дата обращения: 04.04.2024).
5. Tyagi V., Wellekens C. On desensitizing the Mel-cepstrum to spurious spectral components for robust speech recognition // Proceedings (ICASSP '05). IEEE International Conference on Acoustics, Speech, and Signal Processing. 2005. P. 1–21.
6. Волков, Н.А. К вопросу оценки защищенности речевой акустической информации с применением сверточной нейронной сети / Н.А. Волков, А.В. Иванов // Перспектива-2023: материалы X Всероссийской молодежной школы-семинара по проблемам информационной безопасности, Красноярск, 28 сентября – 01 октября 2023 года. – М.: Издательский дом Академии Естествознания. – 2023. – С. 40-45.
7. Паршин С.Е. Исследование параметров алгоритмов распознавания лиц // Сборник научных трудов НГТУ. – 2019. – № 1 (94). – С. 55–70.
8. Simple MNIST convnet – KERAS [Электронный ресурс]. URL: https://keras.io/examples/vision/mnist_convnet/ (дата обращения 09.04.2024).

УДК 004.056

А.Э. Габитов
Уфимский университет
науки и технологий, Уфа, Россия

Научный руководитель:
В.М. Картак
Уфимский университет
науки и технологий, Уфа, Россия

СРАВНИТЕЛЬНЫЙ ОБЗОР МЕТОДОВ ЗАЩИТЫ ГЕТЕРОГЕННОЙ СРЕДЫ
COMPARATIVE REVIEW OF HETEROGENEOUS ENVIRONMENT PROTECTION METHODS

Аннотация: Работа посвящена сравнению методов защиты гетерогенной среды как актуальной задаче защиты информации во многих организациях с гетерогенной структурой. Приводятся методы базирующиеся на мультиагентном подходе. Рассматривается архитектура систем защиты информации, а также методики обнаружения угроз.

Abstract: The article is devoted to the consideration of methods for protecting a heterogeneous environment as current problems of information security in many organizations with a heterogeneous structure. Methods of manifestation using a multi-agent approach are presented. The architecture of information security systems, as well as methods for detecting threats, are considered.

Ключевые слова: Защита информации, гетерогенная среда, мультиагентный подход, агент обнаружение угроз.

Keywords: Information protection, heterogeneous environment, multi-agent approach, threat detection agent.

Расширение производственных и вычислительных мощностей, возросшая необходимость в оперативной обработке данных и стремление к созданию единой информационной сети привели к интеграции информационно-вычислительных ресурсов. Потоки информации, циркулирующие в такой среде, требуют обработки в реальном времени, что часто затруднено из-за проблем с координацией этих потоков.

Защита каждого компонента программно-аппаратных средств, в гетерогенной информационной сети представляет собой важную задачу информационной безопасности.

В данной статье рассматривается сравнение различных подходов к проектированию систем защиты информации для гетерогенных информационных сетей, основанных на мультиагентном подходе. В этих системах агенты, взаимодействуя друг с другом, решают сложные задачи обеспечения информационной безопасности. Например, обнаружение и предотвращение вторжений, выявление аномалий и их предупреждение являются ключевыми задачами в условиях множества потенциальных угроз.

На текущий момент существует значительное количество публикаций, посвященных разработке систем защиты информации с использованием мультиагентного подхода. Авторы предлагают различные стратегии, включая мультиагентные системы защиты информации, оснащенные механизмами обнаружения вторжений, аномалий и других инновационных подходов к обеспечению информационной безопасности в гетерогенных сетях.

В работе [4] представлено использование множества агентов обнаружения угроз, размещенных на каждом узле информационной сети. Эти агенты могут быть как локальными, так и системными. Архитектура системы защиты информации состоит из четырех уровней абстракции, при этом четвертый уровень содержит агентов обнаружения угроз, распределенных по агентским платформам. Получение информации об угрозах происходит на каждом узле сети, а совокупность этих данных формирует базу знаний мультиагентной системы защиты. Такой подход позволяет применять индивидуальные методы выявления и ликвидации угроз на каждом узле сети. Взаимодействие между узлами осуществляется через транспортную подсистему сетевого взаимодействия, использующую стек протоколов TCP/IP на транспортном уровне.

Однако важно отметить, что существует множество других подходов к защите информации, включая работу [5], которая предлагает использование мультиагентной системы защиты информации на различных уровнях сетевой инфраструктуры. Каждый агент обеспечивает специфические функции, начиная от мониторинга и реагирования на угрозы до аутентификации и авторизации. Такой гибкий подход обеспечивает эффективную защиту на всех уровнях сетевой инфраструктуры, сохраняя при этом высокий уровень безопасности.

В исследовании [6] описывается применение мультиагентной системы защиты в гетерогенной среде, представленной кластером серверов с виртуальными машинами, работающими на одном гипервизоре. Защита информации обеспечивается путем контроля как внутреннего, так и внешнего виртуального трафика. Этот контроль осуществляется с помощью встроенных в гипервизор виртуальных межсетевых экранов (агентов), действующих независимо от пользовательских виртуальных

машин. Технология "Стелс" позволяет контролировать пакетный трафик незаметно для остальных компонентов сети.

Мультиагентная система защиты информации обладает консолью управления политиками доступа, что позволяет распространять новые правила политики на все компоненты гетерогенной среды при их изменении. Этот подход обеспечивает защиту как от внешних, так и от внутренних угроз. Каждый агент в системе не имеет централизованного управления виртуальными машинами и не способен самостоятельно функционировать в рамках всей системы защиты информации.

В данном исследовании были рассмотрены современные подходы к созданию систем защиты информации, основанные на мультиагентном подходе. Несмотря на их многочисленные преимущества, эти подходы, как правило, ориентированы на решение конкретных задач, не предоставляя комплексного решения проблемы информационной безопасности в гетерогенных средах. Это означает, что для достижения полной защиты информации требуется радикальное изменение подхода к обеспечению безопасности в таких сетях.

Список использованных источников:

1. Гильфанов, К.Х. Информационные сети и телекоммуникации [Текст] / К.Х. Гильванов. – Казань: Казанский государственный энергетический университет, 2014. – 364 с.

2. Мачульский, Е.В. Задачи обеспечения информационной безопасности в гетерогенных сетях хранения данных / Е. В. Мачульский // Научное периодическое издание «IN SITU». – 2015. – № 4. – С. 44-46.

3. Городецкий В.И. Многоагентные системы: современное состояние исследований и перспективы применения // Новости искусственного интеллекта. – 1996. – № 1. – С. 44-59.

4. Шниперов, А.Н. Разработка системы защиты информации для гетерогенных информационных систем на основе мультиагентного подхода / А.Н. Шниперов, Е.А. Сантьев // Информатика и системы управления. – 2014. – №1(39). – С. 23-34.

5. Ляпустин, А.Е. Безопасность мультиагентной платформы // А.Е. Ляпустин // Программные системы и вычислительные методы. – 2017. – № 3. – С. 16-24.

6. Архитектура системы разграничения доступа к ресурсам гетерогенной вычислительной среды на основе контроля виртуальных соединений / В.С. Заборовский, А.А. Лукашин, С.В. Купреенко, В.А. Мулюха // Вестник УГАТУ. – 2011. – Т. 15. – № 5(45). – С. 170-174.

УДК 004

А.А. Гаврилова
Уфимский университет
науки и технологий, Уфа, Россия

Научный руководитель:
А.Ф. Фатхелисламов
Уфимский университет
науки и технологий, Уфа, Россия

ГЕНЕРАЦИЯ ПАКЕТОВ ТРАФИКА ДЛЯ МОДЕЛИРОВАНИЯ СЕТЕВЫХ АТАК
GENERATING TRAFFIC PACKETS TO SIMULATE NETWORK ATTACKS

Аннотация: В статье рассматривается проблема сетевых атак. Особое внимание уделяется DDoS-атакам, их разновидностям и методам предотвращения. Приводится пример моделирования DDoS-атаки с использованием программы LOIC. Анализируются последствия атаки. Предложен вариант защиты.

Abstract: The article discusses the problem of network attacks. Special attention is paid to DDoS attacks, their types and methods of prevention. An example of a DDoS attack simulation using the LOIC program is given. The consequences of the attack are analyzed. A protection option is proposed.

Ключевые слова: Сетевые атаки, DDoS-атаки, моделирования сетевых атак, генерация пакетов трафика.

Keywords: Network attacks, DDoS attacks, network attack simulations, traffic packet generation.

В современном мире сетевые атаки становятся все более распространенным явлением, угрожая безопасности информационных систем и конфиденциальных данных. Чтобы противостоять этим угрозам, необходимо понимать, как действуют злоумышленники, и готовиться к нападениям заранее.

Сетевая атака представляет собой целенаправленные действия злоумышленников, направленные на захват управления над ПК с целью нарушения функционирования сети, изменения прав доступа, кражи конфиденциальных данных или осуществления других разрушительных воздействий на информацию. Для осуществления таких атак может использоваться как программные, так и аппаратные решения, что позволяет третьим лицам добиться своих целей вредоносными методами[1].

Один из самых эффективных способов защиты от таких атак — моделирование. Сделать это можно, создавая различные типы сетевого трафика, которые имитируют реальные атаки. Таким образом, мы можем проанализировать, как эти атаки повлияют на нашу инфраструктуру, и выработать действенные меры по их устранению, минимизации потенциальных негативных исходов.

DDoS – это распределённая атака на вычислительную систему с целью довести её до отказа.

Некоторые виды DDoS атак:

1. Атака на уровне пропускной способности. Злоумышленники отправляют запросы, требующие установления соединения, одновременно с множества источников, что перегружает сервер.

2. Атака на уровне протоколов. Атакующие отправляют запросы на сервер, похожие на легитимные. Это заставляет сервер тратить дополнительные ресурсы на обработку недействительных запросов, что может привести к отказу в обслуживании.

3. Атака на уровне приложения. Злоумышленники направляют запросы на определённые уязвимые участки программного обеспечения (например, веб-сайт или API), которые требуют интенсивной обработки, что вызывает перегрузку сервера и привести к его недоступности.

Предположим, что злоумышленник находится вне сети, которая будет проводиться из «внешней» среды. Для этого использована хостовая система с гипервизором и виртуальным сервером. Для обеспечения связи между компьютерами в разных сетях, подключенных к одному роутеру, была настроена статическую маршрутизацию.

При моделировании атаки работали с программой LOIC для DDoS-атак на сети. Для имитирования атаки был введён IP-адрес целевого сервера для инициации атаки, применялся протокол UDP, количество потоков - тысяча [2].

После проверки доступности сервера, было замечено, что сервер стал недоступен из-за забитого паразитным трафиком канала передачи данных. Время атаки составило примерно четыре минуты, за которые наблюдалась недоступность всей сети, увеличение времени ответа от сервера и потеря пакетов. Ресурсы сервера недостаточны из-за высокой нагрузки от виртуального оборудования в сети.

Отправили icmp-запрос на устройство в моделируемой сети через указанный порт для проверки его доступности. По результатам проверки видно, что сервер недоступен, потребовалось его перезагрузка для восстановления доступа.

UDP-протокол работает над IP-протоколом, где отсутствует процесс установления связи. Он передает данные без слежки за их целостностью, просто отправляя их по сети в форме отдельных пакетов. Это создаёт

возможность изменить IP-адрес отправителя, что даёт им шанс использовать одно устройство для генерации множества запросов. В результате, получатель начинает обрабатывать не один запрос, а множество запросов с подменёнными IP-адресами отправителя. В течение данной атаки хакер создаёт множество пакетов максимального объёма и отсылает их на сервер. В этот момент брандмауэр сервера не реагирует на такие пакеты, поскольку они заполняют пропускную способность между граничным маршрутизатором и сетевым интерфейсом [3].

Проблема, возникающая в связи с защитой этой атаки, заключается в неэффективном блокировании запросов с использованием IP-адресов из-за подмененных IP-адресов. При вероятности атаки на UDP-порт, становится трудно защититься, поскольку отключение этого порта может нарушить работу сервиса. Фрагментированный флуд UDP не похож тем, что злоумышленник отправляет пакет на устройство жертвы, указывая, что это только его часть. В результате устройство выделяет ресурсы для создания пакета, но остальные фрагменты не доходят. Отбрасывая слишком большие пакеты, вы можете защититься от данных атак. Специальное программное обеспечение используется для анализа сетевого трафика и обнаружения необычной активности и запросов.

Список использованных источников:

1. Сетевые атаки на основе машинного обучения / А.В. Лапшакова, А.М. Милютина, Д.Х. Джураева, Н.И. Халявин // Наука и образование в эпоху перемен: перспективы развития, новые парадигмы: материалы X Всероссийской научно-практической конференции, Ростов-на-Дону, 15 июля 2022 года. Том Часть 1. – Ростов-на-Дону: ООО «Манускрипт», 2022. – С. 44-47.

2. Вахитова, Э.М. Моделирование сетевых атак в условиях учебной лаборатории / Э.М. Вахитова // Информационные технологии обеспечения комплексной безопасности в цифровом обществе: сборник материалов VI Всероссийской молодежной научно-практической конференции с международным участием, Уфа, 19-20 мая 2023 года. – Уфа: Уфимский университет науки и технологий, 2023. – С. 71-73.

3. Ломакин, А.Ю. Способы и методы защиты от DDOS-атак в современных условиях / А.Ю. Ломакин, О.А. Ивлев // Защита информации: IT, правовые и экономические аспекты: сборник научных трудов Межвузовской студенческой научно-практической конференции, Москва, 16–17 марта 2023 года. – Москва: МИРЭА – Российский технологический университет, 2023. – С. 133-136.

УДК 004.738.5

Н.В. Гулякин, И.Ю. Денисов
Стерлитамакский филиал
Уфимского университета, Стерлитамак, Россия

Научный руководитель:
Ю.А. Гнатенко
Стерлитамакский филиал
Уфимского университета, Стерлитамак, Россия

КОРПОРАТИВНЫЙ МЕССЕНДЖЕР С ПРИМЕНЕНИЕМ КРИПТОГРАФИЧЕСКОГО МЕТОДА ШИФРОВАНИЯ
CORPORATE MESSENGER USING CRYPTOGRAPHIC ENCRYPTION METHOD

Аннотация: Статья анализирует применение алгоритма AES и режима CBC в разработке корпоративного мессенджера для обеспечения безопасности передачи данных. Освещаются технические детали реализации и ключевые аспекты шифрования.

Abstract: The article analyzes the application of the AES algorithm and the CBC mode in the development of a corporate messenger to ensure the security of data transmission. The technical details of the implementation and key aspects of encryption are highlighted.

Ключевые слова: Мессенджер, шифрование, AES, CBC, безопасность, Python, корпоративная коммуникация.

Keywords: Messenger, encryption, AES, CBC, security, Python, corporate communication.

В условиях современной информационной среды защита данных является приоритетной задачей для корпоративных систем. Разработка мессенджера с использованием шифрования на основе AES и CBC позволяет эффективно решать задачи по обеспечению конфиденциальности и целостности данных. Архитектура мессенджера использует стандартный подход «клиент-сервер» с шифрованием на обеих сторонах для обеспечения безопасной передачи сообщений между пользователями.

Алгоритм AES (Advanced Encryption Standard) был выбран за его надежность и широкое применение в индустрии. AES — это симметричный алгоритм блочного шифрования, что означает использование одного и того же ключа для шифрования и расшифровки данных. Он поддерживает ключи длиной 128, 192 и 256 бит, обеспечивая высокий уровень защиты [1].

Режим блочного шифрования CBC (Cipher Block Chaining) включает в себя механизм, при котором каждый блок открытого текста перед шифрованием комбинируется с предыдущим зашифрованным блоком. Это обеспечивает то, что одинаковые блоки текста, зашифрованные одним и тем же ключом, приведут к разным зашифрованным блокам, увеличивая тем самым безопасность передачи данных [2].

Процесс шифрования в CBC:

Генерация IV: для первого блока текста требуется инициализирующий вектор, который должен быть случайным и уникальным для каждой сессии шифрования.

XOR-операция: каждый блок открытого текста объединяется с помощью операции XOR с предыдущим зашифрованным блоком. Для первого блока вместо предыдущего зашифрованного блока используется вектор IV.

Шифрование блока: результат XOR-операции шифруется с использованием ключа AES.

В ходе данной работы была разработана программа корпоративного мессенджера, использующего алгоритм AES в режиме CBC для шифрования данных. Это решение обеспечивает высокий уровень безопасности корпоративной коммуникации, что подтверждается как теоретическими разработками, так и практическими испытаниями системы.

Применение симметричного алгоритма шифрования AES, признанного одним из самых надежных в мире, в сочетании с режимом CBC, позволило создать мощную защиту от множества видов атак. Режим CBC, использующий метод цепочечного шифрования блоков с предварительным смешиванием каждого блока с предыдущим шифрованным блоком, значительно увеличивает сложность задачи для потенциального атакующего, пытающегося расшифровать сообщения без знания ключа.

Особое внимание в проекте было уделено генерации и хранению ключей шифрования, а также безопасной инициализации инициализирующих векторов (IV), что является критически важным для предотвращения утечки информации и повторения атак. Система разработана с возможностью легкой интеграции в существующую инфраструктуру компании и предоставляет удобные инструменты для управления и аудита безопасности передаваемых сообщений.

Результаты тестирования программы показали, что использование AES в режиме CBC способствует значительному повышению уровня защиты данных. Программа успешно справляется с задачами по обеспечению конфиденциальности, целостности и аутентичности

сообщений, что делает её надежным инструментом в борьбе с киберугрозами.

Таким образом, внедрение данной технологии не только способствует защите от различных видов атак, включая атаки с изменением сообщений и атаки повторения, но и гарантирует высокий уровень целостности и конфиденциальности корпоративных данных. Разработанный корпоративный мессенджер является значительным вкладом в повышение общей информационной безопасности предприятия, поддерживая устойчивость бизнес-процессов к возможным информационным угрозам.

Список использованных источников:

1. Иванов И.И. Безопасные корпоративные коммуникации / И.И. Иванов, Москва, 2023.

2. Петров П.П. Криптографические методы в информационной безопасности // Журнал "Безопасность и защита информации, № 2. 2022.

УДК 004.056.53

А.И. Гумерова, А.Д. Назарова
Стерлитамакский филиал
Уфимского университета, Стерлитамак, Россия

Научный руководитель:
С.В. Викторов
Стерлитамакский филиал
Уфимского университета, Стерлитамак, Россия

ТЕСТИРОВАНИЕ САЙТОВ НА ФИШИНГ МЕТОДОМ НЕЙРОСЕТЕВОГО АНАЛИЗА
TESTING INTERNET SITES FOR PHISHING BASED ON NEURAL NETWORK ANALYSIS METHOD

Аннотация: В статье приводится описание разработки приложения с использованием машинного обучения для проверки веб-сайтов на наличие фишинговых угроз. Приложение позволяет по URL-адресу тестировать сайты на фишинг. Разработанное приложение представляет собой эффективный инструмент для обеспечения безопасности онлайн-пространства и защиты пользователей от киберугроз.

Abstract: The article describes the development of an application using machine learning to scan websites for phishing threats. The application allows you to test sites for phishing using a URL. The developed application is an effective tool for ensuring the security of the online space and protecting users from cyber threats.

Ключевые слова: Машинное обучение, нейронная сеть, фишинг, кибербезопасность, киберугрозы.

Keywords: Machine learning, neural network, phishing, cybersecurity, cyberthreats.

Фишинг-атаки остаются одной из наиболее распространенных угроз в онлайн-среде, поскольку они основаны на социальной инженерии и могут обмануть даже опытных пользователей. В связи с этим необходимо постоянно развивать новые методы и средства защиты от таких атак. Существуют следующие методы фишинг-атак [1]: фишинг через электронную почту, социальная инженерия, смс-фишинг, вредоносные вложения, фишинг-сайты. Последние являются одним из самых распространенных методов. Вследствие этого возникла потребность разработать приложение с использованием машинного обучения для проверки сайтов на фишинг.

Для обучения нейронной сети был использован датасет Webpage Phishing Detection. Набор данных предназначен для использования в качестве тестов для систем обнаружения фишинга на основе машинного обучения. В нем содержатся данные 11430 фишинговых и легитимных URL-адресов с 87 извлеченными признаками. Признаки относятся к трем разным классам: 56 извлекаются из структуры и синтаксиса URL-адресов, 24 извлекаются из содержимого соответствующих страниц и 7 извлекаются путем запроса внешних служб. Эти признаки включают в себя различные характеристики веб-страниц, такие как length_url (полная длина URL), nb_com (количество «.com» в адресной строке), domain_in_title (наличие домена URL-адреса в названии веб-страницы), domain_age (возраст домена в днях), google_index (индекс Google), page_rank (значение рейтинга страницы Google от Openpagerank) и другие.

Для обработки данных, обучения нейронной сети и извлечения признаков с URL-адреса были написаны специальные функции на языке программирования Python. Обучение нейросети проводилось с использованием модели Random Forest, которая хорошо справляется с задачами классификации на больших объемах данных.

Приложение было реализовано в среде разработки PyCharm [2]. Основной функционал включает в себя возможность ввода URL-адреса в специальное поле для проверки на фишинг (рис. 1).

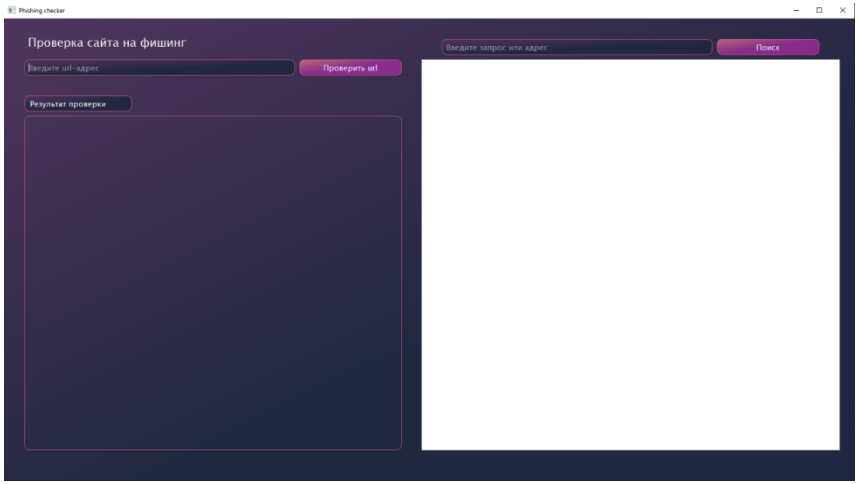

Рисунок 1 – Приложение для проверки URL-адресов на фишинг

После ввода адреса приложение анализирует его с помощью обученной нейронной сети и выводит результат – является ли сайт подозрительным на фишинг или нет и извлеченные с сайта признаки, и их значения (чтобы опытные пользователи могли сами решить, является сайт легитимным или нет) (рис. 2 а)).

Дополнительно в приложении реализовано окно браузера, позволяющее пользователям посещать веб-сайты непосредственно из приложения и проверять их на фишинг (рис. 2 б)). Результат проверки сайта из браузера представлен на рисунке 3. Внедренный в приложение браузер обеспечивает удобство его использования и позволяет быстро проверять подозрительные ресурсы.

Разработанное приложение с использованием машинного обучения для проверки сайтов на фишинг представляет собой важный инструмент в борьбе с киберугрозами в онлайн-среде. Его использование помогает защитить пользователей от потенциальных атак и повысить общий уровень безопасности в интернете.

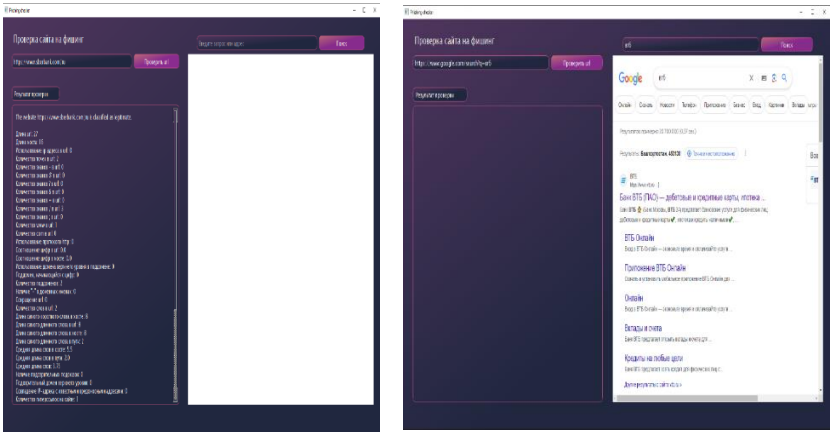

Рисунок 2 – Фрагменты интерфейса отображения результатов:
а) проверки введенного адреса; б) использования браузера

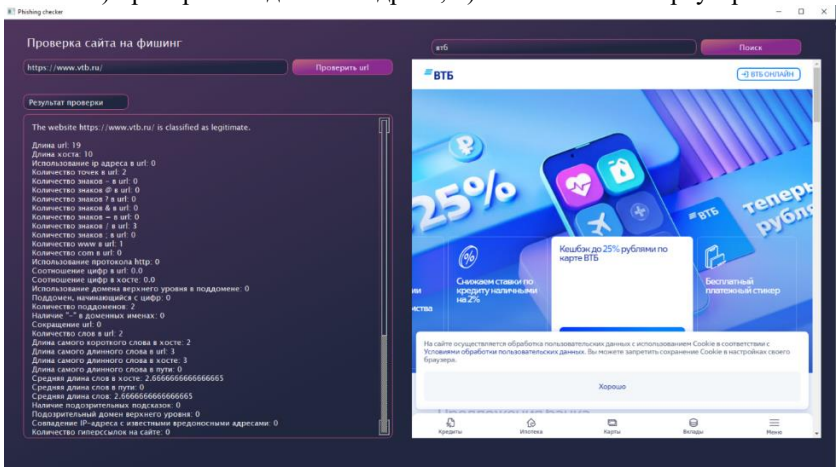

Рисунок 3 – Результат проверки сайта из браузера

Список использованных источников:

1. Вепрев С.Б., Нестерович С.А. Методы фишинговых атак на электронную почту и способы защиты от них // Вестник российского нового университета. Серия: сложные системы: модели, анализ и управление, № 2, 2021. С. 91–100.

2. Бухаров Т.А., Нафикова А.Р. Обзор языка программирования Python и его библиотек // Colloquium-jornal #3(27), 2019 / Technical Science, С.23-25.

УДК 004

Б.М. Давлетшин, В.О. Клыгин
Уфимский университет
науки и технологий, Уфа, Россия

Научный руководитель:
Д.С. Юнусова
Уфимский университет
науки и технологий, Уфа, Россия

ОПРЕДЕЛЕНИЕ ФИШИНГОВЫХ ВЕБ-СТРАНИЦ С ПОМОЩЬЮ МАШИННОГО ОБУЧЕНИЯ
IDENTIFYING PHISHING WEB PAGES USING MACHINE LEARNING

Аннотация: В статье рассматривается применение методов машинного обучения для обнаружения фишинговых веб-страниц. Рассматриваются методы распознавания и наиболее часто используемые приемы злоумышленников для создания угроз данного типа.

Abstract: The paper discusses the application of machine learning methods to detect phishing web pages. The methods of recognition and the most frequently used techniques of attackers to create threats of this type are considered.

Ключевые слова: Фишинг, кибератака, искусственный интеллект, машинное обучение.

Keywords: Phishing, cyberattack, artificial intelligence, machine learning, creating threats of this type.

В эпоху цифровизации нашей повседневной жизни интернет стал неотъемлемой частью нашего существования, проникнув во все сферы нашей жизни и превратив обычные процессы в онлайн-формат: от покупок товаров и услуг до обработки документов и общения в социальных сетях. Все эти привычные действия стали доступными в виртуальном мире, предоставляя нам удобство и быстроту в каждом шаге.

Однако, с ростом числа пользователей интернета возрос и интерес злоумышленников к ценной информации, которую мы оставляем на различных веб-ресурсах. Этот интерес привел к распространению фишинговых атак - одному из наиболее распространенных методов кибератак. Фишинг использует ловушки в виде поддельных веб-сайтов, чтобы заполучить личные данные пользователей [1]. Фишинг отличается от других способов хакерских атак тем, что злоумышленники активно

манипулируют базовыми человеческими эмоциями, такими как любопытство и страх, и также используют информацию, которую смогли собрать из открытых источников о человеке. Этот метод делает фишинговые атаки особенно эффективными, так как они заставляют пользователей доверять поддельным веб-сайтам или электронным сообщениям, не подозревая о возможной угрозе [2].

Одним из серьезных вызовов, связанных с обнаружением фишинговых сайтов, является их схожесть с оригинальными ресурсами. Злоумышленники уделяют большое внимание деталям, таким как дизайн, логотипы, цветовая гамма и даже URL-адреса, чтобы сделать поддельные страницы максимально похожими на реальные. Это создает благоприятные условия для успешной реализации фишинговых атак, поскольку пользователи могут без подозрений предоставлять свои чувствительные данные на фальшивых сайтах.

Определение фишингового сайта требует комплексного подхода. Методы машинного обучения позволяют проводить анализ URL-адреса эффективнее и быстрее человека. Одним из способов выявления подозрительных URL-адресов является анализ специальных символов и их количества.

Для обучения был использован объединенный набор данных из двух датасетов. Первый содержал 11 430 URL-адресов и 87 извлеченных признаков. Набор данных был сбалансирован: в нем было ровно по 50% фишинговых и законных URL-адресов.

Второй включал набор экземпляров веб-сайтов, включающих как законные, так и фишинговые. Каждый веб-сайт был описан с помощью набора признаков, указывающих на его статус. Полный вариант второго набора данных включал 88 647 экземпляров, из которых 58 000 были законными веб-сайтами (помеченными как 0), а 30 647 - фишинговыми (помеченными как 1). Общее количество признаков составляло 111.

Результирующий набор данных является результатом объединения двух первоначальных датасетов с идентичными признаками. Однако в него не включены все признаки из обоих исходных наборов данных, чтобы сосредоточиться на наиболее важных среди них и избежать избыточности. Результирующий набор данных предоставляет полное представление об общих особенностях двух первоначальных наборов данных, сохраняя при этом упрощенный и целенаправленный состав признаков.

Результирующий набор данных включает следующие признаки:

– длина URL: обычно подлинные сайты имеют более короткие URL, чем фальшивые, хотя это не всегда так;

– количество точек: большое количество точек может указывать на поддомены, что не обязательно является признаком фишингового сайта, но может быть использовано вместе с другими признаками для оценки;

– количество дефисов: фальшивые сайты могут содержать много дефисов в попытке имитировать официальные домены;

– наличие специальных символов: (например, ?, =, @, !, #, $, %): некоторые специальные символы могут указывать на фишинговые попытки, особенно если они используются в странных контекстах;

– количество пробелов: нормальные URL обычно не содержат пробелы, и их наличие может быть признаком фишинга;

– наличие символов переданных (например, &, *, +): подозрительные символы могут использоваться в попытках обмана, особенно если они используются не в типичных для URL контекстах;

– наличие символов перенаправления (например, <, >): фишинговые сайты могут пытаться использовать символы перенаправления для ведения пользователей на другие сайты без их согласия.

В таб. 1 представлены результаты методов машинного обучения для решения данной задачи.

Таблица 1 – Результаты методов машинного обучения

Название метода	Точность на обучающем наборе данных	Точность на тестовом наборе данных
Decision Tree	0.9085	0.8768
Random Forest	0.9085	0.8821
Adaboost	0.8707	0.8729
Catboost	0.8967	0.8829
XGboost	0.8954	0.8809

Исходя из результатов, методы Random Forest и Catboost демонстрируют более высокую обобщающую способность, так как достигли более высокой точности на тестовом наборе данных по сравнению с остальными методами.

Обучение и развертывание искусственного интеллекта (ИИ) сталкиваются с проблемами данных, интерпретации моделей и техническими ограничениями. Недостаточность, несбалансированность или не представительность данных могут снизить производительность моделей. Сложность интерпретации решений, особенно нейронных сетей, затрудняет объяснение принятых решений. Неконтролируемое использование ИИ может привести к непредвиденным последствиям. Технические проблемы, такие как отсутствие стандартов и сложность масштабирования, также затрудняют разработку ИИ. После развертывания модели требуется постоянное обслуживание и обновление. Учитывая все

это, разработка и внедрение моделей ИИ требуют внимательного анализа и управления рисками.

Список использованных источников:

1. Митюков Е.А. Жизненный цикл фишинговых атак и техники их реализации // Решение. 2019. Т. 1. С. 140–142.

2. Гарбин, А. Н. Машинное обучение: методы, алгоритмы и задачи / А. Н. Гарбин. – М.: Издательский дом «Лань», 2020. – С. 352.

3 Колесникова, Н.В. Фишинг: методы обнаружения и защиты / Н.В. Колесникова, А.М. Марков. – СПб.: БХВ-Петербург, 2019. – С. 256.

УДК 004

Т.П. Коробко
Уфимский университет
науки и технологий, Уфа, Россия

Научный руководитель:
Д.С. Юнусова
Уфимский университет
науки и технологий, Уфа, Россия

ЗАПРЕЩЕННЫЙ ТЕКСТОВЫЙ КОНТЕНТ В СЕТИ ИНТЕРНЕТ И ЕГО ВЫЯВЛЕНИЕ ПРИ ПОМОЩИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА
PROHIBITED TEXTUAL CONTENT ON THE INTERNET AND ITS DETECTION BY ARTIFICIAL INTELLIGENCE

Аннотация: В данной статье рассматривается значимость разработки системы для выявления запрещенного текстового контента в сети Интернет с использованием методов искусственного интеллекта. Освещаются основные методы анализа текста и принципы работы систем.

Abstract: This paper discusses the significance of developing a system for detecting banned text content on the Internet using artificial intelligence methods. The basic methods of text analysis and principles of systems operation are covered.

Ключевые слова: Запрещенный контент, текстовый контент, сеть Интернет, искусственный интеллект, обработка естественного языка.

Keywords: Forbidden content, text content, Internet, artificial intelligence, natural language processing.

С развитием сети Интернет и ее активным использованием столкновение с запрещенным текстовым контентом становится все более актуальной проблемой. Среди запрещенного контента можно выделить экстремистские материалы, информацию об изготовлении или получении наркотиков, описание способов совершения суицида, а также призывов к его совершению, распространение ложной информации и другие аспекты [1], которые представляют угрозу как для пользователей Интернета, так и для общества в целом.

Для борьбы с данной проблемой в современном обществе активно исследуется возможность применения искусственного интеллекта для автоматизированного выявления запрещенного текстового контента. Использование алгоритмов машинного обучения и нейронных сетей позволяет разрабатывать эффективные системы, способные анализировать тексты и обнаруживать недопустимый контент. Искусственный интеллект (ИИ) находит широкое применение даже сейчас, например, Роскомнадзор в 2024 году планирует сформировать и начать вести реестр заблокированных сайтов с применением ИИ [2].

Существует множество методов анализа текста с применением искусственного интеллекта, которые позволяют выявлять запрещенный контент. Один из основных подходов – использование алгоритмов машинного обучения для классификации текста на основе обучающих наборов данных с размеченными примерами запрещенного и разрешенного контента.

Анализ текста осуществляется на различных уровнях, включая семантический анализ, извлечение ключевых слов и фраз, определение тональности и эмоциональной окраски текста. Технологии обработки естественного языка (Natural Language Processing, NLP) [3] играют ключевую роль в этом процессе, позволяя системе понимать и интерпретировать текстовую информацию.

Системы для выявления запрещенного текстового контента на основе искусственного интеллекта включают в себя несколько ключевых принципов работы [4].

Сначала текст проходит предварительную обработку, включающую в себя, к примеру, удаление лишних символов, приведение к нижнему регистру, токенизацию и лемматизацию. Это необходимо для стандартизации и оптимизации текста перед его анализом алгоритмами машинного обучения.

Далее происходит этап векторизации, где каждому слову или фразе в тексте присваивается числовое значение, позволяющее алгоритмам машинного обучения работать с текстом. Для этого могут использоваться такие как техники векторизации, как Word2Vec или TF-IDF.

Затем применяются алгоритмы машинного обучения, к примеру, наивный Байес, SVM (Support Vector Machines) или нейронные сети [5], для классификации текста на категории "запрещенный" и "разрешенный". Точность и эффективность системы зависят от обучающего набора данных, правильного подбора признаков и параметров алгоритмов.

После это проводится тестирование, в ходе которого система анализируется на тестовых данных, которые не использовались в процессе обучения. Тестирование позволяет оценить точность и надежность системы выявления запрещенного текстового контента. Результаты тестирования могут показать степень верности классификации текста, а также выявить возможные ошибки или улучшения, которые могут быть внесены в систему для повышения ее эффективности.

Одним из вариантов дальнейшего использования полученной модели для выявления запрещенного текстового контента может быть интеграция в уже существующие онлайн-платформы для возможности быстрой обработки и анализа текста в реальном времени, что позволит оперативно реагировать на появление негативного контента и предотвращать его дальнейшее распространение.

Таким образом, использование новейших технологий, таких как обработка естественного языка и применение искусственного интеллекта, открывает новые перспективы для эффективной борьбы с негативным контентом в сети. Важно продолжать улучшать системы выявления запрещенного текстового контента, совершенствуя алгоритмы и методы анализа данных, а также активно проводить тестирования и обновления обучающих наборов данных.

Список использованных источников:

1. Единый реестр запрещённых сайтов // Википедия URL: https://ru.wikipedia.org/wiki/Единый_реестр_запрещённых_сайтов (дата обращения: 02.04.2024).

2. Роскомнадзор использует ИИ для блокировок сайтов // Коммерсантъ URL: https://www.kommersant.ru/doc/6635402 (дата обращения: 14.04.2024).

3. Обработка естественного языка // Википедия URL: https://ru.wikipedia.org/wiki/Обработка_естественного_языка (дата обращения: 16.04.2024).

4. Свидетельство о государственной регистрации программы для ЭВМ № 2023617147 Российская Федерация. Программное обеспечение для

выявления противоправного контента: № 2023616049: заявл. 28.03.2023: опубл. 05.04.2023 / Р.Ф. Исмагилов, Н.Д. Лушников, А.С. Исмагилова; заявитель федеральное государственное бюджетное образовательное учреждение высшего образования «Уфимский университет науки и технологий».

5. Основные модели машинного обучения // БлогЯПрактикума URL: https://practicum.yandex.ru/blog/modeli-mashinnogo-obucheniya/ (дата обращения: 19.04.2024).

УДК 004

О.А. Кунавина, К.С. Забара
Уфимский университет
науки и технологий, Уфа, Россия

Научный руководитель:
А.Ф. Фатхелисламов
Уфимский университет
науки и технологий, Уфа, Россия

ТЕХНОЛОГИЯ ПЕРЕХВАТА И АНАЛИЗА ТРАФИКА В БЕСПРОВОДНЫХ СЕТЯХ
TECHNOLOGY FOR INTERCEPTING AND ANALYZING TRAFFIC IN WIRELESS NETWORKS

Аннотация: Данная рассматривает технологию перехвата и анализа трафика в беспроводных сетях. Приведены примеры способов перехвата трафика, а также способов защиты.

Abstract: This article examines the technology of interception and analysis of traffic in wireless networks. Examples of ways to intercept traffic, as well as methods of protection are given.

Ключевые слова: Wi-Fi, беспроводная сеть, перехват данных.

Keywords: Wi-Fi, wireless network, data interception**.**

Всем хорошо известно о том, как с каждым днем увеличивается потребность использования беспроводных соединений. Сложность прокладки проводных линий связи повлекла к стремительному распространению беспроводных систем передачи данных. Пользователи, имеющие беспроводной доступ к информации, в любом месте и в любое

время способны выполнить работу более быстро и эффективно, чем пользователи, использующие проводные сети. Стоит отметить, что любая информация, имеющая какую-либо ценность, подвергается угрозе.

Еще одним уязвимым местом становится возможность перехвата управления объектами информационной инфраструктуры. Ежедневно все больше домов, образовательных учреждений, предприятий и общественных мест обеспечивают доступ к интернету через Wi-Fi. Это удобство и свобода передачи данных без физического подключения к сети, безусловно, приносят пользу. При этом Wi-Fi-сети (Wireless Fidelity) несут с собой значительно большее количество угроз, чем обычные проводные сети. Именно поэтому акцентировать внимание на обеспечении безопасности Wi-Fi становится одной из важных задач, учитывая, что персональные данные, а также критически важные системы становятся динамическими в виртуальном пространстве.

Под перехватом и анализом трафика в беспроводных сетях понимается процесс сбора, записи и анализа данных, передаваемых через беспроводные сети. Этот процесс может быть проведен как для целей безопасности и мониторинга сети, так и для злоумышленных целей [1]. Перехват и анализ трафика в Wi-Fi сетях является одним из способов получения информации о пользователях и их действиях в сети.

Перехват трафика в Wi-Fi сетях может осуществляться различными способами. Один из наиболее распространенных методов – это использование снифферов (Sniffers) – это программы, способные перехватить и анализировать сетевой трафик. Снифферы полезны в тех случаях, когда нужно извлечь из потока данных какие-либо сведения (например, пароли) или провести диагностику сети. Такие программы могут быть как законными, предназначенными для анализа безопасности сети, так и злоумышленными, направленными на получение конфиденциальной информации.

В локальных сетях, использующих протокол TCP/IP, для определения физического MAC - адреса хоста по IP - адресу используется протокол разрешения адресов (ARP - Address Resolution Protocol). Протокол ARP хранит на каждом сетевом интерфейсе отдельную ARP - таблицу, которая динамически заполняется информацией о соответствии между IP – адресами и MAC – адресами соседних хостов локальной сети. Динамические записи в ARP – таблице периодически обновляются, а неиспользуемые записи постепенно удаляются из кэша. Основным недостатком протокола ARP является то, что в нем не предусмотрена проверка подлинности отправляемых и принимаемых пакетов. Это позволяет злоумышленнику отправить поддельный ARP - ответ, который не был запрошен атакуемым хостом. Таким образом, злоумышленник может подменить MAC - адрес любого хоста в сети,

намеренно изменив запись в ARP - таблице. Данная атака называется ARP – poison (англ. «отравление» ARP).

Детальный анализ трафика позволяет обнаружить в нем пароли, хэши, идентификаторы сеансов и другую важную информацию [2].

Другой способ перехвата трафика – это установка аппаратных устройств, таких как роутер - устройства, которое получает интернет от провайдера и передает его на устройства, подключенные к внутренней сети. Так же может быть использована точка доступа – это базовая станция, предназначенная для обеспечения беспроводного доступа к существующей сети (беспроводной или проводной) или создания новой беспроводной сети. Данные устройства способны записывать и анализировать передаваемую информацию. Это может быть особенно опасно для корпоративных сетей, где злоумышленники могут получить доступ к важной коммерческой информации.

Анализ трафика позволяет выявить различные уязвимости в сети. Это может быть использовано как злоумышленниками для атак на сеть, так и специалистами по информационной безопасности для защиты от таких атак. Анализ трафика может выявить несанкционированные подключения к сети, использование уязвимых протоколов передачи данных или наличие шифрования, которое не соответствует современным стандартам безопасности [4].

Для защиты от перехвата и анализа трафика в Wi-Fi сетях существует ряд мероприятий. Во-первых, следует использовать надежные методы шифрования данных, такие как WPA2 или более современные стандарты безопасности [3].

Также важно регулярно обновлять программное обеспечение на устройствах сети, чтобы закрыть известные уязвимости.

Кроме того, необходимо контролировать доступ к сети, используя сильные пароли и управление доступом по MAC адресу устройства. Также рекомендуется использовать VPN-сервис для безопасного соединения с сетью из общественных мест.

Таким образом, перехват и анализ трафика в Wi-Fi сетях представляет опасность как для пользователей, так и для организаций. Для защиты от таких угроз необходимо принимать соответствующие меры безопасности и регулярно обновлять системы и программное обеспечение.

Список использованных источников:

1. Мэрритт М., Поллино Д. Безопасность беспроводных сетей / пер. с англ. А.В. Семенова. М., 2020, с. 288.

2. Acrylic Wi-Fi [Электронный ресурс]. URL: https://www.acrylicwifi.com/ru/ (дата обращения: 24.04.2024).

3. CommView – сетевой анализ и мониторинг [Электронный ресурс]. URL: http://www. tamos.ru/products/commview/ (дата обращения: 24.04.2024).

4. Вахитова Э.М. Моделирование сетевых атак в условиях учебной лаборатории / Э.М. Вахитова, А.Ф. Фатхелисламов // Информационные технологии обеспечения комплексной безопасности в цифровом обществе: сборник материалов VI Всероссийской молодежной научно-практической конференции с международным участием, Уфа, 2023. – Уфа: Уфимский университет науки и технологий. 2023. С. 71–73. URL: https:// www.elibrary.ru/item.asp?id=44655451 (дата обращения: 24.04.2024).

УДК 004.724.3

Е.А. Лычагин
Магнитогорский государственный технический университет им. Г.И. Носова, Магнитогорск, Россия

Научный руководитель:
Д.Н. Мазнин
Магнитогорский государственный технический университет им. Г.И. Носова, Магнитогорск, Россия

РАЗРАБОТКА ПРИЛОЖЕНИЯ УСТОЙЧИВОГО К ПЕРЕХВАТУ
DEVELOPMENT OF AN INTERCEPTION-RE SISTANT APPLICATION

Аннотация: Разработка приложение для мгновенного обмена сообщениями с устойчивостью к перехвату. Каждый участник имеет собственное хранилище данных в виде FIFO-очереди, обеспечивая правильный порядок сообщений. Сообщения, генерируемые периодически, могут быть ложными или содержать реальную информацию, обеспечивая анонимность передачи. Работа содержит алгоритм и анализ преимуществ и недостатков в контексте обеспечения безопасной и анонимной связи.

Abstract: The development of an instant messaging application with interception resistance is underway. Each participant has a FIFO queue as their own data repository, ensuring message order. Periodically generated messages can be either false or contain real information, ensuring transmission anonymity.

The work includes an algorithm and analysis of advantages and disadvantages in ensuring secure and anonymous communication.

Ключевые слова: Информационная безопасность, криптография, анонимность, анонимные сети, проектирование систем.

Keywords: Information Security, Cryptography, Anonymity, Anonymous Networks, System Design.

В современном цифровом мире обеспечение безопасности и конфиденциальности данных становится все более важным[3]. Угрозы кибербезопасности постоянно эволюционируют, создавая сложности в обеспечении приватности пользователей в онлайн-среде. Разработка приложения для мгновенного обмена сообщениями, устойчивого к перехвату, приобретает приоритетное значение для организаций и частных лиц, желающих защитить свою личную информацию и обеспечить безопасность связи.

Разрабатываемое приложение основано на алгоритме запутывающей маршрутизации [1] с использованием очередей. В сети каждый участник имеет свою очередь для передачи сообщений, которые проходят через промежуточные узлы, выбирающие случайные маршруты. Дополнительные методы обфускации, такие как шифрование и добавление шума к сообщениям, дополняют процесс, обеспечивая анонимность и конфиденциальность данных в реальном времени.

Этот подход к маршрутизации обеспечивает надежность и безопасность передаваемых сообщений, так как он усложняет их отслеживание и перехват. В случае использования шифрования, данные остаются защищенными от несанкционированного доступа даже в случае утечки или перехвата трафика. Кроме того, добавление шума к сообщениям создает дополнительные сложности для их анализа, делая процесс расшифровки и интерпретации данных намного сложнее для злоумышленников.

Приложение должно обеспечивать безопасность передаваемых данных путем использования ассиметричного шифрования [4]. Каждое сообщение должно быть зашифровано с использованием открытого ключа получателя и дешифровано с использованием его закрытого ключа. Приложение должно обеспечивать аутентификацию узлов для предотвращения подделки сообщений и содержать аутентификационный ключ, подтверждающий подлинность отправителя. Приложение должно быть стабильным и надежным, обеспечивая непрерывную передачу сообщений даже при возникновении сетевых сбоев или ошибок, а также реализовывать механизмы обработки ошибок для обеспечения устойчивости его работы.

Важно отметить, что использование ассиметричного шифрования и механизмов аутентификации узлов гарантирует высокий уровень безопасности передаваемых сообщений. Данные меры обеспечивают конфиденциальность данных и защиту от подделки сообщений, что является критически важным в условиях современных угроз кибербезопасности.

Эти требования являются ключевыми [2] для обеспечения высокого уровня безопасности, надежности и удобства использования разрабатываемого приложения для мгновенного обмена сообщениями.

Помимо анонимности данный алгоритм имеет ряд преимуществ:

Основные преимущества данного приложения:

Маршрутизация через случайные узлы и использование шифрования помогает предотвратить анализ трафика и защитить данные от перехвата и анализа, также данный алгоритм позволяет легко добавлять новых участников в сеть и масштабировать, и данная сеть будет устойчива к отказам поскольку сообщения добавляются в очереди для отправки, а не отправляются на прямую.

К недостаткам [5] можно отнести задержки доставки сообщений из-за использования очередей, но данный недостаток можно достаточно легко исправить. Также использования данного алгоритма может снизить пропускную способность сеть из-за необходимости обработки и маршрутизации данных.

В работе представлен обзор процесса разработки приложения для мгновенного обмена сообщениями, основанного на алгоритме запутывающей маршрутизации. Этот подход обеспечивает безопасность, надежность и анонимность в сетевых коммуникациях. Хотя рассмотрены лишь основные принципы, информация может быть полезна для специалистов в области кибербезопасности и сетевых инженеров. Дальнейшие исследования могут улучшить разработку таких приложений.

Список использованных источников:

1. Алгебра анонимных сетей [Электронный ресурс]. – Режим доступа: https://habr.com/ru/articles/724824/ (Дата обращения: 13.02.2024)

2. Ершов Н., Рязанова Н., Проблемы сокрытия трафика в анонимной сети [Электронный ресурс]. – Режим доступа: https://cyberleninka.ru/article/n/problemy-sokrytiya-trafika-v-anonimnoy-seti-i-faktory-vliyayuschie-na-anonimnost (Дата обращения: 13.02.2024)

3. Каплан Ф., Dark Territory: The secret history of cyber war / Каплан Ф., // Simon & Schuster, 2016. – 352 с.

4. Душкин Р.В., Математика и криптография. Тайны шифров и логического мышления / Душкин Р.В. // АСТ, 2017. – 288 с.

5. Жуньен П., Марсалеск С., practical cryprography for develops / Жуньен П., Марсалеск С. // SoftUni, 2017. – 305 с.

УДК 003.26.09

Д.И. Молчанов
Уфимский университет
науки и технологий, Уфа, Россия

Научный руководитель:
Н.В. Кучкарова
Уфимский университет
науки и технологий, Уфа, Россия

ОБЗОР ПОДХОДОВ К ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ С ИСПОЛЬЗОВАНИЕМ МЕТОДОВ КВАНТОВОЙ КРИПТОГРАФИИ
AN OVERVIEW OF APPROACHES TO INFORMATION SECURITY USING QUANTUM CRYPTOGRAPHY METHODS

Аннотация: Статья освещает вопросы использования технологий квантовой криптографии в задачах обеспечения информационной безопасности цифрового общества. Рассматриваются основные принципы и преимущества этой инновационной технологии, а также потенциал ее развития. В статье подчеркивается роль квантовой криптографии в создании надежных защищенных коммуникационных каналов и обеспечении конфиденциальности данных. Развитие и исследования в области квантовой криптографии представляют собой новую ступень в обеспечении защиты информации при ее передаче по каналам связи.

Abstract: The article highlights the issues of using quantum cryptography technologies in the tasks of ensuring information security of a digital society. The main principles and advantages of this innovative technology, as well as the potential for its development, are considered. The article highlights the role of quantum cryptography in creating reliable secure communication channels and ensuring data confidentiality. The development and research in the field of quantum cryptography represent a new step in ensuring the protection of information when it is transmitted through communication channels.

Ключевые слова: Криптография, квантовая, безопасность, киберугрозы, протоколы, информационная, шифрование, инновации, защита, сети.

Keywords: Cryptography, quantum, security, cyber threats, protocols, information, encryption, innovation, protection, networks.

В цифровом мире кибербезопасность становится все более важной. Классические методы шифрования уязвимы, поэтому необходимо использовать современные методы криптографии. Квантовая криптография обеспечивает надежную защиту передачи данных и обнаружение попыток взлома шифрования, что крайне важно при распространенных кибератаках и утечек информации.

Исследования в области квантовой криптографии активно ведутся в различных странах по всему миру. Ученые работают над созданием новых протоколов, систем квантовой криптографии и надежных квантовых сетей связи для повышения безопасности передачи информации.[1]

Квантовая криптография основана на применении принципов квантовой механики для обеспечения безопасности коммуникаций. Она включает в себя ряд ключевых принципов, таких как принцип суперпозиции, принцип измерения, принцип неопределенности Гейзенберга и принцип взаимосвязи. [2]:

– Принцип суперпозиции: Квантовые объекты, такие как кубиты, могут находиться в неопределенном состоянии до момента измерения.

– Принцип измерения: Измерение квантового объекта изменяет его состояние.

– Принцип неопределенности Гейзенберга: Этот принцип утверждает, что невозможно одновременно точно измерить как координату, так и импульс квантового объекта.

– Принцип взаимосвязи: Квантовые объекты, находящиеся во взаимосвязи (или квантово-связанные), могут быть использованы для создания защищенных ключей шифрования.

Существуют различные протоколы квантовой криптографии:

– квантовое распределение ключей (QKD);
– квантовое шифрование;
– квантовая стеганография [3].

Эти протоколы используют специальные алгоритмы и методы, основанные на квантовых свойствах частиц, для обеспечения безопасной передачи информации и защиты данных от несанкционированного доступа. [4].

Один из наиболее известных протоколов квантовой криптографии - протокол квантового распределения ключей (QKD). Этот протокол генерирует случайные ключи с использованием принципов квантовой механики, что обеспечивает абсолютную надежность ключей и защиту от перехвата информации.

Протокол квантового шифрования использует методы квантовой криптографии, которая основана на использовании квантовых свойств частиц для обеспечения безопасной передачи информации. Квантовое шифрование также предлагает возможность проверки целостности переданных данных, что помогает предотвратить любые попытки их модификации или подделки. Кроме того, квантовое шифрование обладает свойством невозможности перехвата информации без изменения самой информации, что обеспечивает дополнительный уровень безопасности.

Протокол квантовой стеганографии представляет собой метод скрытой передачи информации, который использует квантовые системы для встраивания данных в носитель без изменения его видимого содержимого. Квантовая стеганография позволяет передавать информацию таким образом, что ее присутствие не может быть обнаружено без специальных средств для декодирования. Этот метод шифрования данных может быть использован для обеспечения конфиденциальности и защиты информации от несанкционированного доступа.

Квантовая криптография все еще находится на стадии развития и экспериментов, но уже доступна в виде коммерческих продуктов и услуг. Некоторые компании предлагают квантовую защиту для сетей и передачи данных, обеспечивая конфиденциальность коммуникаций.[5] Также начинают разрабатывать квантово-защищенные устройства и приложения для конечных пользователей, включая смартфоны с квантовой защитой. [6]

Квантовая криптография представляет собой передовое направление в области криптографии, обеспечивая высокий уровень безопасности данных через применение квантовых принципов. Несмотря на вызовы, интенсивные исследования продолжаются, что может привести к улучшению безопасности в цифровой среде и установлению новых стандартов защиты данных в будущем.

Список использованных источников:

1. Нильсен М., Чанг И. Квантовые вычисления и квантовая информация. – М.: Мир, 2006. [Электронный ресурс]. – Режим доступа: https://studizba.com/files/show/djvu/3198-1-m-nil-sen-i-chang--kvantovye.html (дата обращения 14.04.2024).

2. Квантовая криптография Учебное пособие Д.А. Кронберг, Ю.И. Ожигов, А.Ю. Чернявский МГУ имени М.В. Ломоносова, факультет ВМК [Электронный ресурс]. – URL: http://sqi.cs.msu.ru/store/storage/ss8dw5n_quantum_cryptography.pdf (дата обращения 14.04.2024).

3. Квантовая криптография [Электронный ресурс]. – URL: https://ru.wikipedia.org/wiki (дата обращения 14.04.2024).

4. Введение в квантовую криптографию: основные понятия, подходы и алгоритмы Е.Ю. Иванова, Е.И. Ларионцева [Электронный ресурс]. – URL: https://cyberleninka.ru/article/n/vvedenie-v-kvantovuyu-kriptografiyu-osnovnye-ponyatiya-podhody-i-algoritmy/viewer (дата обращения 14.04.2024).

5. А.Ю. Быковский, И.Н. Компанец, Квантовая криптография и комбинированные схемы коммуникационных сетей на ее основе, Квантовая электроника, 2018, том 48, номер 9, 777–801 [Электронный ресурс]. – URL: https://www.mathnet.ru/links/3ceef8a659d6d0b6922f8458b9a8a39a/qe16893.pdf (дата обращения 14.04.2024).

6. Технологии квантовой криптографии Е.А. Долгочуб, А.Н. Поликанин [Электронный ресурс]. – URL: https://cyberleninka.ru/article/n/tehnologii-kvantovoy-kriptografii/viewer (дата обращения 14.04.2024).

УДК 004

М.В. Назаров, Д.М. Акмырадов, Р.М. Насибуллин
Уфимский университет
науки и технологий, Уфа, Россия

Научный руководитель:
А.Ф. Фатхелисламов
Уфимский университет
науки и технологий, Уфа, Россия

АНАЛИЗ РАЗЛИЧНЫХ ТИПОВ ПОДКЛЮЧЕНИЙ НА БЕЗОПАСНОСТЬ С ПОМОЩЬЮ ПРОГРАММЫ WIRESHARK
ANALYZING DIFFERENT TYPES OF CONNECTIONS FOR SECURITY USING WIRESHARK SOFTWARE

Аннотация: В работе проводится комплексный анализ безопасности двух протоколов удалённого доступа: Telnet и SSH. Описываются их преимущества и недостатки, а также даются рекомендации по выбору наиболее безопасного варианта. Особое внимание уделяется применению сетевого анализатора Wireshark для оценки уязвимостей различных типов подключений.

Abstract: The work conducts a comprehensive analysis of the security of two remote access protocols: Telnet and SSH. Their advantages and disadvantages are described, and recommendations are given for choosing the

most secure option. Special attention is paid to the use of the Wireshark network analyzer to assess vulnerabilities in various types of connections.

Ключевые слова: Шифрование, аутентификация, криптографический ключ, сетевой трафик, сетевой протокол, несанкционированный доступ, удалённый доступ.

Keywords: Encryption, authentication, cryptographic key, network traffic, network protocol, unauthorized access, remote access.

В современном мире, где сетевая безопасность играет ключевую роль, анализ различных типов подключений становится необходимостью для обеспечения защиты информации и предотвращения потенциальных угроз. В данной научной статье проводится анализ влияния различных типов подключений, таких как Telnet и SSH на общую безопасность сети с использованием программы Wireshark. Взаимосвязь между типами подключений и уровнем безопасности рассматривается с целью выявления потенциальных уязвимостей и разработки рекомендаций по их устранению.

Telnet (TErminaL NETwork) – это сетевой протокол, предназначенный для реализации текстового интерфейса по сети. Он имеет широкое применение, но наиболее востребованным является удалённый доступ к интерфейсу командной строки операционных систем [1]. Однако Telnet предлагает простую модель безопасности, которая не шифрует передаваемые данные. Поэтому злоумышленник, который перехватит трафик, сможет узнать всё, что передаётся. Также Telnet не обладает механизмами аутентификации пользователей, делая систему уязвимой для несанкционированного доступа.

SSH (Secure Shell) - это сетевой протокол, который, как и Telnet, позволяет организовать удалённый доступ к консоли. Но в отличие от Telnet, протокол SSH шифрует все передаваемые данные, что делает их нечитаемыми для злоумышленников. Также он обладает механизмами аутентификации пользователей, используя криптографические ключи, что значительно повышает уровень безопасности [2].

Wireshark – это сетевой анализатор, который позволяет захватывать и анализировать сетевой трафик. Он может быть использован для анализа безопасности различных протоколов, включая Telnet и SSH. Также с помощью Wireshark можно: детально изучить содержимое пакетов данных, выявить потенциальные уязвимости в сетевых подключениях и отследить подозрительную активность.

Для анализа безопасности протоколов Telnet и SSH с помощью программы Wireshark были проведены следующие действия:

1. Запуск программы Wireshark.
2. Захват сетевого трафика.

3. Telnet/SSH-подключение.

4. Остановка захвата.

5. Анализ захваченных пакетов данных в момент подключения.

При анализе Telnet-подключений в Wireshark можно было увидеть содержимое всех команд, введённых на удаленном компьютере, включая пароли (рис. 1). Данная информация может быть использована злоумышленниками для несанкционированного доступа к системе. Также было обнаружено, что Telnet не имеет механизмов аутентификации пользователей.

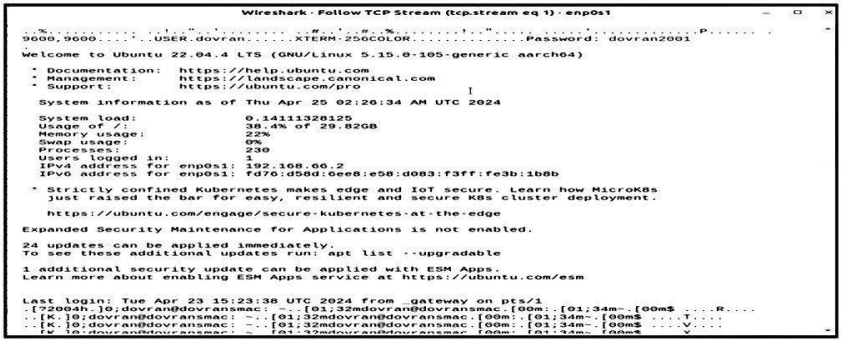

Рисунок 1 – Telnet-подключение

При анализе SSH-подключений в Wireshark можно было видеть только зашифрованный текст (рис. 2), что значительно будет затруднять перехват злоумышленниками конфиденциальной информации.

Рисунок 2 – SSH-подключение

В ходе анализа различных типов подключений, таких как Telnet и SSH, с применением программы Wireshark было выявлено, что протокол Telnet представляет серьёзные угрозы для безопасности из-за передачи данных в открытом виде, что делает его уязвимым для атак, а протокол SSH обеспечивает более высокий уровень безопасности за счёт шифрования данных, аутентификации и защиты от атак. Таким образом, использование Telnet для удалённого доступа не рекомендуется. Особого внимания заслуживает и сетевой анализатор Wireshark, который можно использовать для оценки безопасности сетевых подключений. С помощью него можно выявлять потенциальные уязвимости и принимать меры по их устранению.

Список использованных источников:

1. Сергеев А.Н. Основы локальных компьютерных сетей: учебное пособие/А.Н. Сергеев. – СПб.: Издательство: «Лань», 2016. – 184 с.

2. Олифер В.Г. Компьютерные сети. Принципы, технологии, протоколы / В.Г. Олифер, Н.А. Олифер. – СПб.: Издательство «Питер», 2020. – 1008 с.

УДК 004

Д.Ж. Султанов
Уфимский университет
науки и технологий, Уфа, Россия

Научный руководитель:
Д.С. Юнусова
Уфимский университет
науки и технологий, Уфа, Россия

ИСПОЛЬЗОВАНИЕ НЕЙРОСЕТЕЙ ДЛЯ РАСПОЗНАВАНИЯ ФИШИНГОВЫХ URL
USING NEURAL NETWORKS TO RECOGNIZE PHISHING URLS

Аннотация: В современном мире, где интернет является неотъемлемой частью нашей повседневной жизни, фишинг выступает как одна из самых распространенных и опасных угроз в цифровом пространстве. Фишинговые атаки часто начинаются с отправки электронного письма, содержащего поддельную ссылку. Эта ссылка ведет на веб-сайт, который злоумышленники подготовили таким образом, чтобы сайт выглядел законным. Для пользователей это становится серьезной

проблемой, так как они могут быть введены в заблуждение и раскрыть свои конфиденциальные данные.

Abstract: In today's world, where the Internet is an integral part of our daily lives, phishing acts as one of the most widespread and dangerous threats in the digital space. Phishing attacks often begin by sending an email containing a fake link. This link leads to a website that the attackers have prepared in such a way that the site looks legitimate. This becomes a serious problem for users, as they may be misled and disclose their confidential data.

Ключевые слова: Сеть Интернет, искусственный интеллект, фишинг.

Keywords: Internet, artificial intelligence, phishing.

Фишинговые URL продолжают быть одним из наиболее частых инструментов в арсенале киберпреступников. Они создаются с намерением имитировать официальные веб-страницы, чтобы обманом заставить пользователей предоставить свои личные данные.

Основная проблема в выявлении фишинговых URL заключается в том, что злоумышленники постоянно совершенствуют методы, используя различные технические приемы. К ним относятся подделка доменных имен, использование доменов, похожих на настоящие, и применение сложных перенаправлений. Традиционные методы борьбы с фишингом, такие как черные списки известных фишинговых URL, сталкиваются с проблемами, поскольку киберпреступники быстро развивают новые фишинговые сайты и меняют тактики атак.

Искусственная нейронная сеть представляет собой тип вычислительной системы, разработанный для имитации процессов обработки информации, происходящих в биологическом мозге. Она состоит из большого количества связанных между собой искусственных нейронов [1].

Принцип работы нейросети (Рисунок 1):

1. Входной слой: принимает исходные данные.
2. Скрытые слои: содержат нейроны, которые обрабатывают данные, поступившие из входного слоя. Количество скрытых слоев и нейронов в них может варьироваться в зависимости от сложности задачи.
3. Выходной слой: предоставляет результат обработки данных.

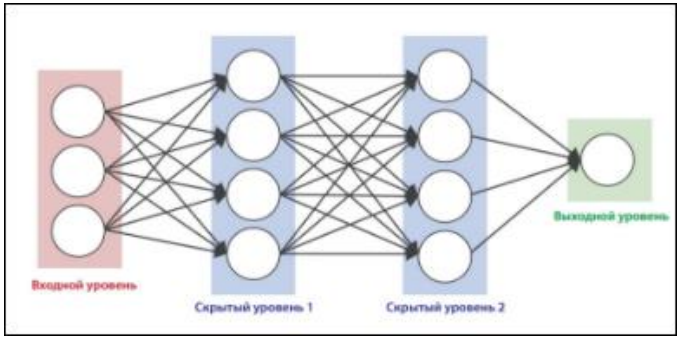

Рисунок 1 – Схема работы нейронной сети

Искусственные нейронные сети представляют собой мощный инструмент для анализа информации и данных, что делает их особенно эффективными в борьбе с фишингом.

Использование искусственной нейронной сети для обнаружения фишинговых URL-адресов осуществляется в два этапа: обучение и распознавание. Во время этапа обучения нейросеть получает набор данных для обучения, который включает в себя специально отобранные и обработанные примеры. Затем, согласно выбранной методике обучения, происходит корректировка весов, что позволяет нейросети при получении нового обучающего примера выдавать на выходе соответствующий класс этого примера (Рисунок 2).

На этапе распознавания нейросеть анализирует неизвестные URL-адреса. В зависимости от результата анализа, который представлен в виде выходного вектора, URL-адрес классифицируется как принадлежащий к одному из ранее определенных классов.

В области использования нейросетей для борьбы с фишингом были проведены различные исследования, направленные на повышение эффективности распознавания фишинговых сайтов и защиту пользователей в интернете. Вот некоторые из них:

– Исследование «Яндекса»: с ноября 2023 года «Яндекс» начал активные тестирования обнаружения фишинговых сайтов с помощью нейросетей. Эта технология анализирует различные параметры сайтов, в том числе и URL адреса, чтобы определить потенциальную опасность для пользователей [2].

– В рамках международного журнала прикладных и фундаментальных исследований был проведен анализ проблемы фишинга в цифровом пространстве. Исследование включало выявление наиболее актуальных проблем и способов противодействия фишинговым атакам [3].

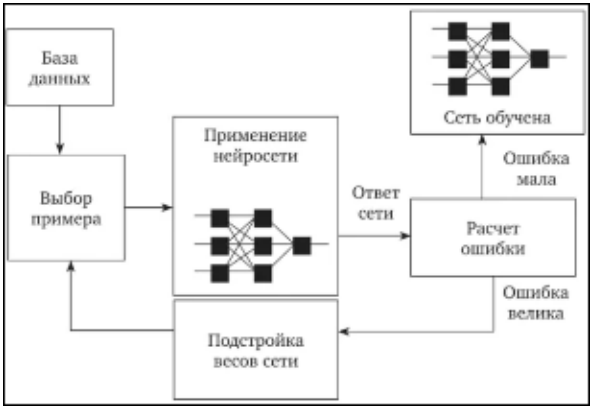

Рисунок 2 – Процесс обучения нейронной сети

Эти исследования подчеркивают значительный потенциал нейросетей в обеспечении кибербезопасности и защите пользователей от фишинговых атак. Они также указывают на необходимость постоянного развития и обновления алгоритмов машинного обучения для адаптации к постоянно меняющимся методам злоумышленников.

Список использованных источников:

1. Исмагилова, А.С. Особенности параметров входного слоя нейронной сети программного комплекса многофакторной аутентификации / А.С. Исмагилова, Н.Д. Лушников // Актуальные проблемы радиоэлектроники и телекоммуникаций: материалы Всероссийской научно-технической конференции, Самара, 25–28 апреля 2023 года. – Самара: ООО «Артель», 2023. – С. 165-166.

2. Нейросеть помогла "Яндексу" выявить почти 400 тыс. фишинговых сайтов за 5 месяцев // Искусственный интеллект Российской Федерации URL: https://ai.gov.ru/mediacenter/neyroset-pomogla-yandeksu-vyyavit-pochti-400-tys-fishingovykh-saytov-za-5-mesyatsev/ (дата обращения: 20.04.2024).

3. Анализ проблемы фишинга в цифровом пространстве // Международный журнал прикладных и фундаментальных исследований URL: https://applied-research.ru/ru/article/view?id=13594 (дата обращения: 20.04.2024).

4. От черного списка до машинного обучения. Антифишинг в Яндекс.Браузере // Habr URL: https://habr.com/ru /companies/yandex/articles/309808/ (дата обращения: 20.04.2024).

5. Механизм распознавания фишинговых сайтов по косвенным признакам // Молодой ученый URL: https://moluch.ru/archive/318/72550/ (дата обращения: 20.04.2024).
6. Нейронные сети и машинное обучение // zvukobook.ru URL: https://zvukobook.ru/raznoe/nejronnye-seti-i-mashinnoe-obuchenie-kak-rabotayut-nejronnye-seti-i-chto-takoe-mashinnoe-obuchenie.html (дата обращения: 20.04.2024).
7. Нейросетевые модели прогнозирования // studme.org URL: https://studme.org/168435/menedzhment/neyrosetevye_modeli_prognozirovaniya (дата обращения: 20.04.2024).

УДК 004

А.С. Файзуллина
Уфимский университет
науки и технологий, Уфа, Россия

Научный руководитель:
А.Ф. Фатхелисламов
Уфимский университет
науки и технологий, Уфа, Россия

УГРОЗЫ ОТКРЫТЫХ СЕТЕЙ БЕСПРОВОДНОЙ ПЕРЕДАЧИ ДАННЫХ
THREATS TO OPEN WIRELESS NETWORKS

Аннотация: Данная статья рассматривает угрозы открытых сетей беспроводной передачи данных. Приведены угрозы беспроводных сетей, последствия реализации угроз и возможные способы защиты.

Abstract: This article examines the threats to open wireless data networks. The threats of wireless networks, the consequences of the implementation of threats and possible methods of protection are given.

Ключевые слова: Беспроводная сеть, Wi-FI, угрозы передачи данных.

Keywords: Wireless network, Wi-Fi, data transmission threats.

Беспроводные сети являются наиболее перспективными и популярными, так как позволяют с наименьшими затратами обеспечивать передачу информации на большие расстояния без использования проводов и большого количества аппаратуры, в отличии от проводных сетей. Принцип обеспечения безопасности беспроводной сети отличается от других особенностями угроз, уязвимостей, рисков и способов защиты

прежде всего тем, что среда передачи данных увеличивает спектр возможных угроз и уязвимостей из-за чего, повышается количество способов доступа к каналам связи. Для обеспечения безопасности беспроводной сети, необходимо провести тщательный анализ всех возможных угроз, последствий их реализации, выделить наиболее успешные и эффективные способы защиты.

Описание угроз и мер безопасности в беспроводных сетях описаны в ГОСТ Р ИСО/МЭК 27033-3-2014 [1]. Рассмотрим наиболее распространенные угрозы открытой беспроводной сети передачи данных.

Обнаружение сети через сторонние устройства и программы. Для обнаружения беспроводных сетей WLAN используются различные утилиты, например, NetStumber. Данная утилита способна идентифицировать SSID сети WLAN и определять, используется ли в ней система шифрования WEP. Информация о степени защиты сети является очень ценной, она позволяет определить злоумышленнику дальнейшие действия, которые приведут к потери конфиденциальности и целостности передающейся в ней информации [2]. В таких случаях стоит уделять внимание настройке мощности передачи сигнала от точки доступа, применять специальные инструменты для контроля над распространением сигнала и использовать специальное глушение сигнала. Можно установить режим скрытого идентификатора SSID, который основывается на том, что для своего обнаружения точка доступа время от времени транслирует кадры-маячки (beacon frames) [3].

Подслушивание. Возможно пассивное слежение злоумышленником за коммуникацией в сети с целью захвата данных, которые передаются по сети, и перехвата учетных данных проверки подлинности. Использование криптографических протоколов SSL/TLS для передачи данных в сети Интернет может обезопасить от прослушивания пакетов и осуществления несанкционированного доступа к личным данным.

Аномалия типа «отказ в обслуживании» DoS (от англ. Denial of Service) – сетевая атака, проводимая злоумышленником в отношении сетевого объекта. При DDoS-атаке сервер перестает отвечать на запросы клиентов, что может привести к недоступности сервиса. В этом случае используют специальные сервисы защиты от DDoS-атак, повышают устойчивость серверов.

Глушение клиентских или базовых станций. Когда преднамеренная или непреднамеренная интерференция превышает возможности получателя или отправителя в канале связи, выводя этот канал из строя, происходит глушение в сети. Оно может вызвать отказ в обслуживании клиента, препятствуя реализации соединения. Чтобы предотвратить случаи глушения необходимо тщательно проанализировать место установки и предусмотреть создание резервных каналов связи [4].

Угрозы криптозащиты. Криптографические средства защиты информации применяются и в беспроводных сетях. Однако взлом злоумышленником системы безопасности приводит к нарушению коммуникаций и неправомерному использованию информации, передающейся в сети. Так, WEP, являющийся протоколом безопасности технологии Wi-Fi, использует простой ключ, который может быть получен перебором. Для защиты от этой угрозы используется, например, ограничение количества ввода ключей.

Угрозы физической защиты. Угроза доступа к авторизированным устройствам злоумышленников. Например, завладев устройством злоумышленник, получает физический доступ и способен заменять программное обеспечение или красть учетные данные, например, статические ключи. Следует помнить о защите устройств от несанкционированного доступа [5].

Внедрение несанкционированных точек доступа. В роли таких точек выступают отдельные аппаратные или программные точки доступа. Пользователь, подключаясь к такой точке доступа, предоставляет злоумышленникам все свои передаваемые данные. Так же такая точка может прослушивать сеть с целью перехвата всего трафика. В борьбе с такими точками доступа применяют метод конвергенции и векторный метод обнаружения.

Атака маршрутизации. Злоумышленник стремится управлять таблицей маршрутизации на сетевом уровне с целью перенаправления трафика в сетях [6]. В этом случае следует ограничить диапазон IP-адресов, которым доступно подключение к маршрутизатору и определить параметры доступа к настройке маршрутизатора.

Система аутентификации. Злоумышленник пытается украсть учетные данные зарегистрированных пользователей сети. Маскарад – случай, когда один пользователь стремится выдать себя за другого для получения определенных привилегий и возможности действий от лица другого пользователя. Подмена стороны аутентификационного обмена – злоумышленник в ходе данной атаки принимает участие в процессе аутентификации между двумя сторонами с целью модификации трафика. Они являются основными атаками на систему аутентификации. Необходимо применять сложные системы аутентификации, ограничивать количество попыток ее прохождения и время сессии.

Таким образом, стремительное развитие беспроводных сетей, помимо приобретения новых возможностей, привело к появлению новых угроз безопасности. Для обеспечения защищенности сети следует принимать соответствующие меры безопасности и анализировать случаи появления новых угроз.

Список использованных источников:

1. ГОСТ Р ИСО/МЭК 27033-3-2014. Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 3. Эталонные сетевые сценарии. Введ. 2015-11-01. URL: https://docs.cntd.ru/document/1200113374 (дата обращения: 24.04.2024).

2. Милосердов, А.О. Классификация угроз и уязвимостей в беспроводных сетях / А.О. Милосердов // Ученые записки УлГУ. Серия: Математика и информационные технологии. – 2023. – № 2. – С. 72-85.

3. Скрыпников, А.В. Защита данных при передаче по беспроводным каналам связи / А.В. Скрыпников, В.В. Денисенко, К.С. Евтеева // Международный журнал гуманитарных и естественных наук. – 2019. – № 8-2. – С. 35-38. – DOI 10.24411/2500-1000-2019-11485.

4. Андреев, М.Ф. Обработка сетевых пакетов в ядре Linux для противодействия атакам типа «отказ в обслуживании» / М.Ф. Андреев, А.С. Исмагилова // Информационные технологии обеспечения комплексной безопасности в цифровом обществе: сборник материалов VI Всероссийской молодежной научно-практической конференции с международным участием, Уфа, 19–20 мая 2023 года. – Уфа: Уфимский университет науки и технологий, 2023. – С. 9-14. – EDN VMOTBK.

5. Исмагилова, А.С. Программная реализация защиты от несанкционированного доступа / А.С. Исмагилова, Н.Д. Лушников // Безопасность информационных технологий. – 2023. – Т. 30, № 1. – С. 81-91. – DOI 10.26583/bit.2023.1.06.

6. Милосердов, А.О. Атаки на беспроводные сети: виды, ущерб, мощность / А.О. Милосердов // Актуальные вопросы современной науки: теория, методология, практика, инноватика: сборник научных статей по материалам XIII Международной научно-практической конференции, Уфа, 17 ноября 2023 года. – Уфа: Общество с ограниченной ответственностью "Научно-издательский центр "Вестник науки", 2023. – С. 112-126.

СЕКЦИЯ 2. СОВРЕМЕННЫЕ ВЫЗОВЫ В ОБЛАСТИ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

УДК 004.056.5

К.И. Абрамов, А.В. Сафронова, К.Д. Щанькин
Поволжский государственный университет
телекоммуникаций и информатики, Самара, Россия

Научный руководитель:
Н.И. Козырева
Поволжский государственный университет
телекоммуникаций и информатики, Самара, Россия

КВАНТОВЫЕ КОМПЬЮТЕРЫ И БУДУЩЕЕ КРИПТОГРАФИИ: ВЫЗОВЫ И ВОЗМОЖНОСТИ
QUANTUM COMPUTERS AND THE FUTURE OF CRYPTOGRAPHY: CHALLENGES AND OPPORTUNITIES

Аннотация: Развитие квантовых компьютеров имеет революционный потенциал в науке и бизнесе, позволяя решать сложные задачи в областях квантовой химии, физики, финансов и машинного обучения. Статья подчеркивает необходимость создания новых технологий и алгоритмов для успешного использования квантовых компьютеров, указывая на потенциальные угрозы безопасности данных из-за возможности взлома криптографических протоколов. Развитие новых квантово-устойчивых криптографических алгоритмов становится ключевым аспектом обеспечения безопасности информации в будущем.

Abstract: The development of quantum computers has revolutionary potential in science and business, allowing us to solve complex problems in the fields of quantum chemistry, physics, finance and machine learning. The article emphasizes the need to create new technologies and algorithms for the successful use of quantum computers, pointing to potential threats to data security due to the possibility of cracking cryptographic protocols. The development of new quantum-stable cryptographic algorithms is becoming a key aspect of ensuring information security in the future.

Ключевые слова: Квантовые компьютеры, безопасность данных, криптографические методы, квантовые алгоритмы, принципы квантовой механики.

Keywords: Quantum computers, data security, cryptographic methods, quantum algorithms, principles of quantum mechanics.

Квантовые компьютеры основаны на принципах квантовой механики и могут производить вычисления на основе квантовых битов или кубитов вместо традиционных 2-разрядных вычислений. Это были совершенно новые компьютерные концепции, которые проложили путь к решению задач, недоступных для классических компьютеров.

Несмотря на раннее развитие квантовых компьютеров, они оказали значительное влияние на различные области науки и коммерции. В научной сфере, в областях квантовой химии, физики и материаловедения, ученые способны решать задачи, которые ранее считались невозможными из-за их сложности и большого количества. В бизнесе квантовые компьютеры могут занять место в области финансов, логистики и машинного обучения, создавать алгоритмы и методы оптимизации.

Но, несмотря на потенциальные преимущества, даже квантовые компьютеры сопряжены с серьезными техническими проблемами. Для их создания требуются очень успешные научные исследования и разработка новых технологий, а также индивидуальных методов программирования и алгоритмов.

Квантовые компьютеры также обещают множество преимуществ для бизнеса. Они могут оптимизировать процессы транспортировки, финансов и искусственного интеллекта. Квантовые алгоритмы, например, могут значительно улучшить прогноз рыночных тенденций и оптимизировать инвестиционный портфель. [1]

Развитие квантовых компьютеров представляет серьезную угрозу для традиционных методов шифрования, которые играют важную роль в обеспечении безопасности данных в цифровой среде. Классические алгоритмы, такие как RSA и ECC, теперь основаны на сложных математических задачах, которые надежно защищают информацию от несанкционированного доступа.

Однако квантовые компьютеры используют кубиты и квантовые операции для параллельного анализа больших объемов данных для решения сложных задач, которые не могут решить классические компьютеры, что дает важные преимущества при решении криптосистем, основанных на сложных математических задачах.

Способность квантовых компьютеров вычислять или выполнять дискретные логарифмические вычисления "на лету" представляет угрозу для методов, которые до сих пор считались надежными. Например, алгоритм Шора, разработанный для квантовых компьютеров, действительно может решить проблему большого количества факторов на основе алгоритма Шора, что означает, что информация, зашифрованная с помощью таких алгоритмов, может быть атакована с помощью квантового компьютера [2].

Развитие квантовых компьютеров вызвало серьезные опасения по поводу безопасности хранения и передачи информации. Квантовый компьютер на то и квантовый, что он способен решать задачи, которые современные классические компьютеры считают сложными или невыполнимыми.

Одной из основных проблем является угроза, исходящая от криптосистем, основанных на классических алгоритмах. Квантовые компьютеры могут легко обойти защиту, обеспечиваемую современными методами шифрования, что может привести к утечке конфиденциальной информации. Например, взлом ключа шифрования может представлять серьезную угрозу безопасности и конфиденциальности информации.

Традиционные криптографические стандарты, такие как RSA и ECC, основаны на вычислительной сложности математических задач, которые квантовые компьютеры могут решать очень быстро. Это означает, что схемы шифрования, которые сегодня считаются надежными, могут нанести ущерб квантовым атакам, угрожающим целостности и конфиденциальности данных [2].

Чтобы преодолеть эту проблему, нам необходимо разработать алгоритмы квантовой стабильности, способные обеспечить безопасность данных в присутствии квантовых компьютеров. Такие алгоритмы выдерживают квантовые атаки и надежно защищают информацию в течение длительного времени [3].

Интеграция квантовой криптографии открывает новые возможности для создания криптосистем, более устойчивых к атакам со стороны квантовых компьютеров. Квантовые принципы обеспечивают конфиденциальность обмена данными и защищают информацию от злоумышленников.

Разработка квантовых компьютеров является серьезной проблемой для шифрования, а разработка квантовых решений для обеспечения надежной защиты данных в цифровой среде, необходимые инвестиции в исследования и разработка строгих методов шифрования для квантовых вычислений являются основным фактором подготовки к изменениям в условиях информационной безопасности.

Чтобы адаптироваться к изменениям, вызванным распространением квантовых технологий, необходима активная работа по созданию новых криптографических методов и средств защиты, способных противостоять квантовым атакам. Это включает исследования в области квантовой криптографии, разработку алгоритмов квантово-сбалансированного шифрования и решений для защиты данных от квантовых вычислений [2].

Инвестиции в разработку квантово-стабильных решений важны с военной точки зрения для обеспечения надежности и стабильности информационных систем за счет развития квантовых технологий.

Квантовые компьютеры также могут представлять серьезную угрозу традиционным методам шифрования, поэтому они могут помочь подготовиться к дальнейшим вызовам кибербезопасности.

Развитие квантовых компьютеров приводит к значительным изменениям в криптографии и появлению новых угроз для современной криптографии и безопасности. Стремительное развитие квантовых вычислений усиливает необходимость изменения криптографических стандартов и разработки алгоритмов квантовой стойкости для защиты информации.

Интеграция технологии квантового шифрования требует исследовательских резервов для создания решений с квантовой стойкостью для адаптации к изменяющимся цифровым средам, что создаёт устойчивое шифрование для решения современных проблем и можно положиться на потенциал квантовых технологий в решении проблем, связанных с устойчивым шифрованием. Это может обеспечить эффективную защиту данных в будущем.

Список использованных источников:

1. Loa Сергей Квантовые компьютеры: путь от фантастики до реальности и их влияние на науку и бизнес / Loa Сергей [Электронный ресурс] // vc.ru: [сайт]. – URL: https: // vc.ru/tech/683297-kvantovye-kompyutery-put-ot-fantastiki-do-realnosti-i-ih-vliyanie-na-nauku-i-biznes (дата обращения 20.04.2024).

2. Квантовые алгоритмы: решение сложных задач / [Электронный ресурс] // FasterCapital: [сайт]. – URL: https: // fastercapital.com/ru/content/Квантовые-алгоритмы--решение-сложных-задач-с-Q.html (дата обращения 20.04.2024).

Квантовые компьютеры: новые возможности вычислений и шифрования / [Электронный ресурс] // VK: [сайт]. – URL: https://vk.com/wall-201406556_307788 (дата обращения 20.04.2024).

УДК 004

Ю.С. Азнабаев
Уфимский университет
науки и технологий, Уфа, Россия

Научный руководитель:
И.А. Шагапов
Уфимский университет
науки и технологий, Уфа, Россия

АНАЛИЗ ИНСТРУМЕНТОВ МОДЕЛИРОВАНИЯ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
ANALYSIS OF INFORMATION SECURITY THREAT MODELING TOOLS

Аннотация: В статье рассматриваются инструменты для моделирования угроз безопасности информации, а также для графического представления сценариев реализации возможных угроз безопасности информации.

Abstract: The article discusses tools for modeling threats to information security, as well as for graphically representing scenarios for the implementation of possible threats to information security.

Ключевые слова: Модель угроз, сценарии реализации, информационная безопасность, актуальность угроз, инструменты моделирования.

Key words: Threat model, implementation scenarios, information security, threat relevance, modeling tools.

В современном мире каждая организация может столкнуться с угрозами информационной безопасности, которые не столь явные, но способные причинить огромный вред, также во многих случаях вред от таких угроз больше, чем от экономических или физических.

После первого случая нарушения информационной безопасности или же после требований регулирующих органов, возникает ситуация, где нужно определиться с тем, от чего отталкиваться при формировании системы защиты информации.

Организация, создавая систему защиты информации, должна определиться с тем: что она защищает, от чего она защищает и какой ущерб ей может быть нанесен. Модель угроз является документом, который отвечает на данные вопросы и вследствие чего становится опорной точкой при создании подобных систем.

Необходимость моделирования угроз безопасности заключается в формировании оптимальной системы защиты информации не, только чтобы защитить систему от актуальных угроз, но также чтобы не возникало ситуации, когда организация защищается от угроз не присущих ей.

Федеральной службой по техническому и экспортному контролю 5 февраля 2021 года был утвержден методический документ – Методика оценки угроз безопасности информации. Данный методический документ приводит к единообразию процесс моделирования угроз и осуществляет его в три этапа.

На первом этапе определяются негативные последствия реализации угроз по отношению к физическим, юридическим лицам и государству. На втором этапе определяются информационные активы (программное обеспечение, средства защиты информации, машинные носители и т.д.). На третьем этапе оценивается возможность возникновения угроз и определяется то, насколько они актуальны.

Основная сложность в данной методике заключается в создании сценариев реализации угроз. Создание таких сценариев осуществляется на последнем этапе, при оценке актуальности угроз безопасности информации. В самом документе сценарии представлены только в графическом виде, однако возможно также табличное представление. Именно процесс графического представления сценариев создает сложность, потому что методичка определяет, что должен быть определен хотя бы один сценарий каждого способа реализации возможной угрозы [1]. Соответственно, если актуальных угроз много и у каждой угрозы есть несколько сценариев реализации, то для каждого из них нужно создавать свое графическое представление, что не представляется простой задачей. Однако у такого вида представления имеются свои положительные стороны такие как: наглядность и удобство.

Существуют немалое количество инструментов, которые могут облегчить процесс создания сценариев реализации угроз. Список можно начинать с самых простых графических редакторов, однако существуют специализированные программные обеспечения для моделирования угроз, которые в свою очередь также ранжируются от простых, где вручную нужно вбивать существующие угрозы, до сложных, где моделирование угроз буквально автоматизируется. Программа сама найдет существующие угрозы и тактики атак, после внесения данных об информационных активах организации.

Примерами инструментов для графического представления сценариев реализации угроз могут являться:

1. OWASP Threat Dragon [2];
2. CAIRIS [3];

3. Mozilla SeaSponge [4];
4. Threagile [5].

Данные программные обеспечения являются бесплатными. Каждый из них предоставляет удобный веб-интерфейс или возможность установки локально на компьютере, а также визуализирует сценарии реализации возможных угроз в виде диаграммы потоков данных.

Недостатком данных программ будет являться отсутствии поддержки русского языка и в преобладании ручных процессов наполнения информацией.

Другим примером подобных инструментов, но с автоматизацией моделирования угроз могут являться:

1. IriusRisk;
2. SD Elements;
3. Splunk Enterprise Security;
4. ThreatModeler;
5. Tutamen Threat Model Automator.

Главным преимуществом данных программных обеспечений является в первую очередь автоматизация моделирования угроз, они включают в себя базы данных атак, угроз, например ATT&CK, CAPEC и в процессе моделирования будут предлагать актуальные угрозы системы, с полным набором информации о них. В программах данного списка также есть возможность получения графического представления сценариев реализации возможных угроз информационной безопасности, также различных отчетов с рекомендациями.

Отдельные недостатки данной группы программ не приведены, а рассмотрены только возможности, которые они предоставляют, так как они недоступны с территории нашей страны.

Использование рассмотренных инструментов облегчает создание модели угроз. Однако главным недостатком всех данных программных обеспечений будет являться то, это продукты иностранного рынка, и соответственно из этого вытекает следующий недостаток, они не могут полностью соответствовать требованиям ФСТЭК. Например, они не будут учитывать перечень угроз безопасности информации, содержащиеся в банке данных угроз безопасности информации ФСТЭК России.

Российский рынок программного обеспечения еще не представил собственных решений для моделирования угроз. С учетом требований методики оценки угроз безопасности информации, востребованность подобных инструментов растет с каждым днем.

Список использованных источников:

1. Методика оценки угроз безопасности информации. Методический документ ФСТЭК России от 5 февраля 2021 г. // Официальный сайт ФСТЭК России [Электронный ресурс]. – URL: https://fstec.ru/component/attachments/download/2919 (дата обращения 21.04.2024).
2. OWASP Threat Dragon [Электронные ресурс]. – URL: https://owasp.org/www-project-threat-dragon/ (дата обращения 21.04.2024).
3. CAIRIS [Электронный ресурс]. – URL: https://github.com/cairis-platform/cairis (дата обращения 21.04.2024).
4. SeaSponge [Электронный ресурс]. – URL: https://github.com/mozilla/seasponge (дата обращения 21.04.2024).
5. Threagile [Электронный ресурс]. – URL: https://github.com/Threagile/threagile (дата обращения 21.04.2024).

УДК 004.056.53: 373.1

А.С. Асанбаева
Уфимский университет
науки и технологий, Уфа, Россия
У.Р. Ахметов
РГУ нефти и газа им. И.М. Губкина, Москва, Россия

Научный руководитель:
А.А. Корнилова
Уфимский университет
науки и технологий, Уфа, Россия

ПРИМЕНЕНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА С ЦЕЛЬЮ ПОВЫШЕНИЯ БЕЗОПАСНОСТИ В ОБРАЗОВАТЕЛЬНЫХ УЧРЕЖДЕНИЯХ
THE USE OF ARTIFICIAL INTELLIGENCE TO IMPROVE SAFETY IN EDUCATIONAL INSTITUTIONS

Аннотация: Технологии искусственного интеллекта постепенно внедряются в сферу видеоаналитики. Видеоаналитика на основе ИИ помогает распознавать события либо до того, как они произойдут, либо по мере того, как происходят, чтобы дать возможность быстро среагировать и принять необходимые меры. Использование данной системы может значительно повысить безопасность образовательных учреждений. В

работе рассматривается вопрос внедрения видеоаналитики в образовательных учреждениях.

Abstract: Artificial intelligence technologies are gradually being introduced into the field of video analytics. AI-based video analytics helps to recognize events either before they occur or as they occur, in order to allow you to react quickly and take the necessary measures. The use of this system can significantly improve the safety of educational institutions. The paper considers the issue of the introduction of video analytics in educational institutions.

Ключевые слова: Безопасность, видеонаблюдение, видеоаналитика, искусственный интеллект, безопасность образовательной организации.

Key words: Security, video surveillance, video analytics, artificial intelligence, security of an educational organization.

В настоящее время вопрос безопасности в образовательных организациях остается актуальным, с каждым днем угроз становится все больше, меняется их характер и степень опасности. Поэтому и средства защиты должны совершенствоваться и работать в комплексе. Анализируя комплексную безопасность образовательных учреждений, необходимо учитывать и ориентироваться на приемлемые уровни риска, которые установлены Федеральными законами, директивными документами, техническими регламентами и т.д. Риски должны быть максимально допустимые в реальных условиях технического, экономического и социального состояния общества. В данном случае критерием качества обеспечения комплексной безопасности является степень снижения риска по сравнению с максимально допустимым.

Комплексная безопасность образовательной организации – это состояние защищенности образовательного учреждения от реальных и прогнозируемых угроз социального, техногенного и природного характера, обеспечивающее его безопасное функционирование. Она может быть достигнута путем реализации комплексной системы мер и мероприятий правового, организационного, технического, кадрового, финансового характера [1].

В данной статье рассмотрим инженерно-техническую часть, а именно видеонаблюдение и возможность его совершенствования при помощи искусственного интеллекта (ИИ) для улучшения безопасности образовательных учреждений.

На сегодняшний день образовательные заведения имеют камеры видеонаблюдения в здании. Видео в онлайн режиме транслируются на пост охраны, где обстановка анализируется сотрудником службы безопасности. На данном этапе большую роль играет человеческий фактор, а именно снижение концентрации человека. По статистике среднее время концентрации внимания составляет до 40 минут. То есть для полного

контроля за объектом этих средств недостаточно. Для минимизации человеческого фактора многие профессии подвергаются цифровизации, где человеческий труд заменяют автоматизированным, например, при помощи технологий ИИ.

Цифровизация затронула все сферы деятельности, поэтому использование технологий ИИ уже не является чем-то неизвестным, а становится привычным явлением, так и сферу видеоаналитики ИИ не обошел стороной. В [2] описан алгоритм внедрения системы интеллектуальной видеоаналитики в образовательных учреждениях.

В целях оценки целесообразности использования систем интеллектуальной видеоаналитики в образовательных учреждениях РФ необходимо рассмотреть алгоритм работы таких систем.

1. Получение фото или видеоматериала с камер видеонаблюдения, архивов видеозаписей и т.д.
2. Локализация объектов в системе при помощи нейронных сетей, обнаружение объектов в кадре, таких как люди, транспорт, подозрительные предметы.
3. Фиксация объекта и наблюдение за ним.
4. Анализ действий предмета/объекта на фото или видеозаписи, это помогает определить намерения действий, например, предугадать действия человека в кадре или понять куда будет двигаться автомобиль.
5. Определение лица, при помощи алгоритмов для распознавания, это помогает определить личность человека в кадре и его дальнейшие действия.
6. Фиксация нарушений, заложенных в программе.
7. Уведомление пользователя(ей), о нарушение или обнаружении подозрительный предмет на территории в течение долгого времени.

Система дает пользователям возможность для формирования отчетности по нарушениям, посещениям и другим различным событиям, это помогает анализировать и улучшать безопасность объекта [3].

При использовании систем, которые базируются на использовании цифровых технологий, нужно всегда учитывать определенные нюансы, возникающие при установке систем видеоаналитики на различных объектах, в том числе и образовательных учреждениях: недостаточное количество данных при обучении модели; нехватка вычислительных ресурсов; низкий процент обеспечения информационной безопасности.

В вопросе обеспечения техническими средствами охраны образовательные учреждения опираются на Национальный стандарт 2019 года. Но в части технических средств охраны в документе есть требования только к наличию в школах систем видеонаблюдения, системы контроля и управления доступом, сигнализации. И часто школы останавливают свой

выбор на самом бюджетном оборудовании, которое, к сожалению, не решает проблему.

Для решения проблемы предлагается разработка системы распознавания предметов, представляющих потенциальную угрозу. Для разработки данной системы выбран метод Single Shot Multi Box Detector, а именно SSD300, так как с уменьшение размерности входного изображения увеличит скорость работы алгоритма. Для извлечения признаков алгоритм SSD использует глубокую сверточную нейронную сеть VGG16, а распознавание объектов осуществляется с помощью специального модуля, состоящего из двух сверточных слоев: регрессии и классификации. Для реализации алгоритма SSD был выбран язык программирования Python. Для создания и обучения нейронной сети, используемой TensorFlow 2.0. Данная система работает с изображениями, которые приходят с камер видеонаблюдения с выбранной периодичностью. Система анализирует полученное изображение, и при положительном результате нахождения постороннего предмета, выводит сообщение на экран [4].

Таким образом, установка системы видеоаналитики в школе обусловлена прежде всего вопросами общественной безопасности во всех ее проявлениях. Использование нейронных сетей может помочь при совершенствовании систем видеонаблюдения, при помощи различных алгоритмов видеокамеры смогут определять личности людей, правонарушения, подозрительные предметы на территории. Все это, в свою очередь может значительно повысить процент безопасности в образовательных учреждениях и не только. Тем самым системы видеоаналитики помогут распознавать виновных в случившихся событиях, а также предотвратить противоправные события вовсе.

Список использованных источников:

1. Балыхин Г.А. Обеспечение безопасности образовательного процесса: комплексный подход к решению проблемы. В сб.: Комплексная безопасность в системе образования. – М.: ИФ «Образование в документах», 2007. – 248 с.

2. Комплексная безопасность образовательного учреждения: понятийный аппарат, правовые основы, система мер обеспечения. Краткий справочник // Серия: «Библиотечка заместителя руководителя образовательного учреждения по обеспечению безопасности» / Отв. редактор Е.С. Кушель; авт.-сост. профессор В.Ф. Пилипенко. – М.: Центр «Школьная книга», 2007. – 160 с.

3. Петрова Н.П., Бондарева Г.А. Цифровизация и цифровые технологии в образовании // Мир науки, культуры, образования. – 2019. – № 5(78). – С. 353–355.

4. Гелиг А., Матвеев А. Введение в математическую теорию обучаемых распознающих систем и нейронных сетей. Учебное пособие / Аркадий Гелиг, Алексей Матвеев - Издательство СПбГУ, 2018. – 224 с.

УДК 004.032.26

Р.Ш. Асанов
Уфимский университет
науки и технологий, Уфа, Россия

Научный руководитель:
Н.Г. Миронова
Уфимский университет
науки и технологий, Уфа, Россия

УЯЗВИМОСТИ НС-МОДЕЛЕЙ И АТАКИ НА НС-СИСТЕМЫ
VULNERABILITIES OF NEURAL NETWORKS. ATTACKS ON NN SYSTEMS

Аннотация: В статье рассмотрены уязвимости и типы атак на системы нейронных сетей.

Abstract: The article discusses vulnerabilities and types of attacks on neural network systems.

Ключевые слова: Нейронная сеть, уязвимость, глубокое обучение, атака.

Keywords: Neural network, vulnerability, deep learning, attack.

Глубокие нейронные сети (ГНС, DNN) широко используются для решения многих сложных задач (классификации, обработке естественного языка и изображений, обнаружении вредоносных программ, антиспам-фильтрации, поведенческом анализе, автономной навигации, управлении автоматикой и робототехникой и мн.др.). Однако нейронные сети имеют ряд уязвимостей (например, зависимость от обучающего датасета, нестабильность), подверженность ряду атак (например, Adversarial inputs, Data poisoning и др.), что снижает эффективность их применения и дает возможность злоумышленникам значимо влиять на результат работы инструментов с ГНС. Функциональная уязвимость НС-моделей (как с учителем, так и без учителя) – их «когнитивная слепота», неспособность обнаруживать категории событий, явлений и данных при принятии

решения, относительно которых нейросети не было предоставлено сведений на этапе обучения; и, если человек, осознав пробел знаний, будет искать дополнительную информацию, нейросетевые модели не обладают собственной мотивацией к устранению этого дефекта. [1]

В 2013 году С. Сегеди с коллегами продемонстрировали Adversarial Attack (потерю способности ML-модели правильно распознавать чуть зашумленное изображение, неотличимое от тестового образца для человеческого глаза, но определяемое моделью как нечто иное); позже описаны другие атаки: Limited-memory Broyden Fletcher Goldfarb Shanno (L-BFGS); Fast Gradient Sign Method (FGSM); DeepFool; One-Pixel Attack и др. Так, Н. Моргулис [2] продемонстрировал, как навигационные системы автомобиля с распознаванием дорожных знаков могут быть обмануты дорожными знаками, в которые намеренно внесены небольшие искажения, заставить автомобиль совершать потенциально аварийные действия (аналогично, можно ожидать, что отравление модели или обучающего набора НС-модели системы защиты для обнаружения признаков кибератаки может делать такую систему защиты слепой к угрозам ИБ).

Атаки на модели НС различаются по результату воздействия на систему (атаки изменения поведения пытаются нарушить целостность системы, а атаки нарушения конфиденциальности направлены на получение злоумышленником доступа к обучающим данным, архитектуре, веса обученной модели и т.д.).

Атаки на ML-модели могут быть направлены на:

– выявление/хищение архитектуры модели (т.н. атаки WhiteBox);

– выявление обучающего набора, чтобы понять логику работы ML-модели и понять, как ее обмануть (BlackBox);

– на выявление логики, алгоритма и его гиперпараметров (атаки GrayBox), например, с помощью специальных запросов/образцов и анализа ответной реакции.

Атаки отравления НС-моделей состоят в манипуляции обучающими данными или их разметкой. Атаки уклонения направлены на обман НС-модели предъявлением искаженных и зашумленных образцов, чтобы заставить инструмент на основе НС-модели принять неверное решение или вызвать сбой в работе. Атаки могут быть виртуальными (в цифровой среде) или физическими (когда атака реализуется в реальном мире, например, предъявление маски или камуфляжа при распознавании, аутентификации, чтобы быть распознанным нейросетью как другой человек или объект).

По росту публикаций о способах атак на ML можно заключить, что вредоносное машинное обучение (Adversarial Machine Learning) как область исследований и практик кибератак активно развивается, а теория и методология безопасности систем машинного обучения пока лишь в

начальной стадии своего развития и отстает в этой «гонце вооружений». Среди мер противодействия AML-угрозам – идентификация подобных угроз (например, MITRE и MS ведут базу подобных угроз [4], а в «Техническом отчете по стратегии предотвращения угроз ETSI-SAI-005-GR» приведены некоторые методы распознавания ряда таких атак). Разработчикам ML-моделей рекомендуют придерживаться стандартов DevSecOps - принципов безопасной разработки и проектирования, чтобы снизить риски раскрытия информации об архитектуре ML-модели. Подходы к проактивной защите от вредоносного ML: дообучение ML модели с сетью-«противником» (имитирующим некоторые атаки и обучающим модель им противостоять), метод «защитной дистилляция» и др. Хотя для ряда конкретных прикладных моделей НС были разработаны различные методы корректировки (переобучения), но эти методы не являются универсальными для широкого класса ГНС-моделей. В случае мощных атак (атака C&W) и эти методы противодействия малоэффективны, либо не подходят для больших ГНС. Т.о., противодействие AML-угрозам – актуальное и перспективное направление информационной безопасности.

Список использованных источников:

1. Миронова Н.Г. Когнитивные искажения нейросетевых моделей и проблема доверия синтетическому «знанию» / Современные вопросы педагогики и психологии: теоретико-методологические подходы и практические результаты исследований: монография / А.А. Киселев, А.И. Кугай, Г.И. Авходиев [и др.]. – Чебоксары: ИД «Среда», 2024. – 172 с. – С. 124.
2. N. Morgulis, A. Kreines, S. Mendelowitz, Y. Weisglass, Fooling a Real Car with Adversarial Traffic Signs. – 2019. – http://arxiv.org/abs/1907.00374/ (дата публикации: 30 июня 2019)
3. Скрытая угроза: критерии классификации атак на нейронные сети // Блог компании Smart Engines – URL: https://habr.com/ru/companies/smartengines/articles/753584/ (дата публикации: 11 августа 2023).
4. Shankar R.S.K., O'Brien D., … Failure Modes in Machine Learning (Режимы сбоя в машинном обучении) / Microsoft Build – URL: https://learn.microsoft.com/ru-ru/security/engineering/failure-modes-in-machine-learning/ (дата публикации: 2 июня 2023).

УДК 004

И.И. Ахмадуллин
Уфимский университет
науки и технологий, Уфа, Россия

Научный руководитель:
А.Ю. Сенцова
Уфимский университет
науки и технологий, Уфа, Россия

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ В ЭПОХУ НЕЙРОННЫХ СЕТЕЙ
PERSONAL DATA PROTECTION IN THE ERA OF NEURAL NETWORKS

Аннотация: в статье раскрыты основные принципы обеспечения безопасности, связанные с раскрытием персональных данных в сети Интернет при помощи нейронных сетей. Особое внимание уделяется проблемам защиты персональных данных и м ерам, позволяющим обеспечить безопасность персональных данных при обработке их с помощью искусственного интеллекта.

Abstract: The article reveals the basic principles of security related to the disclosure of personal data on the Internet using neural networks. Special attention is paid to the problems of personal data protection and measures to ensure the security of personal data when processing them using artificial intelligence.

Ключевые слова: Информация, персональные данные, утечка персональных данных, защита персональных данных, нейронные сети, искусственный интеллект, машинное обучение.

Keywords: Information, personal data, personal data leakage, personal data protection, neural networks, artificial intelligence, machine learning.

В настоящее время нейронные сети становятся все более популярным инструментом бизнеса для решения различного рода задач. В числе достоинств искусственной нейронной сети можно отметить следующее: это один из методов искусственного интеллекта, который помогает электронным устройствам и учит их обрабатывать данные по принципу человеческого мозга. То есть у компьютеров появляется возможность принимать «разумные» решения без участия человека.

Таким образом, нейронные сети уже сейчас находят свое применение в различных сферах жизни, и круг проблем, которые можно решить с их помощью, с каждым годом расширяется. Сейчас самыми популярными

сферами, применяющими нейронные сети, являются финансовый сектор и медицинские организации.

Защита персональных данных (ПДн) является одной из проблем, с которой современные компании сталкиваются при использовании нейронных сетей. В качестве примера можно рассмотреть следующую статистику: Роскомнадзор в предыдущем году зафиксировал порядка 170 утечек ПДн. В открытом доступе оказалось колоссальное количество данных (более 300 миллионов записей) о гражданах РФ. Основными регулирующими нормативными правовыми актами в сфере защиты ПДн являются Конституция Российской Федерации, Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ, Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ.

Стоит отметить, что нейронные сети можно классифицировать в зависимости от выполняемых задач: многослойные нейронные сети для обработки числовых данных; сверточные нейронные сети для работы с изображениями; рекуррентные нейронные сети для работы с изменяющейся информацией; генеративные нейронные сети для создания текстов, изображений и видео [1].

Нейросеть может отслеживать и анализировать действия пользователя в Интернете для разработки персонализированных предложений. Пользователи сами предоставляют данные, например, когда что-то ищут в браузере или используют «умные» гаджеты с трекерами. Чем больше персональной информации о пользователе будет у нейронной сети, тем лучше и точнее она будет работать, а следовательно, от этого зависит конечный результат.

Отсутствие приватности персональных данных при применении нейросетей – еще одна проблема, которую надо учесть при построении системы защиты информации. Используя полученные ПДн, злоумышленники могут не просто совершать звонки под видом банковского работника, но и с помощью нейронных сетей подменить голос пользователя или его лицо [2]. Один из популярных способов фальсификации данных с применением нейронной сети – это создание фальшивых видео и фотографий, которые с легкостью можно загрузить в сеть Интернет, соответственно, и использовать против пользователя. Персональные данные из взломанных аккаунтов могут запросто использоваться даже в криминальных схемах и шпионаже [3].

Нейронные сети способны к сохранению персональных данных пользователя. То есть практически невозможно полностью удалить информацию из системы, которую предоставили хотя бы единожды. С помощью вредоносного кода, можно проникнуть в сеть, ознакомиться и использовать конфиденциальные данные, например, данные

о медицинских обследованиях, банковских картах и счетах и адресе проживания [4].

Чтобы обезопасить себя и свои данные при использовании нейронных сетей, стоит выделить основные задачи системы защиты персональных данных: работа нейронных сетей с зашифрованными персональными данными; обеспечение обезличивания ПДн; обеспечение правового регулирования при использовании ПДн нейронными сетями [5].

Для того чтобы решить вышеперечисленные задачи, следует использовать определенные методы защиты:

1. Криптографические механизмы шифрования данных. Если использовать зашифрованные данные, конечный результат может быть получен также в зашифрованном виде.
2. Обезличивание персональных данных для модели нейронной сети. При обезличивании данных нейросеть будет получать меньшее количество информации, а как отмечалось ранее, именно совокупная информация о человеке предоставляет возможность нейросети работать более точно.
3. Совершенствование правового регулирования должно заключаться в регулярном письменном согласовании изменений персональных данных с их субъектом. Субъекту персональных данных должна предоставляться возможность регулярного ознакомления с обновленными данными. При любом изменении следует уведомлять пользователя.

В заключение стоит отметить, что применение нейронных сетей существенно облегчает и упрощает работу человека при помощи искусственного интеллекта. Нейронные сети могут регулярно обучаться и легко находить оптимальные решения поставленных задач. При этом не стоит забывать о защите данных, которые используют при обработке нейросети.

Список использованных источников:

1. Бычков, А.И. Проблемы защиты персональных данных / А.И. Бычков. – Москва: Infotropic Media, 2020. – 116 с. – ISBN 978-5-9998-0352-8. – Текст: электронный // Лань: электронно-библиотечная система. – URL: https://e.lanbook.com/book/234317 (дата обращения: 10.03.2024).

2. Исмагилова, А.С. Комплексная биометрическая аутентификация пользователей информационной системы с применением нейронных сетей / А.С. Исмагилова, Н.Д. Лушников // Инженерный вестник Дона. – 2024. – № 1(109). – С. 178-188.

3. Евстафьев, В.А. Искусственный интеллект и нейросети: практика применения в рекламе: учебное пособие / В.А. Евстафьев, М.А. Тюков. – Москва: Дашков и К, 2023. – 426 с. – ISBN 978-5-394-05455-6. – Текст:

электронный // Лань: электронно-библиотечная система. – URL: https://e.lanbook.com/book/392276 (дата обращения: 11.03.2024).

4. Петренко, В.И. Защита персональных данных в информационных системах. Практикум: учебное пособие для вузов / В.И. Петренко, И.В. Мандрица. – 5-е изд., стер. – Санкт-Петербург: Лань, 2024. – 108 с. – ISBN 978-5-507-47575-9. – Текст: электронный // Лань: электронно-библиотечная система. – URL: https://e.lanbook.com/book/392402 (дата обращения: 09.03.2024).

5. Скрипник, Д.А. Обеспечение безопасности персональных данных: учебное пособие / Д.А. Скрипник. – 2-е изд. – Москва: ИНТУИТ, 2016. – 121 с. – Текст: электронный // Лань: электронно-библиотечная система. – URL: https://e.lanbook.com/book/100272 (дата обращения: 09.03.2024).

УДК 004

Д.М. Ахмедьянов
Уфимский университет
науки и технологий, Уфа, Россия

Научный руководитель:
Р.М. Яппаров
Уфимский университет
науки и технологий, Уфа, Россия

ИСПОЛЬЗОВАНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: ВОЗМОЖНОСТИ ВЫЗОВЫ И ПЕРСПЕКТИВЫ
THE USE OF ARTIFICIAL INTELLIGENCE IN ENSURING INFORMATION SECURITY: OPPORTUNITIES, CHALLENGES AND PROSPECTS

Аннотация: В статье рассматривается использование искусственного интеллекта в обеспечении информационной безопасности её возможности и вызовы, и перспективы.

Abstract: The article discusses the use of artificial intelligence in ensuring information security, its capabilities and challenges and prospects.

Ключевые слова: Информационная безопасность, искусственный интеллект.

Keywords: Information security, artificial intelligence.

Начать хотелось бы с того, что в современном мире, когда количество данных и сложность информационных систем неуклонно растут, задачи обеспечения безопасности становятся все более масштабными и сложными. В этом контексте искусственный интеллект (ИИ) представляет собой мощный инструмент, способный существенно улучшить способность организаций защищать свои активы [1]. Однако наряду с возможностями, которые открывает ИИ, возникают новые вызовы и риски.

В последние годы мы стали свидетелями способности ИИ обеспечивать информационную безопасность. Это дает огромные возможности для удобства и комфорта, снижая затраты на энергию и сокращая нагрузку на окружающую среду. Однако с этим возрастает и риск безопасности, который нельзя игнорировать.

В первую очередь нужно отметить, что искусственный интеллект может анализировать большие объемы данных в реальном времени, выявлять аномальные паттерны поведения и предпринимать меры для нейтрализации угроз автоматически [2]. Это особенно важно в контексте современных кибератак, которые могут развиваться слишком быстро для реакции человека.

Также ИИ позволяет повышать точность систем безопасности, Интеграция ИИ позволяет уменьшить количество ложных срабатываний, которые часто встречаются в традиционных системах безопасности. Машинное обучение способно адаптироваться и обучаться на основе новой информации, что повышает общую эффективность системы.

Еще одним очень важным элементом безопасности является прогностическая безопасность, искусственный интеллект способен не только реагировать на угрозы, но и предсказывать их, анализируя текущие тенденции и исторические данные [3]. Это дает возможность предотвращать атаки еще до их начала.

Еще не стоит забывать про такие вещи как обучение и адаптация, системы ИИ могут постоянно учиться и адаптироваться к новым угрозам, что делает их крайне эффективными против адаптивных киберугроз, которые эволюционируют, чтобы обходить традиционные методы защиты.

Но также не стоит забывать про возможные риски, так же как и защитные системы используют ИИ, такими же технологиями могут воспользоваться и злоумышленники. Например, использование ИИ для автоматизации фишинговых атак или создания малициозного ПО, способного адаптироваться к защитным механизмам.

Вопросы конфиденциальности и защиты данных, связанные с анализом больших данных ИИ, вызывают опасения. Необходимо строгое регулирование использования данных и ИИ в целях обеспечения безопасности, чтобы не нарушать права человека [4].

Ну и, конечно же, не стоит забывать про зависимость от технологий, усиленное внедрение ИИ в аспекты безопасности приводит к увеличению зависимости от этих систем. Ошибки в работе ИИ или потенциальные уязвимости в алгоритмах могут привести к серьезным последствиям [5].

Мировое сообщество постоянно работает над улучшением технологий ИИ в области безопасности. Идет активное развитие новых методик машинного обучения, которые могут адаптироваться и реагировать на сложные киберугрозы [6]. Однако для минимизации рисков необходимо развитие не только технологий, но и юридических, этических норм, а также обучение специалистов.

Искусственный интеллект, несомненно, играет ключевую роль в борьбе с киберугрозами и улучшении общей инфраструктуры безопасности. Однако, чтобы полностью раскрыть его потенциал, необходим комплексный подход, учитывающий все аспекты внедрения и использования ИИ-технологий.

Список использованных источников:

1. Хромин А.А. Проблема искусственного интеллекта. – [Электронный ресурс]. URL: http://www.structuralist.narod.ru/articles/ai.htm (дата обращения: 23.04.2024).

2. Анисимов С.Ю. Алгоритмы искусственного интеллекта. – [Электронный ресурс]. URL: http://faqs.org.ru/progr/common/ai.htm (дата обращения: 23.04.2024).

3. Чипига, А.Ф. Информационная безопасность автоматизированных систем / А.Ф. Чипига. – М.: Гелиос АРВ, 2017. – 336 с.

4. ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения» [Электронный ресурс] // ГАРАНТ: справочно-правовая система / URL: https://base.garant.ru/5921891/. – (дата обращения: 23.04.2024).

5. Янбердин, У.М. Искусственный интеллект и кибербезопасность / У.М. Янбердин, Р.М. Яппаров // Прикладные процессы в области информационной безопасности. Тенденции развития методов защиты информации: Материалы научно-практических конференций, Самара, 19–20 октября 2023 года. – Самара: Поволжский государственный университет телекоммуникаций и информатики, 2023. – С. 34-36.

6. Свидетельство о государственной регистрации программы для ЭВМ № 2023686833 Российская Федерация. Биометрическая аутентификация пользователей информационной системы на основе искусственных нейронных сетей: № 2023685836: заявл. 22.11.2023: опубл. 08.12.2023 / Н.Д. Лушников, А.С. Исмагилова.

УДК 004

А.С. Ворсина
Уфимский университет
науки и технологий, Уфа, Россия

Научный руководитель:
Ф.Т. Байрушин
Уфимский университет
науки и технологий, Уфа, Россия

ПРОБЛЕМЫ БЕЗОПАСНОСТИ ИСПОЛЬЗОВАНИЯ ФАЙЛОВ COOKIES
SECURITY ISSUES WITH THE USE OF COOKIES

Аннотация: В статье раскрыты особенности применения файлов cookies. Описаны вопросы обеспечения безопасности данных пользователей при использовании файлов cookies, а также методы и средства их защиты.

Abstract: The article reveals the features of the use of cookies. It describes the issues of ensuring the security of user data when using cookies, as well as methods and means of protecting them.

Ключевые слова: Защита информации, информационная безопасность, файлы cookies, персональные данные, веб-сайт, браузер, Интернет.

Keywords: Information protection, information security, cookies, personal data, website, browser, Internet.

Файлы cookies (куки-файлы) представляют собой текстовые файлы, которые содержат фрагменты данных пользователя, которые интернет-ресурс использует для идентификации устройства. Когда пользователь покидает сайт, то куки-файлы по умолчанию сохраняются. При повторном посещении ресурса пользователь уже будет идентифицирован («узнан»). Файлы cookies не обладают негативным характером, но если они попадут в руки мошенников, то злоумышленники завладеют данными пользователей. Это является серьезной проблемой информационной безопасности.

Куки-файлы содержат информацию о действиях человека на веб-ресурсах: ФИО, логин, пароль, число и периодичность посещений ресурса, выбранные и просмотренные товары и услуги, устройство, с которого был осуществлен вход, IP-адрес пользователя. То есть у веб-ресурсов появляется возможность составления портрета пользователя.

Не так давно сайты могли обрабатывать данные из cookies без уведомления пользователя, который посещает сайт, и в своих интересах. Но законодательство меняется стремительными темпами, как и новые технологии, и сейчас требования к использованию куки-файлов ужесточилось. В 2016 году Европейский парламент и Совет Европейского Союза сформулировали положения, где все сведения о действиях пользователей в сети Интернет получили статус конфиденциальной информации, на получение и использовании которой требуется обязательное разрешение от пользователя.

Поэтому на действия, которые совершаются с применением куки-файлов, начали распространяться определенные правила, как и для обработки персональных данных (ПДн) пользователя: обработка куки-файлов должна осуществляться только в соответствии с заранее определенной целью и заканчиваться после ее достижения; хранение куки-файлов в виде, который позволяет определить субъекта ПДн, не должно быть дольше, чем этого требуют цели обработки; обработка куки-файлов должна осуществляться только с согласия субъекта ПДн; оператор ПДн должен принять необходимые и достаточные меры по защите данных; оператор ПДн должен принимать необходимые меры по уточнению данных и др.

Если пользователь заходит на сайт, у него автоматически выходит окно согласия на обработкуфайлов cookies. Данное окно можно закрыть и не предоставлять данные, либо нажать на кнопку «Согласен». В общей политике обработки ПДн на веб-ресурсе необходимо также прописать информацию о сборе и обработке файлов cookies. Размещение данного документа на сайте обязательно. Стоит отметить, что если оператор ПДн нарушит законодательство в области ПДн, штраф для юр. лиц составляет до 100 тысяч рублей, при повторном нарушении – до 300 тысяч рублей.

Многие пользователи сети Интернет обеспокоены, что принимая согласие на обработку файлов cookie, они предоставляют доступ к информации третьим лицам, которой могут воспользоваться мошенники. Действительно, риски информационной безопасности существуют, но при определенных условиях:

- применение незащищенного общественного Wi-Fi;
- использование взломанных и зараженных вредоносным ПО устройств и др.

Если не уделять должное внимание защите своих данных, то они могут быть под угрозой, а следовательно, файлы cookies могут быть использованы в чужих целях. Но если соблюдать правила цифровой гигиены, риски будут минимизированы. Одна из таких рекомендаций – полный анализ согласия на принятие правил обработки cookie. Не стоит давать согласие, автоматически нажимая на каждом сайте кнопку

«Согласен». Также пользователь может вручную удалить сохраненные файлы. Включить эту функцию можно в настройках браузера. Существует также режим «инкогнито», когда автоматически файлы cookies будут стираться после окончания визита.

Применение поисковой системы DuckDuckGo вместо распространённых поисковиков поможет защитить пользователя от сбора данных. Данная поисковая система ориентирована в первую очередь на конфиденциальность и приватность. Она не сохраняет данные о пользователях и не передает их третьим лицам.

Повысить безопасность данных поможет применение технологий VPN. VPN обеспечивает зашифрованное подключение к сети Интернет, защищая данные пользователя, обеспечивая анонимный доступ к ресурсам в сети. Рассматривая сервисы, которые предоставляют услуги по созданию защищенного канала соединения с Интернетом, можно разделить на платные и бесплатные. Стоит отметить, что платные VPN-сервисы являются более надежными по сравнению с бесплатными, так как они имеют прибыль от покупки подписки, в том время как бесплатные могут зарабатывать на продаже рекламы и даже пользовательских данных.

Наиболее распространенными платными сервисами являются: ExpressVPN; ZenMate; Private Internet Access; PrivateVPN и др.

Как отмечалось ранее, в браузерах можно заблокировать использование файлов cookies. Выполнить настройки по блокированию файлов, пользователь может повысить конфиденциальность. Более надежную защиту представляет KasperskySecurityCloud. Данное комплексное решение защитит от сбора данных о действиях пользователя в Интернете. Также KasperskySecurityCloud может предоставить защиту от спама, фишинга, вирусного ПО.

Список использованных источников:

1. Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 12.12.2023) «Об информации, информационных технологиях и о защите информации». – URL: http://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения 15.03.2024).

2. Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 06.02.2023) «О персональных данных». - URL:http://www.consultant.ru /document/cons_doc_LAW_61798/ (дата обращения 14.03.2024).

3. Байрушин, Ф.Т. Информационная безопасность как фактор обеспечения социальной стабильности в российском обществе / Ф.Т. Байрушин, И.В. Салов, И.Р. Абрамов // Евразийский юридический журнал. № 8(183). 2023. С.427-429

4. Байрушин, Ф.Т. Информационная безопасность в современном многополярном укладе общественного устройства / Ф.Т. Байрушин,

И.В. Салов, И.Р. Абрамов // Евразийский юридический журнал. № 8(183). 2023. С.416-417

5. Бычков, А.И. Проблемы защиты персональных данных / А.И. Бычков. – Москва: InfotropicMedia, 2020. – 116 с. – ISBN 978-5-9998-0352-8. – Текст: электронный // Лань: электронно-библиотечная система. – URL: https://e.lanbook.com/book/234317 (дата обращения: 13.03.2024).

6. Леонтьев, А.С. Защита информации: учебное пособие / А.С. Леонтьев. – Москва: РТУ МИРЭА, 2021. – 79 с. – Текст: электронный // Лань: электронно-библиотечная система. – URL: https://e.lanbook.com/book/182491 (дата обращения: 25.03.2024).

УДК 004

Р.Т. Галеев
Уфимский университет
науки и технологий, Уфа, Россия

Научный руководитель:
И.А. Шагапов
Уфимский университет
науки и технологий, Уфа, Россия

МОДЕЛЬ МАШИННОГО ОБУЧЕНИЯ В ОБЛАЧНЫХ ТЕХНОЛОГИЯХ
THE MACHINE LEARNING MODEL IN CLOUD TECHNOLOGIES

Аннотация: В работе выполнен обзор литературы по защите от атак на основе машинного и глубокого обучения и проблемам безопасности в облачных вычислениях. Анализ тематических исследований описывает наиболее распространенные проблемы безопасности в облаке; применяются модели машинного обучения, различные наборы данных, метрики производительности, меры противодействия и защиты на основе глубокого обучения, разработанные для предотвращения проблем безопасности. Целью исследования является изучение модели машинного обучения в облачных технологиях.

Abstract: The paper provides a review of the literature on protection against attacks based on machine and deep learning and security issues in cloud computing. Case study analysis describes the most common security issues in the cloud; machine learning models, various datasets, performance metrics, deep learning-based countermeasures and defenses designed to prevent security problems are applied. The purpose of the study is to study the machine learning model in cloud technologies.

Ключевые слова: Облачные вычисления, кибербезопасность, угрозы, машинное обучение, глубокое обучение, обнаружение вторжений
Keywords: Cloud computing, cybersecurity, threats, machine learning, deep learning, intrusion detection.

Сегодня одна из проблем, с которой сталкивается облачная среда, – сохранение конфиденциальности данных. Многие предприятия передают свои данные в облако и выполняют анализ данных удаленно. Данные, передаваемые на аутсорсинг в облако, и данные, которыми обмениваются клиент и облачный сервер, всегда находятся под угрозой раскрытия сервером или другими клиентами в облаке, поэтому конфиденциальность пользователя не гарантируется полностью в облачной среде. По этим причинам методы на основе машинного и глубокого обучения должны использоваться для защиты облачной среды от вторжений, а также сохранения конфиденциальности данных для клиентов [1].

Повышение точности – это общая будущая цель каждой модели машинного или глубокого обучения. Некоторые исследователи пытаются повысить точность с помощью операций предварительной обработки, а некоторые пытаются построить гибридную модель для повышения точности. Добавление одного шага или корректировка правильных параметров также является распространенным методом повышения точности модели. Будущая работа может быть направлена на улучшение модели машинного или глубокого обучения, чтобы она работала более точно.

Разработка модели на основе методов активного обучения или методов ансамблевого обучения является одной из тенденций в области безопасности облачных вычислений [2]. Однако если следовать этим методам, временная сложность еще больше увеличится. Например, авторы и упомянули в будущей работе возможность использования методов активного обучения и методов ансамблевого обучения соответственно.

Применение модели к нескольким наборам данных также является общей будущей областью применения в области обнаружения вторжений. Очень важно использовать актуальный набор данных, который содержит данные об облачных атаках.

Методы отбора признаков также будут широко использоваться в будущем при обнаружении или классификации атак. Согласно проанализированным тематическим исследованиям, будущие темы облачной безопасности на основе машинного и глубокого обучения сосредоточены на конфиденциальности, накладных расходах на вычисления, ранжировании хостов, которые производят атаки, наборе данных и обнаружении атак. Будущая работа по устранению накладных расходов на вычисления может быть сосредоточена на улучшении

планирования заданий; использование простых и эффективных операций шифрования; использование эффективной генерации ключей. Будущая работа также может быть направлена на ранжирование хостов, которые производят атаки или участвуют в краже данных, с помощью алгоритмов самообучения. Этот метод предоставляет дополнительную информацию об энергозависимой памяти зараженных машин и может уменьшить необходимость для эксперта-человека определять важные критерии для обнаружения скомпрометированной машины; сбор нескольких наборов данных. Работа, связанная с обнаружением атак и вторжений, может быть сосредоточена на сокращении времени обнаружения; обнаружение вторжений в зашифрованные пакеты с использованием мета эвристических алгоритмов; охват широкого спектра атак, таких как программы-вымогатели, вредоносные программы для Android, рекламное ПО, а также обнаружение APT-атак с использованием автокодировщика свертки; повышение точности обнаружения атак с помощью следующих методов: ансамблевое обучение, временные методологии, выбор признаков, гибридные модели, оптимальный классификатор или методы активного обучения[3].

Данное исследование посвящено роли методов машинного и глубокого обучения в защите облачной среды от различных атак, угроз и уязвимостей. В работе описаны возможные направления облачной безопасности на основе машинного и глубокого обучения и пробелы в тематических исследованиях, а также открытые проблемы облачной безопасности на основе машинного и глубокого обучения. Ожидается, что эта область исследований станет тенденцией в ближайшие годы, поскольку она растет все больше, а в настоящее время большинство ИТ-компаний предпочитают полагаться на облачные вычисления для предоставления своих услуг. Наконец, подходы на основе машинного и глубокого обучения являются эффективным решением для обнаружения любых подобных атак наряду с достаточными, актуальными и разнообразными обучающими данными.

Список использованных источников:

1. «Искусственный интеллект. Современный подход», Стюарт Рассел, Питер Норвиг 2021, с. 1409.

2. Ильяшенко О.Ю. Современное состояние развития облачных технологий / Ильяшенко О.Ю., Ильяшенко В.М., Лукьянченко Е.Л.//Экономика и предпринимательство. – 2020 - № 10. – С. 1219.1223.

3. «Практичный ИИ» Облачные технологии и машинное обучение, Ной Гифт, 2019, с. 304.

УДК 004

М.И. Галяува
Уфимский университет
науки и технологий, Уфа, Россия

Р.М. Яппаров
Уфимский университет
науки и технологий, Уфа, Россия

ЗАЩИТА ДАННЫХ ПОЛЬЗОВАТЕЛЯ В МЕССЕНДЖЕРАХ
PROTECTION OF USER DATA IN MESSENGERS

Аннотация: В статье раскрыты особенности защиты данных, связанные с использованием мессенджеров. Особоевниманиеуделяетсяпроблемамзащитыинформациииимерамбезопасности при использовании мессенджеров.

Abstract: The article reveals the features of data protection related to the use of messengers. Special attention is paid to the problems of information protection and security measures when using messengers.

Ключевые слова: Информация, информационная безопасность, пользовательские данные, мессенджеры, общение, мобильное приложение.

Keywords: Information, information security, user data, messengers, communication, mobile application.

Мессенджеры плотно вошли в жизнь пользователей сети Интернет, это обусловлено ростом количества пользователей смартфонов, а также широкими возможностями для коммуникации [1]. Согласно исследованиям 2023 года, рейтинг самых популярных мессенджеров по охвату аудитории возглавляют WhatsApp и Telegram. Помимо личных целей мессенджеры применяются для корпоративного общения между сотрудниками. То есть утечка данных из мессенджеров может нанести как ущерб личной информации, так и конфиденциальной информации компании.

Используя уязвимости в приложениях, злоумышленники используют методы социальной инженерии, фишинговых атак и внедрения вредоносного ПОдля кражи персональных данных, реквизитов банковских счетов и другой конфиденциальной информации [2].

Пользователь мессенджеров может столкнуться со следующими угрозами безопасности информации:

– слабые алгоритмы шифрования;

– вредоносные ссылки и файлы, содержащиеся в сообщениях от злоумышленников;

– взлом аккаунта и отправка сообщений;

– возможность доступа к переписке третьих лиц;

– раскрытие местоположения пользователя и др.

Во многих популярных на сегодняшний день мессенджерах применяется сквозное шифрование данных (end-to-endencryption, E2EE), что позволяет повысить уровень безопасности отправляемых сообщений. При данном типе шифрования сообщения шифруются на устройстве пользователя, который их отправляет, а расшифровка происходит только на устройстве получателя. Т.е. во время пути отправки информация находится в зашифрованном виде. Стоит отметить, что в Telegramреализован собственный протоколшифрования данных –MTProto.

Также одной из функций защиты является создание секретных чатов, для входа в которые требуется ввод дополнительного пароля или биометрическая аутентификация пользователя.

В некоторых приложениях (WhatsApp, Viber, Telegram, Signal и др.) содержится функция отправки «исчезающих сообщений». Т.е. сообщения могут быть полностью удалены после прочтения получателем либо после истечения заданного пользователем времени. Эта настройка отключена по умолчанию, поэтому для ее активации следует перейти в настройки приложения и установить таймер.

Данные из переписок могут храниться, как на устройствах пользователей, так и в облачных серверах. Например, вWhatsApp иViber переписка хранится только на устройствах пользователей и если злоумышленник сможет взломать платформу программы, то получить данные в открытом виде они просто не смогут. При этом создавая копию в облачном хранилище данные будут в незашифрованном виде, что подразумевает угрозу безопасности информации. В отличие от вышеперечисленных сервисов Telegramхранит информацию на защищенном сервере. А резервные копии данных хранятся в облачном хранилище в зашифрованном виде.

В настройках безопасности обоих мессенджеров также можно скрыть фотографию от всех пользователей или тех, кто не являетсяконтактом, существует возможностьскрытия последнего визита в приложение, а например, в мессенджере Telegram можно скрыть номер телефона и оставить только никнейм.

Одной из функций по защите информации, например, от третьих лиц и даже собеседника является блокировка создания фотографии экрана чата и уведомление пользователя о том, что собеседник сделал скриншот переписки.

Обезопасить профиль в мессенджере поможет двухфакторная аутентификация, которая для входа будет требовать введение кода из смс на номер телефона пользователя, биометрическая идентификация с помощью отпечатка пальца или распознавания лица. Даже в случае потери или кражи устройства мошенник не сможет осуществить вход без дополнительных сведений о пользователе [3].

Стоит отметить, что в число наиболее эффективных мессенджеров в вопросах защиты информации входят мессенджеры: Signal, AWS Wickr и Threema.Они используют более надежное шифрование данных, повышая уровень приватности данных. Их применение позволит повысить безопасность данных, а также защитит пользователя от утечки информации.

Высокая безопасность и анонимность данных при использовании мессенджеров зачастую связана с ущербом других функций, например, замедлением скорости работы самого приложения или скорости отправки сообщений. При выборе приложения для ежедневного общения пользователю следует выбирать оптимальный вариант, сочетающий баланс между удобством и безопасностью пользовательских данных.

Список использованных источников:

1. Благов, А.В. Анализ социальных сетей: учебное пособие / А.В. Благов, И.А. Рыцарев. – Самара: Самарский университет, 2020. – 104 с. – ISBN 978-5-7883-1556-0. – Текст: электронный // Лань: электронно-библиотечная система. – URL: https://e.lanbook.com/book/188862 (дата обращения: 11.04.2024).

2. Бондаренко, И.С. Информационная безопасность: учебник / И.С. Бондаренко. – Москва: МИСИС, 2023. – 254 с. – ISBN 978-5-907560-71-0. – Текст: электронный // Лань: электронно-библиотечная система. – URL: https://e.lanbook.com/book/360344 (дата обращения: 13.03.2024).

3. Свидетельство о государственной регистрации программы для ЭВМ № 2023686833 Российская Федерация. Биометрическая аутентификация пользователей информационной системы на основе искусственных нейронных сетей: № 2023685836: заявл. 22.11.2023: опубл. 08.12.2023 / Н.Д. Лушников, А.С. Исмагилова.

УДК 004

Е.И. Гвоздева
Уфимский университет
науки и технологий, Уфа, Россия

Научный руководитель:
И.В. Салов
Уфимский университет
науки и технологий, Уфа, Россия

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПРИ ОРГАНИЗАЦИИ УДАЛЕННОЙ РАБОТЫ
INFORMATION SECURITY IN THE ORGANIZATION OF REMOTE WORK

Аннотация: В статье раскрыты особенности защиты, связанные с организацией удаленной работы сотрудников. Особое внимание уделяется проблемам защиты информации и мерам безопасности при организации удаленной работы.

Abstract: The article reveals the features of protection related to the organization of remote work of employees. Special attention is paid to the problems of information protection and security measures when organizing remote work.

Ключевые слова: Информация, информационная безопасности, удаленный доступ, удаленная работа, удаленное рабочее место, VPN.

Keywords: Information, information security, remote access, remote work, remote workplace, VPN.

В настоящее время очень популярен формат удаленной работы сотрудников. Особую роль в этом сыграла пандемия COVID-19, когда многие организации переводили сотрудников на работу в дистанционном формате. Стоит отметить, что не все компании готовы работать в таком формате, а те, что готовы, не могут полноценно обеспечить защиту конфиденциальной информации, с которой работают сотрудники. Утечка конфиденциальной информации может привести к серьезным последствиям, поэтому очень важно выделить уязвимости и угрозы информационной безопасности (ИБ), а также средства и методы защиты данных при организации удаленной работы.

Основными проблемами при организации удаленного доступа, являются:

1. Невозможность использования многих технических средств защиты информации. Например, внедрение на каждое рабочее место

межсетевого экрана или глушителя связи является затратным и достаточно сложным. Привычные для офиса физические средства защиты (СКУД, сейфы, опечатывающие устройства, системы сигнализации) установить не получится.

2. Использование сотрудниками собственной техники для работы. Далеко не все организации способны предоставить сотрудникам полноценные рабочие места для работы, соответственно, приходится применять личную технику. Вероятность того, что устройство будет заражено вирусной программной или работник использует нелицензионное ПО, очень высока. Нет гарантии того, что ПК не будет заражен, что может привести к утечке данных.

3. Невысокий уровень защиты домашней сети. Часто пользователи не меняют заводские пароли от Wi-Fi или делают сеть общедоступной, отключая пароль вовсе. Установка и выбор VPN может показаться сложной задачей.

4. Низкий уровень защиты при обмене информацией. При переходе на удаленный формат работы общение между сотрудниками происходит через мессенджеры, электронную почту, видеоконференцсвязь и другие сервисы. Вероятность взлома аккаунтов очень высока, если не соблюдается должный уровень парольной защиты.

5. Основной проблемой, которую сейчас многие организации не могут решить является идентификация пользователя на протяжении всего рабочего дня. Подключиться к рабочему месту сотрудника моет любой человек, отследить, что в данный момент на рабочем месте находится именно тот сотрудник, а не злоумышленник достаточно проблематично.

Четкое разграничение прав доступа сотрудников при организации удаленной работы является необходимой мерой безопасности. Сотрудники должны иметь доступ только к той информации, которая им необходима и разрешена для работы в соответствии с выполняемыми компетенциями.

Также следует ввести регламент работы со служебной информацией и ознакомить с ним всех сотрудников. Например, возможно ограничить доступ к информации в соответствии с рабочим временем, если сотрудник в нерабочее время будет пользоваться данными, это может стать сигналом НСД.

Одной из эффективных мер информационной безопасности является регулярное обучение и повышение квалификации персонала по защите информации. Большая часть утечек информации связана с сотрудниками компании из-за невнимательности или незнания элементарных правил цифровой гигиены. Поэтому неотъемлемой частью совершенствования системы защиты и поддержания необходимого уровня является обучение.

Обеспечить защиту информации только организационными мерами нельзя, нужно применять и технические средства защиты. Реализация может заключаться в следующем:

– постоянная аутентификация сотрудников посредством ввода пароля, смс-сообщения на телефон сотрудника или аппаратного токена;

– установка антивирусного программного обеспечения на устройства;

– применение корпоративных VPN-сервисов для защищенного соединения между устройством пользователя и сервером;

– использование двухфакторной аутентификации;

– внедрение средств мониторинга устройств и анализа действий;

– передача файлов и информации в зашифрованном виде;

– применение лицензионного программного обеспечения;

– систематическая смена паролей и усиление парольной защиты;

– своевременное обновление и проверка системы и ПО;

– использование только рабочих накопительных устройств и др.

Как было отмечено ранее, основной проблемой, которую в настоящее время трудно решить – это идентификация пользователя на протяжении всего времени работы. Помочь в этом может программный комплекс «Стахановец».

Функциональные возможности комплекса «Стахановец» весьма широкие и включают в себя: снимки и видеозапись с веб-камеры, а также микрофона с целью идентификации, а также понимая состояния сотрудника; контроль присутствия и активности сотрудника в рабочее время на рабочем месте; контроль и мониторинг рабочего стола сотрудника (возможность удаленного подключения); мониторинг запускаемых программ; мониторинг веб-трафика (посещение сайтов, отправка файлов и контроль почты); перехват ввода текста с клавиатуры; контроль и блокировка подключаемых устройств (флеш-накопители, диски и др.); контроль печати и др.

Программный комплекс «Стахановец» является устройством с широким функционалом, который в условиях удаленной работы позволяет выявить бизнес-риски, связанные с утечкой информации. Если программа понимает, что идет нарушение безопасности, то руководству организации будет сформирован и отправлен отчет. Также существует возможность формировать отчеты о деятельности сотрудников в рабочее время и оценки их эффективности.

Список использованных источников:

1. Бондаренко, И. С. Информационная безопасность: учебник / И.С. Бондаренко. – Москва: МИСИС, 2023. – 254 с. – ISBN 978-5-907560-

71-0. – Текст: электронный // Лань: электронно-библиотечная система. – URL: https://e.lanbook.com/book/360344 (дата обращения: 13.03.2024).

2. Давидюк, Н.В. Мониторинг безопасности информационных систем: учебное пособие / Н.В. Давидюк, И.М. Космачева. – Санкт-Петербург: Интермедия, 2020. – 116 с. – ISBN 978-5-4383-0204-9. – Текст: электронный // Лань: электронно-библиотечная система. – URL: https://e.lanbook.com/book/161352 (дата обращения: 13.03.2024).

3. Космачева, И.М. Проектирование защищенных баз данных: учебное пособие / И.М. Космачева, Н.В. Давидюк. – Санкт-Петербург: Интермедия, 2020. – 144 с. – ISBN 978-5-4383-0191-2. – Текст: электронный // Лань: электронно-библиотечная система. – URL: https://e.lanbook.com/book/161362 (дата обращения: 13.03.2024).

4. Шевченко, О.А. Удаленка. Дистанционная (удаленная) работа. Комментарий законодательства и схемы: учебное пособие / О.А. Шевченко, К.С. Балицкий, Е.А. Кашехлебова. – Москва: Проспект, 2021. – 31 с. – ISBN 978-5-392-34278-5. – Текст: электронный // Лань: электронно-библиотечная система. – URL: https://e.lanbook.com/book/281033 (дата обращения: 13.03.2024).

УДК 004

Д.Р. Давлетова
Уфимский университет
науки и технологий, Уфа, Россия

Научный руководитель:
И.А. Шагапов
Уфимский университет
науки и технологий, Уфа, Россия

АКУТАЛЬНЫЕ ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ В СОВРЕМЕННЫХ УСЛОВИЯХ
THE ACTUAL PROBLEMS OF ENSURING THE SECURITY OF CRITICAL INFORMATION INFRASTRUCTURE IN MODERN CONDITIONS

Аннотация: В статье кратко описываются актуальные проблемы обеспечения безопасности критической информационной инфраструктуры и рассматриваются предложения для совершенствования защиты информации.

Abstract: The article briefly describes the current problems of ensuring the security of critical information infrastructure and discusses proposals for improving information security.

Ключевые слова: Критическая информационная инфраструктура, защита информации, киберугрозы, атака.

Keywords: Critical information infrastructure, information security, cyber threats, attack.

В современных условиях обеспечение безопасности критической информационной инфраструктуры является одним из наиболее важных и актуальных вопросов.

Критическая информационная инфраструктура - объекты критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия таких объектов. [1]

На данный момент обеспечение безопасности критической информационной инфраструктуры (КИИ) сталкивается с большим количеством актуальных проблем и задач:

1. Киберугрозы нового поколения. Появление новых технологий, таких как искусственный интеллект (ИИ), облачные вычисления и интернет вещей (IoT), приводит к появлению новых уязвимостей и потенциальных угроз для КИИ.
2. Киберпреступники могут атаковать критическую инфраструктуру через с помощью различных каналов. Они включают в себя физические вмешательства, социальную инженерию и кибератаки.
3. Трудности управления большими объемами данных. В современной КИИ хранятся и обрабатываются большие объемы данных. В связи с этим появляются сложности в управлении и обеспечении безопасности этой информации.
4. Недостаточная защита от киберугроз. Большое количество организаций и государств сталкиваются с проблемой слабой защиты своих критических информационных систем. Это может быть связано с отсутствием квалифицированных специалистов в области информационной безопасности, недостаточными бюджетными средствами и сложностью внедрения и поддержания современных средств защиты.

Рисунок 1 – Объем закупок ПО в 2021 г.

Рисунок 2 – Объем закупок ПО в 2023 г.

В 2023 году увеличилось число атак на веб-ресурсы организаций. [3]

Рисунок 3 – Число атак на веб-ресурсы компаний

Большое количество серьезных кибератак в Российской Федерации сосредоточены на государственные учреждения. 10 апреля 2023 года Федеральная таможенная служба России пострадала от хакерской атаки. В результате была приостановлена работа Единой автоматизированной информационной системы таможенных органов. [4] Это привело к значительным финансовым потерям.

В 2023 году количество кибератак увеличилось на 27,5%. Это указывает на увеличение роли защиты КИИ.

Предложения для обеспечения безопасности критической информационной инфраструктуры:

Мониторинг событий информационной безопасности и анализ безопасности. Анализировать и подробно расследовать события и инциденты информационной безопасности следует не только для выявления потенциальных угроз и слабых мест, но и для предотвращения повторений кибератак.

Разработка и реализация строгой политики управления доступом, которая определяет права доступа к критическим данным и системам на основе принципа минимальных привилегий.

Физическая безопасность. Системы и оборудование КИИ должны быть защищены от физического доступа несанкционированных лиц. Это может включать в себя использование биометрических систем доступа, видеонаблюдение, ограниченный доступ и т.д.

Внедрение многоуровневой системы защиты, включая межсетевые экраны, системы обнаружения вторжений, системы предотвращения

утечки данных и антивирусные программы для обнаружения и предотвращения кибератак.

Регулярное обновление программного обеспечения и операционных систем с целью устранения уязвимостей и поддержания высокого уровня защиты.

Внедрение механизмов шифрования данных на уровне передачи и хранения, чтобы предотвратить несанкционированный доступ к конфиденциальной информации.

Проведение регулярных аудитов безопасности для выявления потенциальных уязвимостей и слабых мест в инфраструктуре, а также незамедлительное исправление обнаруженных проблем.

Список использованных источников:

1. Федеральный закон от 26 июля 2017 г. N 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» [Электронный ресурс] // КонсультантПлюс: справочно-правовая система / URL: https://www.consultant.ru/document/cons_doc_LAW_220885/ (дата обращения 17.04.2024).

2. ГОСТ Р 56546-2015 «Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем» - Введ. 2016-04-01 [Электронный ресурс] // Кодекс: справочно-правовая система/ Режим доступа: URL: https://docs.cntd.ru/document/1200123702 (дата обращения 17.04.2024).

3. Кибербезопасность в 2023–2024 гг. – URL: https://www.ptsecurity.com/ru-ru/research/analytics/kiberbezopasnost-v-2023-2024-gg-trendy-i-prognozy-chast-tretya/ (дата обращения 17.04.2024).

4. Атаки на КИИ – URL: https://repost.press/news/ataki-na-kii-novyj-instrument-gibridnoj-vojny (дата обращения 17.04.2024).

УДК 004.75

Б.А. Ерушев
Магнитогорский государственный технический
университет им. Г.И. Носова, Магнитогорск, Россия

Научный руководитель:
И.И. Баранкова
Магнитогорский государственный технический
университет им. Г.И. Носова, Магнитогорск, Россия

АНАЛИЗ АТАК НА ОБЛАЧНЫЕ СЕРВИСЫ
ANALYSIS OF ATTACKS ON CLOUD SERVICES

Аннотация: Статья анализирует безопасность облачных услуг IaaS, подчеркивая сложности модели безопасности из-за зависимости от многочисленных компонентов. Используя сканеры уязвимостей, авторы выявили уязвимости, включая сертификаты SSL и перенаправление HTTP-запросов. Помимо этого, рассматривается модели атак, такие как Man-in-the-Cloud и DDoS. В заключении предложены рекомендации, включая ограничение доступа и периодическое отзывание токенов, для улучшения безопасности облачных вычислений.

Abstract: The article analyzes the security of IaaS cloud services, emphasizing the complexities of the security model due to reliance on numerous components. Using vulnerability scanners, the authors identified vulnerabilities including SSL certificates and HTTP request redirection. Additionally, attack models such as Man-in-the-Cloud and DDoS are discussed. In conclusion, recommendations are provided, including access restriction and periodic token revocation, to enhance cloud computing security.

Ключевые слова: Информационная безопасность, облачные вычисления, инфраструктура, угрозы безопасности.

Keywords: Information security, cloud computing; infrastructure, security threats.

Модель облачных услуг IaaS предполагает зависимость от сложенных компонентов облака, что дополнительно усложняет модель безопасности. Безопасность каждого слоя зависит от безопасности всех нижележащих слоев. Однако каждый слой отличается в контрольных механизмах безопасности, поскольку у каждого свои требования и уязвимости в

области безопасности. Любое нарушение безопасности в любом из слоев непременно повлияет на безопасность всей облачной среды.

Оценки были проведены сначала с использованием сканера Nmap, а затем с использованием Nessus и Armitage. Результаты сканера Nmap позволили определить активные узлы в сети, а также получить сведения об операционной системе, открытых портах и работающих службах. Полученная информация из сканирования IP-адресов и портов помогла определить, какие хосты нужно сканировать на наличие уязвимостей. С использованием Nessus и Armitage было проведено сканирование сервера и обнаружены различные уязвимости, связанные с открытыми портами.

Изучение уязвимостей может помочь злоумышленникам в их эксплуатации. Nessus классифицирует обнаруженные уязвимости в зависимости от их степени риска с использованием оценки уязвимости, назначенной Общей системой оценки уязвимости (CVSS). Например, сканер Nessus обнаружил уязвимость среднего уровня, утверждая, что сертификат SSL сервера не может быть доверен. Эту уязвимость может использовать злоумышленник для проведения атак типа Man-in-the-Cloud на удаленный хост. Еще одна уязвимость среднего уровня, обнаруженная Nessus, — это перенаправление POST-запросов HTTP Proxy, которое может позволить атакующему пройти через брандмауэр, подключившись к чувствительным портам, таким как порт 23, с использованием прокси. Более того, сканер уязвимостей Armitage обнаружил различные уязвимости. Однако успешно скомпрометировать цель при попытке вручную или автоматически использовать уязвимости с помощью модуля атак Armitagene не вышло. Тем не менее, атака методом грубой силы с использованием модуля ssh_login успешно предоставила доступ к цели и открыла сессию, которая использовалась для взаимодействия и загрузки задней двери для поддержания доступа к цели.

Как изображено во Второй фазе, была смоделирована атака Man-in-the-Cloud на файл аутентификации Dropbox. Результаты эксперимента показали, что злоумышленники могут передавать файлы аутентификации пользователей на другое устройство, что может привести к несанкционированному удаленному доступу, мошенничеству с идентификацией, краже конфиденциальной информации или даже реализации вредоносного программного обеспечения. Man-in-the-Cloud является угрозой для большого количество учетных записей из-за популярности этих учетных записей не только для личного использования, но и в крупных организациях. Вторая смоделированная атака во Второй фазе — это атака DDoS, которая окажет отрицательное воздействие на работу облачной среды. Ресурсы, такие как сетевая пропускная способность и память, будут недоступны для законных пользователей из-за высокого потребления как HTTP-DoS, так и SYN-флуда

Как показано в Третьей фазе экспериментальной рамки, существует множество бесплатных программных средств и решений для защиты критических активов при развертывании облачной вычислительной среды. Некоторые инструменты могут предоставлять уровень защиты и одновременно контролировать, и наблюдать за использованием общего пула ресурсов. Эти методики позволяют администраторам облачных вычислений контролировать сетевой трафик, уязвимые ВМ, уязвимости в предоставляемых услугах и приложениях с целью обеспечения максимальной защиты, которая является главной целью для любого облачного провайдера. Доступные инструменты могут быть использованы для шифрования данных, которые синхронизируются, хранятся или обрабатываются.

Ниже приведены рекомендации по применению лучших практик в качестве контрмер, когда речь заходит о безопасности облачных вычислений:

– Поставщики синхронизации файлов должны внедрить ограничение доступа к учетной записи для конкретного набора устройств, идентифицированных владельцем учетной записи.

– Пользователям должно поступать уведомление о необычном доступе к учетной записи, отправляя предупредительные электронные письма или сообщения.

– Пользователи должны явно отзывать все токены периодически.

– Предприятия должны улучшать безопасность, используя контролируемые решения доступа к облаку; это решение направлено на мониторинг использования и доступа к облачным сервисам.

Список использованных источников:

1. Безопасность облачных сервисов: практическое руководство / Н. Павлов, Д. Хлобыстов, А. Петров // Питер, 2018.

2. Баранкова И.И., Михайлова У.В., Лукьянов Г.И. Формирование компетенций специалиста по информационной безопасности // Актуальные проблемы современной науки, техники и образования Тезисы докладов 77-й международной научно-технической конференции. 2019.

3. Безопасность облачных сервисов / А.В. Хмелев // БХВ-Петербург, 2018.

УДК 0.04.056.5

Б.И. Зайнуллин
Уфимский университет
науки и технологий, Уфа, Россия

Научный руководитель:
Н.Г. Миронова
Уфимский университет
науки и технологий, Уфа, Россия

ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ РЕШЕНИИ ЗАДАЧИ МИГРАЦИИ ИС ОРГАНИЗАЦИИ НА ОТЕЧЕСТВЕННЫЕ ПЛАТФОРМЫ
INFORMATION SECURITY PROBLEMS IN SOLVING THE PROBLEM OF MIGRATING AN ORGANIZATION'S INFORMATION SYSTEM TO DOMESTIC PLATFORMS

Аннотация: Проблемы информационной безопасности при миграции информационных систем организаций на отечественные платформы. Рассматриваются основные угрозы и риски, связанные с этим процессом, а также предлагаются практические подходы к их решению. Анализируются технические и организационные аспекты обеспечения безопасности при переходе на отечественные платформы с целью минимизации потенциальных уязвимостей и угроз.

Abstract: Problems of information security in the migration of information systems of organizations to domestic platforms. The main threats and risks associated with this process are considered, and practical approaches to their solution are proposed. The technical and organizational aspects of ensuring security during the transition to domestic platforms are analyzed in order to minimize potential vulnerabilities and threats.

Ключевые слова: Миграция информационных систем, Отечественные платформы, Информационная безопасность, Угрозы и риски.

Keywords: Migration of information systems, Domestic platforms, Information security, Threats and risks.

В современных условиях глобализации и цифровизации информационные системы становятся ключевыми элементами инфраструктуры любой организации. Однако зависимость от иностранных технологий и платформ создает значительные риски, связанные с информационной безопасностью и суверенитетом данных. В связи с этим, миграция информационных систем на отечественные платформы

становится не только вопросом экономической целесообразности, но и стратегической безопасности. В данной статье рассматриваются проблемы информационной безопасности, возникающие при переходе на отечественные платформы, а также предлагаются пути их решения.

Основная мысль данной статьи заключается в том, что процесс миграции информационных систем на отечественные платформы, хотя и сопряжен с рядом проблем и рисков в области информационной безопасности, является необходимым шагом для обеспечения национальной кибербезопасности и технологического суверенитета. Важно тщательно продумать и реализовать меры, направленные на минимизацию этих рисков.

Одной из ключевых проблем при миграции ИС является обеспечение сохранности и конфиденциальности данных. Перенос больших объемов информации на новые платформы связан с риском утраты или компрометации данных. Это может происходить как в процессе передачи, так и при хранении на новых системах. Нарушение конфиденциальности данных может привести к серьезным последствиям, включая утрату коммерческой тайны, нарушение законодательства о защите персональных данных и значительные репутационные потери.

Переход на отечественное программное обеспечение и оборудование представляет собой стратегическое решение, сопряженное с финансовыми и техническими вызовами для компаний. Одним из основных аспектов, вызывающих недовольство, является вопрос окупаемости проекта. Внедрение отечественного ПО и оборудования требует значительных финансовых вложений, что может вызвать сопротивление внутри компании, особенно если уже были вложены средства в предыдущее решение.

Отечественные платформы, несмотря на усилия разработчиков, могут содержать уязвимости, которые могут быть использованы злоумышленниками. Недостаточная зрелость некоторых отечественных решений увеличивает вероятность наличия уязвимостей, которые могут быть использованы для атак на информационные системы. Этот аспект требует особого внимания, так как отсутствие своевременного обнаружения и устранения уязвимостей может привести к масштабным инцидентам безопасности.

При миграции ИС часто возникает необходимость интеграции новых платформ с уже существующими системами и приложениями. Несовместимость технологий может привести к созданию дополнительных точек уязвимости и сложностям в защите информации. Проблемы интеграции могут также повлиять на стабильность и производительность систем, что негативно скажется на бизнес-процессах организации.

Миграция на новые платформы требует наличия специалистов, обладающих необходимыми знаниями и навыками. В условиях дефицита квалифицированных кадров возникает риск неправильной настройки систем безопасности, что может привести к возникновению уязвимостей. Обучение сотрудников новым технологиям и методам защиты информации становится критически важным элементом успешной миграции.

Процесс миграции может столкнуться с рядом правовых и регуляторных барьеров, связанных с защитой персональных данных и информационной безопасностью. Несоблюдение законодательных требований может повлечь за собой серьезные юридические последствия. Важно учитывать все правовые аспекты при планировании и реализации миграции информационной системы.

Переход на новое ПО влечет за собой импорт всего объема данных и накопленной информации компании.

Это требует значительного времени и проверки правильности переноса данных, что вызывает опасения среди компаний.

Сложности адаптации персонала к новой системе также играют важную роль. В определенный момент времени прежняя система становится привычнее для пользователей, и персонал может не желать принимать нововведения. Поэтому важно провести тестовый период и обучить сотрудников работе в новой системе.

Для решения этих проблем необходимо разработать и внедрить комплексную стратегию миграции, включающую тщательное планирование всех этапов переноса данных, начиная от подготовки и заканчивая интеграцией с существующими системами. Важно предусмотреть меры по защите данных на каждом этапе миграции. Перед началом миграции необходимо провести детальный аудит безопасности выбранных отечественных платформ. Это позволит выявить и устранить потенциальные уязвимости до начала использования систем в рабочем режиме. Обучение и повышение квалификации специалистов позволит минимизировать риски, связанные с неправильной настройкой и эксплуатацией систем.

Сотрудничество с государственными регуляторами и частными компаниями, занимающимися кибербезопасностью, позволит учитывать все правовые аспекты и обеспечить соблюдение законодательства в области защиты информации. После завершения миграции необходимо организовать постоянный мониторинг работы новых платформ и регулярное обновление систем безопасности. Это позволит оперативно выявлять и устранять новые уязвимости.

Миграция информационных систем на отечественные платформы представляет собой сложный и многоступенчатый процесс, сопряженный

с множеством рисков в области информационной безопасности. Однако, при правильном подходе и внедрении комплексных мер по защите данных, эти риски можно значительно снизить. Обеспечение безопасности информации при миграции ИС является ключевым фактором для достижения технологической независимости и национальной кибербезопасности.

Список использованных источников:

1. Васильков А.В. Безопасность и управление доступом в информационных системах / А.В. Васильков, И.А. Васильков. – Москва: ФОРУМ: ИНФРА-М, 2018. – 368 с.

2. Жигулин Г.П. Организационное и правовое обеспечение информационной безопасности / Г.П. Жигулин. – Санкт-Петербург: СПбНИУИТМО, 2014. – 173 с.

3. ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. [Электронный ресурс]. URL: https://docs.cntd.ru/document/1200057516 (дата обращения 20.04.2024).

УДК 004

А.И. Зарипова
Уфимский университет
науки и технологий, Уфа, Россия

Научный руководитель:
И.А. Шагапов
Уфимский университет
науки и технологий, Уфа, Россия

СПЕЦИФИКА СОЗДАНИЯ СПЕЦИАЛИЗИРОВАННОЙ ОРГАНИЗАЦИИ ДЛЯ ХРАНЕНИЯ КОНФИДЕНЦИАЛЬНЫХ ДОКУМЕНТОВ И НОСИТЕЛЕЙ, КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ
THE SPECIFICS OF CREATING A SPECIALIZED ORGANIZATION FOR STORING CONFIDENTIAL DOCUMENTS AND MEDIA, CONFIDENTIAL INFORMATION

Аннотация: Статья исследует различные методы обеспечения конфиденциальности при хранении документов, включая использование

специальных контейнеров, шифрования для электронных документов и управление доступом. Статья также затрагивает вопрос важности физической безопасности хранилищ и аудита доступа для защиты чувствительных данных.

Необходимо знать о важности физической безопасности хранилищ и управления доступом к помещениям, где хранятся конфиденциальные документы. Освещая роль ограниченного доступа и систем видеонаблюдения, статья предлагает практические советы по обеспечению безопасности при хранении чувствительных данных.

Annotation: The article explores various methods of ensuring confidentiality when storing documents, including the use of special containers, encryption for electronic documents and access control. The article also addresses the importance of physical storage security and access auditing to protect sensitive data.

It is necessary to be aware of the importance of physical security of storage facilities and access control to the premises where confidential documents are stored. Highlighting the role of restricted access and video surveillance systems, the article offers practical tips on ensuring security when storing sensitive data.

Ключевые слова: Конфиденциальность, безопасность, хранение, доступ, информационная безопасность, защита информации

Keywords: Confidentiality, security, storage, access, information security, information protection

Ежегодно предприятия накапливают огромное количество документов и записей, которые требуют постоянного хранения и управления на протяжении всего их жизненного цикла. В зависимости от отрасли периоды хранения могут варьироваться от пяти лет и более, что делает потребность в большем пространстве растущей проблемой для многих организаций.

Однако найти безопасное место для хранения на рабочем месте не всегда возможно. Хранение документов дома также требует больших затрат и времени. Лучшим решение: это хранение конфиденциальных документов в защищенном удаленном хранилище, чтобы организация могла сосредоточиться на деятельности, приносящей доход, одновременно повышая информационную безопасность.

Основная цель удаленного хранения документации − переместить важные файлы и документы из уязвимых складских помещений на рабочих местах и мест самостоятельного хранения в безопасное помещение.

Внешнее хранение записей также является экономически эффективным и долгосрочным решением, которое защищает информацию от кражи, нарушений безопасности и стихийных бедствий, таких как пожар или наводнение.

Выбор безопасного хранилища документов для конфиденциальных данных дает множество преимуществ:

– Перераспределяет дорогостоящую офисную недвижимость для использования в целях приносящей доход деятельности.

– Повышает производительность сотрудников, обеспечивая быстрый и легкий доступ к информации.

– Обеспечивает соблюдение законов о конфиденциальности в отношении управления и доступности данных.

– Помогает отслеживать периоды хранения и уничтожать записи, чтобы освободить место в инвентаре.

– Меры безопасности защищают бизнес-активы от кражи, ущерба окружающей среде, потери или несанкционированного доступа.

Когда сотрудничаете с поставщиком удаленного хранилища документов, весь процесс хранения и управления файлами выполняется обученными профессионалами. Поставщик организует безопасную транспортировку деловых записей в удаленное хранилище, где информация будет проиндексирована и сохранена с использованием системы штрих-кодов, чтобы упростить поиск, нахождение и запрос файлов. Если нужен доступ к информации, ее можно отсканировать и отправить по электронной почте в течение нескольких часов или физические документы могут быть доставлены на объект.

Использование офисных помещений для хранения конфиденциальных бумажных документов или отдельного хранилища обходится дорого, и его не всегда легко найти. Также должны учитывать текущие расходы, включая оплату труда сотрудников, аренду, стеллажи для хранения документов и ящики для документов.

Более экономичное решение − обратиться к профессиональной службе управления записями. Всего за несколько тысяч рублей за коробку в год можете хранить свои документы и медиафайлы в помещении с контролируемым климатом, с круглосуточным наблюдением и строгими протоколами безопасности. Благодаря этому можно оплачивать только то пространство, которое используется для хранения файлов, что делает его более доступным в условиях офиса.

В отличие от использования офисных помещений или помещений индивидуального хранения для хранения файлов, в удаленных хранилищах документов ведется круглосуточное наблюдение и соблюдаются строгие протоколы безопасности для защиты информации от взлома и кражи. Только уполномоченный персонал имеет доступ к записям, и все сотрудники регулярно проходят обучение по соблюдению правил защиты данных. Также предусмотрены надлежащие меры климат-контроля, противопожарной защиты и борьбы с вредителями, чтобы предотвратить повреждение или потерю файлов в безопасном хранилище [1].

Если нужен доступ к документам компании, внешние хранилища предлагают различные способы поиска. Если нужны физические документы, файлы или коробки можно запросить онлайн в хранилище и доставить в компанию.

Однако более эффективный способ получить доступ к записям − обратиться к поставщику удаленного хранилища, который предлагает услуги сканирования по требованию. Благодаря этой форме поиска файлов сотрудники могут связаться с компанией, чтобы запросить сканирование документов и отправку им по электронной почте в течение нескольких часов.

Хранение конфиденциальных документов в удаленном помещении позволяет компании соответствовать законам о конфиденциальности в том, что касается управления данными и их доступности. Когда срок хранения информации подходит к концу, уполномоченный персонал может легко определить, какие бумажные документы и носители информации истекли и требуют уничтожения [2].

Все файлы и ящики также индексируются и сканируются на каждом этапе пути, чтобы обеспечить безопасную цепочку хранения и постоянное соблюдение требований.

Список использованных источников:

1. Внуков, А.А. Защита информации: учебное пособие для бакалавриата и магистратуры / А.А. Внуков. – М.: Юрайт, 2019. – 240 с.

2. Гришина, Н.В. Информационная безопасность предприятия: учебное пособие/ Н.В. Гришина. – М.: Форум: ИНФРА-М, 2018. – 238 с.

УДК 004.056

А.И. Зыков
Уфимский университет
науки и технологий, Уфа, Россия

Научный руководитель:
М.Р. Шафиков
Уфимский университет
науки и технологий, Уфа, Россия

КИБЕРТЕРРОРИЗМ КАК УГРОЗА ОСНОВАМ КОНСТИТУЦИОННОГО СТРОЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
CYBERTERRORISM AS A THREAT TO THE CONSTITUTIONAL ORDER OF THE RUSSIAN FEDERATION

Аннотация: В статье рассматривается проблема кибертерроризма. Акцент сделан на кибертерроризм в контексте его потенциальной угрозы для конституционного строя Российской Федерации. Значительное внимание в статье уделяется критической информационной инфраструктуре как главному объекту воздействия кибертеррористов, а также обеспечению ее безопасности с помощью мер и средств, определенных российским законодательством.

Annotation: In the article it is considered the problem of cyberterrorism. The emphasis is placed on cyberterrorism in the context of its potential threat to the constitutional order of the Russian Federation. The article pays considerable attention to the critical information infrastructure as the main target of cyberterrorists, as well as ensuring its security through measures and means defined by the Russian legislation.

Ключевые слова: Кибертерроризм, киберпреступность, угрозы безопасности, информационная безопасность, критическая информационная инфраструктура.

Keywords: Cyberterrorism, cybercrime, security threats, information security, critical information infrastructure.

Конституционный строй – система правовых отношений, закрепляющая способ организации государства, при котором признаются и гарантируются права и свободы человека и гражданина, а государство подчинено праву и демократической Конституции [1]. Кибертерроризм же направлен на дестабилизацию страны и полное игнорирование конституционного строя.

Кибертерроризм – целенаправленная атака на киберпространство, или информационные ресурсы, которая угрожает опасности и угрозе

современному обществу, что может повлечь за собой особо тяжкие последствия, если такая атака совершается с целью нарушения безопасности общества, угрозе людей или к провокационным действиям терроризма [2].

Кибертеррористы своей приоритетной целью ставят нарушение устойчивого развития и целостности государства. Поэтому большинство кибератак направлены на наиболее важные объекты государства – критическую информационную инфраструктуру (КИИ). Защита данных критической информационной инфраструктуры не просто необходимость, – это способ предотвращения кибератак, которые могут иметь разрушительные последствия для национальной безопасности и благополучия граждан

По Федеральному закону от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры» под КИИ понимаются информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, т.е. объекты критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия таких объектов.

Исследование, проведенное «К2 Тех» в конце 2023 года, выявило, что 32% субъектов КИИ сталкивались с различными инцидентами безопасности. Минимум 35% из этих случаев привели к финансовым убыткам. Самым частым результатом таких инцидентов, в основном вызванных DDoS-атаками и взломами сайтов, являются простои.

С каждым годом неуклонно растет количество атак на объекты КИИ. Так, отечественными специалистами было отражено более 65 тысяч атак на объекты критической информационной инфраструктуры в 2023 году [3].

Согласно ФСТЭК, на начало 2024 года основными причинами успеха кибератак на объекты КИИ являются: слабые пароли пользователей и администраторов, однофакторная идентификация, использование паролей, установленных по умолчанию, активные учетные записи уволенных сотрудников, использование для доступа к информационной инфраструктуре личных устройств работников, использование на рабочих местах личных мессенджеров и социальных сетей [4].

Согласно Приказу ФСТЭК № 235, система безопасности объекта КИИ строится на применении правовых, организационных, технических и иных мер, направленных на обеспечение устойчивого функционирования объектов КИИ, при этом создаваемые системы безопасности должны соответствовать предъявляемым требованиям к: силам обеспечения безопасности КИИ (ответственному структурному подразделению и работникам), средствам (программным и программно-аппаратным) и организационно-распорядительным документам (ОРД).

Приказом ФСТЭК № 239 устанавливаются требования к защите объектов КИИ и их данных. В зависимости от категории значимости объекта КИИ должны быть меры защиты информации, показанные на рисунке 1.

Также, при построении защиты КИИ и его данных необходимо учитывать и другие руководящие документы в области обеспечения безопасности информации (например, ФСТЭК России от 11.02.2013 № 17 для ГИС или Постановления Правительства РФ от 01.11.2012 № 1119 для ИСПДн).

Рисунок 1 – Меры обеспечения безопасности данных КИИ

Немаловажной мерой обеспечения безопасности КИИ РФ является создание. Система представляет собой иерархически связанные ведомственные и корпоративные Центры ГосСОПКА, обменивающиеся информацией о зафиксированных атаках, методах их предотвращения и устранения последствий кибератак.

Таким образом, большинство кибертеррористических атак направлено на объекты КИИ. Применение комплекса разнообразных мер защиты, включая технические, физические, организационные меры, соответствующие требованиям правового регулирования в области КИИ, позволит существенно снизить уязвимость таких объектов к кибератакам, обеспечить эффективное обнаружение и оперативное реагирование на потенциальные угрозы.

Список использованных источников:

1. Дудка, О.Ф., Михеенков, Е.Г. Правоведение: курс лекций [Текст] / О.Ф. Дудка, Е.Г. Михеенков. – Часть 1. – Томск: Издательство СибГМУ, 2021. – 168 с.

2. Стенькина, Е.Н. Кибербезопасность, как основной фактор национальной и международной безопасности в отрасли экономики:

тенденции, базовые понятия и термины [Текст] / Е.Н. Стенькина – Москва: Первое экономическое издательство, 2021. – 258 с.

3. В 2023 году было отражено 65 тысяч атак на объекты КИИ / [Электронный ресурс] // IT Channel News: новости ИТ-канала: [сайт]. – URL: https://www.novostiitkanala.ru/news/detail.php?ID=175107 (дата обращения: 10.04.2024).

4. ФСТЭК назвала 6 главных причин успешных кибератак на предприятия и госорганы / [Электронный ресурс] // Геоинформ: [сайт]. – URL: https://www.geoinform.su/blog/fstehk-nazvala-6-glavnykh-prichin-uspeshnykh-kiberatak-na-predprijatija-i-gosorgany (дата обращения: 10.04.2024).

УДК 004.056.5 (075)

К.О. Карлышева, Т.В. Корноухова
Поволжский государственный университет
телекоммуникаций и информатики, Самара, Россия

Научный руководитель:
М.А. Буранова
Поволжский государственный университет
телекоммуникаций и информатики, Самара, Россия

МЕТОДЫ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ДЛЯ КОРРЕЛЯЦИИ СОБЫТИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
ARTIFICIAL INTELLIGENCE METHODS FOR CORRELATING INFORMATION SECURITY EVENTS

Аннотация: Важной задачей в обеспечении информационной безопасности инфокоммуникационных систем является оперативное и точное реагирование на инциденты. Важным инструментом для этого на современном этапе являются информационно-аналитические системы. При реализации данных систем используют различные механизмы, основанные на определении корреляции. Поиск новых методик определения корреляций, их классификация являются важными задачами в области информационной безопасности.

Abstract: An important task in ensuring information security of infocommunication systems is prompt and accurate response to incidents. An important tool for this at the present stage is information and analytical systems.

When implementing these systems, various mechanisms based on determining correlation are used. The search for new methods for determining correlations and their classification are important tasks in the field of information security.

Ключевые слова: Корреляция, искусственный интеллект, машинное обучение.

Keywords: Correlation, artificial intelligence, machine learning.

В инфокоммуникационных системах существующие методы не всегда в состоянии достаточно эффективно и оперативно выполнять задачи защиты. Для повышения эффективности используют средства защиты информации, относящиеся к классу информационно-аналитических систем безопасности. Как известно, в данных системах широко применяются методы, основанные на определении корреляции.

Корреляции данных в инфокоммуникационных системах связана с некоторыми проблемами, главные из которых это весьма неопределенная инфраструктура. Кроме того, определенные трудности вносит тот факт, что источники, генерируют разнородный трафик большого объема, и объем трафика возрастает ежегодно. Это происходит на фоне все возрастающей сложности и скрытости потенциальных атак. Несмотря, но то, что исследованию методов корреляции данных научным сообществом уделяется достаточно большое внимание на протяжении более чем двадцати лет, даже современные методики еще требуют или ручной настройки, или настройки в автоматизированном режиме под решение конкретных задач.

Однако это, в свою очередь, требует достаточно подробного анализа имеющихся инструментов для активной защиты (например, корреляции) для разработки более эффективных и простых в использовании подходов. В последние годы исследования в данной области направлены на изучение методов искусственного интеллекта, в частности методов машинного обучения [1,2].

Следует учесть, что внедрение в высокопроизводительные системы машинного обучения весьма затруднительно и внедрение их в индустрию информационной безопасности недостаточно быстрое. Для этого есть несколько причин, например, отсутствие прозрачности (системы считаются «черными ящиками»), сложные конфигурации и большие размеры моделей сложные для понимания людьми, их корректность и надежность сложно проверить. Это в свою очередь требует глубокого изучения методов машинного обучения и анализа при внедрении в системы информационной безопасности. Возможно внимание здесь следует уделить применения комбинированной методики корреляции [3, 4].

В аналитических подходах, позволяющих прогнозировать некоторые события, корреляции событий безопасности позволяют анализировать как имеющиеся и хранящиеся данные, так и события в реальном времени и автоматически определять изменяющиеся пороговые значения. Это позволяет обнаруживать аномальные события и предотвращать кибератаки на ранних стадиях. Корреляция событий безопасности также находит применение в расследовании инцидентов, когда необходимо исследовать источник атаки и инициирующие события. Большинство исследователей рассматривают подходы к корреляции событий с точки зрения применяемых методов. В целом выделяют три основные группы методов корреляции событий: основанные на сходстве, последовательности и конкретных случаях или знаниях [5-7].

Для корреляции широко используются методы искусственного интеллекта. Из них можно выделить следующие модели: модели, основанные на правилах, семантические модели, графические модели, модели машинного обучения. В целом методы искусственного интеллекта, используемые для корреляции событий, это те же методы, которые используются в целом в задачах информационной безопасности.

Одним из возможных методов корреляционного анализа, используемых в машинном обучении является применение методов, основанных на вероятностном анализе, например, наивный байесовский алгоритм, который использует теорию Байеса. Или, например, EM-алгоритм, который может быть использован в качестве одного из способов кластеризации. Он позволяет аппроксимировать исходное распределение смесью плотностей других, более удобных для анализа распределений. Как правило, это нормальное распределение, но для инфокоммуникационных приложений более корректным будет использование смесей экспоненциальных распределений.

Так можно определить параметры распределения в виде выражений:

$$p^{(\nu+1)} = \frac{f_j^{(\nu)}(x_i)\, p_j^{(\nu)}}{\sum_{i=1}^{N} g^{(\nu)}(x_i)} / N$$

$$\lambda_j^{(\nu+1)} = \frac{\sum_{i+1}^{N} \frac{f_j^{(\nu)}(x_i)\, x_i}{g^{(\nu)}(x_i)}}{\sum_{i+1}^{N} \frac{f_j^{(\nu)}(x_i)}{g^{(\nu)}(x_i)}}$$

где (ν) - шаг алгоритма, $f_j^{(\nu)}(x_i) = \lambda_j e^{-\lambda_j x_i}$ - будет использоваться компонента смеси, p_j - веса компонент, λ_j - параметры распределения.

Использование в качестве метода ЕМ-алгоритма позволит отфильтровать полученные для анализа данные, например, на этапе агрегации и фильтрации. Этот подход имеет некоторые преимущества: это простота реализации, он понятен и для него возможно определение пути вычисления результата.

Несмотря на некоторые ограничения, искусственный интеллект играет большую роль в информационной безопасности. Искусственный интеллект способствует развитию кибербезопасности, помогая преодолеть возникающие трудности, например, при анализе событий.

Список использованных источников:

1. Федорченко А.В., Левшун Д.С., Чечулин А.А., Котенко И.В. Анализ методов корреляции событий безопасности в SIEM-системах. Часть 1 // Труды СПИИРАН, 2016. Вып. 4(47), с. 5-27.

2. Федорченко А.В., Левшун Д.С., Чечулин А.А., Котенко И.В. Анализ методов корреляции событий безопасности в SIEM-системах. Часть 2 // Труды СПИИРАН, 2016, вып. 6(49), с. 208-225.

3. Duncan N., Shem Mbandu A. A Survey of Artificial Intelligence in Cyber Security // International Journal of Computer Applications Technology and Research, 2022, vol. 11, iss. 12, pp. 474-477

4. Levshun D.A., Kotenko I.V. A survey on artificial intelligence techniques for security event correlation: models, challenges, and opportunities // Artificial Intelligence Review. 2023, vol. 56, iss: 8, pp. 1-44.

5. Salah S, Macia-Fernandez G, D´ıaz-Verdejo J.E. () A model-based survey of alert correlation techniques // Computer Networks. 2013, vol. 57(5), pp. 1289–1317.

6. Mirheidari S.A., Arshad S., Jalili R. Alert correlation algorithms // A survey and taxonomy. In: International Symposium on Cyberspace Safety and Security, 2013, pp. 183–197.

7. Yu Beng L., Ramadass S., Manickam S. A survey of intrusion alert correlation and its design considerations // IETE Technical Review, 2014, vol. 31(3), pp. 233–240.

УДК 004.056.5

В.А. Летяев, М.А. Рожков, А.А. Бухнер
Поволжский государственный университет
телекоммуникаций и информатики, Самара, Россия

Научный руководитель:
Н.В. Киреева
Поволжский государственный университет
телекоммуникаций и информатики, Самара, Россия

ЭВОЛЮЦИОНИРУЮЩАЯ УГРОЗА ВРЕДОНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ: ОТ ВИРУСОВ ДО АВТОНОМНОГО КИБЕРОРУЖИЯ
EVOLUTIONARY THREAT OF MALICIOUS SOFTWARE: FROM VIRUSES TO AUTONOMOUS CYBER WEAPONS

Аннотация: В статье говорится об угрозе, которую представляют собой вредоносные программы и искусственный интеллект при кибератаках. Количество и сложность вредоносных программ растет, а использование искусственного интеллекта увеличивает риски кибербезопасности. Также рассматривается влияние автоматизированных атак и квантовых технологий. Сочетание этих технологий повышает уровень кибербезопасности, но киберпреступники могут использовать их для проведения разрушительных атак.

Abstract: The article discusses the threat posed by malicious software and artificial intelligence in cyber-attacks. The number and complexity of malicious programs are increasing, and the use of artificial intelligence is amplifying cybersecurity risks. It also considers the impact of automated attacks and quantum technologies. The combination of these technologies enhances cybersecurity, but cybercriminals may exploit them to carry out destructive attacks.

Ключевые слова: Вредоносное ПО, кибервойна, кибератаки, киберпреступность, искусственный интеллект, квантовая технология, безопасность данных.

Keywords: Malware, cyberwarfare, cyberattacks, cybercrime, artificial intelligence, quantum technology, data security.

Современный мир столкнулся с растущей угрозой вредоносного программного обеспечения (ПО), которое оказывает все более изощренное и разрушительное воздействие в киберпреступности. Быстрое распространение и усиленная самовоспроизводимость этого ПО представляют серьезные вызовы для кибербезопасности. В условиях

перехода многих процессов в онлайн-режим, появилось огромное количество вредоносных программ, среди которых ransomware (программы-вымогатели) особенно активно распространяется. Кибератаки выходят на новый уровень, открывая эпоху транснациональной кибервойны и кибершпионажа. В контексте быстро развивающихся компьютерных технологий и растущей киберугрозы, важно понимать, что роль искусственного интеллекта (ИИ) в кибербезопасности имеет двойную природу. Системы ИИ могут существенно усилить защиту, но и представляют новые угрозы, включая потенциальные атаки без человеческого участия. В таком контексте, перспективы использования квантовых технологий для борьбы с киберугрозами становятся все более актуальными и перспективными.

Вредоносное ПО, мощное оружие в кибервойне [1], становится все более изощренным, быстро распространяется и самовоспроизводится. Вредоносное ПО также является одной из самых опасных форм киберпреступности, поскольку оно может ускользать от обнаружения, препятствовать проведению криминалистического анализа в режиме реального времени и использовать сложные стратегии обхода с серьезными и долгосрочными последствиями.

В то время как современный мир переживает стремительный прогресс в области компьютерных технологий, международная киберпреступность также стремительно растет. Во время пандемии, когда многие процессы перешли в режим онлайн, резко возросло количество вредоносных программ, таких как программа-вымогатель.

Современные кибератаки открыли эру транснациональной кибервойны и агрессивного кибершпионажа, иногда даже между государствами и суверенными организациями. Одним из наиболее эффективных способов защиты от кибервойн является использование сложных вредоносных программ. Наиболее распространенным видом кибератак является использование вирусов.

Что такое вирус [2]? В области информационной безопасности вирус — это вредоносная программа, которая вторгается в код других программ, области системной памяти или загрузочные сектора и распространяет свои копии по различным каналам связи. Основная цель вирусов - распространение, но они также могут повреждать аппаратные и программные системы, удалять файлы, уничтожать операционные системы, приводить в негодность данные и сетевые структуры. Чаще всего вирусы распространяются через Интернет, USB-накопители и электронную почту, включая макровирусы, почтовые вирусы, полиморфные вирусы и троянские кони. Помимо вирусов, которые вредят электронным устройствам, существуют и другие вредоносные программы - ботнеты, компьютерные черви, кейлоггеры, шпионские программы и

программы-вымогатели. Вредоносное программное обеспечение развилось до такой степени, что теперь его можно использовать для влияния на работу ядерных центрифуг, кражи конфиденциальной информации связи со злоумышленниками по спутниковым каналам.

По мере расширения использования искусственного интеллекта в сфере кибербезопасности растет и обеспокоенность по поводу его потенциального вреда. Системы кибербезопасности сложны и взаимосвязаны, а системы, основанные на искусственном интеллекте, способны усилить воздействие уязвимостей в этих системах. Такие системы могут создать ложное ощущение безопасности и заставить организации игнорировать другие уязвимости в своих системах, а также создать новые уязвимости и предоставить новые возможности для атак.

Инструменты на основе ИИ могут быть использованы для создания автономного оружия [3], способного совершать атаки без вмешательства человека. Это может привести к новой эре кибервойны, когда страны и организации будут использовать инструменты ИИ для разрушительных атак на критически важные объекты инфраструктуры.

Алгоритмы искусственного интеллекта зависят от качества данных, на которых они обучаются, и любая предвзятость в данных приведет к искажению систем ИИ. Это может привести к дискриминации определенных групп. Автоматизированные атаки, возможность использования в агрессивных целях, риск предвзятости и дискриминации — вот лишь некоторые из опасностей, с которыми необходимо бороться. Учитывая массовое распространение множества подключенных объектов, легко представить масштабы вредоносных атак, направленных на эти устройства. Квантовая технология [4] может стать перспективным решением с точки зрения скорости выполнения и обработки больших объемов данных и дать толчок к решению многих задач. Таким образом, сочетание крупномасштабных квантовых технологий и искусственного интеллекта произведет революцию в кибербезопасности. В то же время киберпреступники получат стратегическое преимущество, используя мощные возможности квантовых вычислений для проведения разрушительных атак.

Вредоносное ПО является мощным оружием в кибервойне с возрастающей сложностью и распространением. Оно олицетворяет угрозу кибербезопасности, способную обойти защиту и нанести серьезный ущерб. С развитием ИИ и квантовых технологий киберпреступники могут активно использовать их для проведения новых разрушительных атак. Главная задача сегодня – разработка мощных киберзащитных механизмов, способных противостоять новым вызовам в области информационной безопасности.

Список использованных источников:

1. Масалков А. С. Особенности киберпреступлений в России: инструменты нападения и защиты информации [Текст] / Масалков А.С. – Москва: ДМК Пресс, 2018 – 226 с.
2. Алёшин С.Ю. Описание и классификация вредоносного программного обеспечения. Основные методы защиты, используемые антивирусными программами [Текст] / Алёшин С. Ю. // Молодой ученый. – 2022. – № №2 (397). – С. 5-10.
3. Tsagourias Nicholas, Buchan Russell Autonomous Cyber Weapons and Command Responsibility / Tsagourias Nicholas, Buchan Russell [Электронный ресурс] // SSRN: [сайт]. – URL: https://ssrn.com/abstract=3870733 (дата обращения: 19.04.2024)
4. ИВВ Квантовая криптография: защита информации в эпоху квантовых технологий. Нерушимый код: исследование квантовой криптографии [Текст] / ИВВ – Екатеринбург: Ridero, 2023 – 62 с.

УДК 0.04.056.5

Н.В. Масальский
Уфимский университет
науки и технологий, Уфа, Россия

Научный руководитель:
Н.Г. Миронова
Уфимский университет
науки и технологий, Уфа, Россия

ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА: АКТУАЛЬНЫЕ ПРОБЛЕМЫ
ENSURING THE PROTECTION OF PERSONAL DATA USING ARTIFICIAL INTELLIGENCE TECHNOLOGIES: CURRENT ISSUES

Аннотация: Данная работа обсуждает актуальные проблемы, связанные с обеспечением защиты персональных данных при использовании технологий искусственного интеллекта. Рассматриваются технические аспекты этой проблематики. Также обсуждаются этические и социальные вопросы, связанные с обработкой и хранением персональных данных с применением искусственного интеллекта.

Abstract: This paper discusses current issues related to ensuring the protection of personal data when using artificial intelligence technologies. The technical aspects of this issue are considered. Ethical and social issues related to the processing and storage of personal data using artificial intelligence are also discussed.

Ключевые слова: Защита персональных данных, Искусственный интеллект, Технологии защиты данных, Безопасность данных.

Keywords: Personal data protection, Artificial intelligence, Data protection technologies, Data security.

Современные технологии искусственного интеллекта (ИИ) предоставляют мощные инструменты для борьбы с этими угрозами, предлагая новые подходы к обеспечению безопасности данных. Использование машинного обучения для обнаружения аномалий в поведении систем, управление шифрованием и анонимизация данных – лишь некоторые из аспектов, в которых ИИ может сыграть решающую роль. Введение ИИ в системы защиты данных не только повышает их эффективность, но и вызывает ряд юридических и этических вопросов, требующих тщательного анализа и регулирования. Эта статья направлена на изучение возможностей ИИ в контексте защиты персональных данных, а также на обсуждение связанных с этим проблем и перспектив.

Методы искусственного интеллекта в защите данных. Искусственный интеллект предоставляет разнообразные инструменты для защиты персональных данных, каждый из которых имеет уникальные возможности и применения.

Обнаружение и предотвращение утечек данных: Использование машинного обучения для мониторинга и анализа сетевого трафика позволяет выявлять необычные паттерны, которые могут указывать на утечку информации. Алгоритмы классификации и кластеризации анализируют поведение пользователей и транзакции в реальном времени, помогая предотвратить потенциальные угрозы до того, как они причинят вред.

Шифрование данных с использованием ИИ: Искусственный интеллект может усилить процессы шифрования, управляя ключами шифрования динамичнее и эффективнее, адаптируясь к изменяющимся условиям безопасности. Нейронные сети способны прогнозировать потенциальные угрозы и автоматически изменять ключи шифрования.

Анонимизация данных: Применение генеративно-состязательных сетей для создания анонимизированных версий данных, которые могут быть использованы для исследований и аналитики, не раскрывая при этом идентификационную информацию. Эти ИИ-модели обучаются на реальных наборах данных для генерации новых, в которых исходные

идентифицирующие характеристики заменены на неидентифицируемые, но при этом сохраняется статистическая полезность информации.

Примеры применения ИИ в области защиты данных:

Финансовый сектор: Банки и страховые компании используют ИИ для мониторинга и анализа транзакций в реальном времени, что помогает обнаруживать и предотвращать мошенничество. Например, системы на основе машинного обучения анализируют поведение клиентов и историю транзакций, выявляя подозрительные операции, которые могут указывать на несанкционированный доступ или попытки кражи данных.

Здравоохранение: В этой сфере конфиденциальность и защита данных имеют особенно высокую важность. Использование ИИ позволяет обеспечить безопасность медицинских записей и личной информации пациентов. Инструменты ИИ анализируют доступ к базам данных, обнаруживая и блокируя неавторизованные попытки доступа, а также помогают анонимизировать личные данные для исследовательских целей, сохраняя при этом их полезность для медицинских исследований.

Онлайн магазины: В сфере розничной торговли ИИ используется для защиты данных клиентов и предотвращения утечек. Системы на основе ИИ отслеживают и анализируют пользовательское поведение на сайтах, выявляя аномальные действия, которые могут свидетельствовать о попытках взлома или других видах мошенничества.

Отрицательные стороны с которыми можно столкнуться при использовании ИИ в области защиты данных заключается в следующих аспектах:

Соблюдение законодательства: Во многих странах существуют строгие законы, регулирующие обработку персональных данных, такие как GDPR в Европейском Союзе и Федеральный закон №152 "О персональных данных" в России. Использование ИИ в защите данных должно строго соответствовать этим нормативам, чтобы избежать юридических санкций и укрепить доверие пользователей.

Ответственность: Определение ответственности за ошибки или ущерб, вызванные решениями ИИ, остается сложной задачей. Необходимо разработать четкие механизмы контроля за действиями ИИ, чтобы можно было отслеживать и корректировать неправильные решения системы.

В перспективе углубленное изучение возможностей и ограничений ИИ разработка международных стандартов и протоколов а также сотрудничество между различными заинтересованными сторонами могут способствовать более безопасному и справедливому использованию искусственного интеллекта в защите личных данных. Путь к достижению этого баланса требует совместных усилий ученых технологов правозащитников и политиков направленных на создание общества в котором технологии служат благу человечества.

Обеспечение защиты персональных данных в эпоху цифровизации и использования технологий искусственного интеллекта представляет собой не только техническую задачу, но и сложную проблему, требующую комплексного решения на уровне нормативного правового регулирования и практической реализации. В ходе анализа данной темы становится очевидным, что существующие правовые механизмы не всегда адекватно реагируют на новые вызовы, возникающие в связи с быстрым развитием технологий искусственного интеллекта.

Нормативно-правовые акты, направленные на защиту персональных данных, должны быть гибкими и адаптивными, способными оперативно реагировать на изменения в технологическом пространстве. Это предполагает не только разработку новых законов и положений, но и постоянное обновление существующих нормативных актов в соответствии с реальными вызовами и потребностями общества.

Актуальные проблемы в области защиты персональных данных с использованием искусственного интеллекта включают в себя не только технические аспекты, такие как разработка надежных алгоритмов шифрования и методов анонимизации данных, но и вопросы этики и социальной ответственности. Важно не только обеспечить безопасное хранение и передачу данных, но и учитывать их потенциальное воздействие на личность и общество в целом.

Список использованных источников:

1. Томас Эрл, Заигхам Махмуд 2021 г. “Cloud Computing: Concepts, Technology & Architecture”. [Электронный ресурс]. — URL: https://zlib.pub/book/cloud-computing-concepts-technology-architecture - 6q8jsi267e80 (дата обращения 21.04.2024).

2. Кевин П. Мерфи 2020 г. "Machine Learning: A Probabilistic Perspective". [Электронный ресурс]. URL: https://www.cs.ubc .ca/~murphyk/MLbook/pml-toc-22may12.pdf (дата обращения 21.04.2024).

3. Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 06.02.2023) О персональных данных. [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения 21.04.2024).

УДК 004

А.Р. Махмутов
Уфимский университет
науки и технологий, Уфа, Россия

Научный руководитель:
В.М. Картак
Уфимский университет
науки и технологий, Уфа, Россия

МОДЕЛИРОВАНИЕ СЕТИ ПРОМЫШЛЕННОГО ИНТЕРНЕТА ВЕЩЕЙ С ПОМОЩЬЮ ТЕХНОЛОГИЙ ВИРТУАЛИЗАЦИИ
INDUSTRIAL INTERNET OF THINGS NETWORK MODELING USING VIRTUALIZATION TECHNOLOGIES

Аннотация: В работе рассматривается вопрос применения технологий виртуализации в процессе моделирования фрагмента сети промышленного Интернета вещей. Проведен обзор популярных проектов, позволяющих виртуализировать устройства Интернета вещей. Обозначены ключевые ограничения, присущие моделированию сети Интернета вещей исключительно виртуальным способом.

Annotation: The paper is devoted to the issue of using virtualization technologies in the process of modeling a fragment of an Industrial Internet of Things network. We did a review of popular virtualization projects of IoT devices. Also we highlighted key limitations thar are specific to modeling the IoT network exclusively in a virtual way.

Ключевые слова: Виртуализация, Интернет вещей, Моделирование, Конечные устройства, Передача данных.

Keywords: Virtualization, Internet of Things, Modelling, End nodes, Data transmission.

Введение. Интернет вещей (IoT) стремительно набирает популярность, что оказывает влияние как на потребительский сектор (Consumer IoT), так и на промышленный (Industrial IoT). Соответственно, с ростом объема Интернета вещей увеличивается и число подключенных к Интернету промышленных объектов и SCADA систем. Вместе с ростом доступных из глобальной сети объектов промышленности растет и количество компьютерных атак, которые нацелены как компрометацию данных, обрабатываемых в таких сетях, так и на отказоустойчивость рассматриваемых объектов. В рамках работы [1] обозначен этот тренд и затронута тематика моделирования на стенде фрагмента сети промышленного Интернета вещей с целью проверки эффективности

существующих мер защиты информации, оценки модели с точки зрения противостояния характерным атакам, а также выработки рекомендаций по результатам проведения атак. В работе обозначены 3 способа построения стенда моделирования:

– Аппаратный – моделирование осуществляется исключительно на физическом оборудовании без использования технологий виртуализации;

– Программно-аппаратный – при моделировании используются технологии виртуализации совместно с физическим оборудованием;

– Программный – моделирование осуществляется исключительно при помощи технологий виртуализации.

В данной работе проводится краткий обзор способов виртуализации устройств Интернета вещей а также рассматривается вопрос применимости технологий виртуализации в рамках работ по моделированию сети промышленного Интернета вещей.

Обзор решений. Существует множество решений по виртуализации, которые способны эмулировать работу конечных устройств Интернета вещей. При этом, в зависимости от конкретной технологии, эмуляция может выполняться как в отношении одного устройства, так и их множества, с возможностью объединения в виртуальную сеть для совместного взаимодействия виртуальных устройств в режиме реального времени. Также, в зависимости от используемой технологии, у пользователя появляется возможность устанавливать взаимодействие виртуальных устройств с устройствами из реального мира.

Проект Simuli [2], ранее называвшийся IoTIFY Virtual Lab, позволяет пользователю работать с виртуальной копией Arduino Uno, STM32 Nucleo F411RE, Raspberry Pi непосредственно в браузере с возможностью хранения проекта в облаке, а также с использованием локального гипервизора, к примеру VMware или VirtualBox, оффлайн. Проект поддерживает минимально необходимый набор датчиков для эмуляции конечного устройства Интернета вещей. К примеру, при помощи этого решения может быть собрана виртуальная сеть из множества устройств Arduino Uno, с подключением виртуальных датчиков для генерации информации и виртуальным Ethernet-модулем с последующей передачей данных через брокера сообщений MQTT на реальный сервер.

Инструмент виртуализации Raspberry Pi Azure IoT Online Simulator [3] позволяет сосредоточиться на работе с одноплатным микрокомпьютером Raspberry Pi с возможностью эмуляции макетной платы, а также минимально необходимым набором датчиков. Однако, функционал такого инструмента крайне ограничен и не позволяет строить собственные сети.

Другим решением, позволяющим работать с виртуальной копией устройств Интернета вещей является онлайн-инструмент Tinkercad [4], сервис также содержит минимально необходимый набор датчиков и иных

периферийных устройств для генерации потока информации и отладки программного кода конечного устройства без использования реальных устройств. Однако, решение не позволяет одновременно эмулировать множество устройств с возможностью объединения в одну виртуальную сеть и не позволяет подключение сторонних библиотек для Arduino. В проекте TinkercadNetConnector [5] проблема невозможности объединения устройств в одну виртуальную сеть была решена, однако, иные ограничения не позволяют проводить с высокой точностью построение модели сети промышленного Интернета вещей.

Заключение. В результате рассмотрения существующих решений по виртуализации устройств Интернета вещей получен следующий вывод – обозначенные технологии могут быть использованы при работе в рамках тематики моделирования сетей Интернета вещей. Виртуализация может быть использована как при работе по направлению машинного обучения, так и по информационной безопасности [6]. В контексте наших исследований по максимально точному моделированию фрагмента сети промышленного Интернета вещей с целью проведения атак и определения недостатков имеющихся средств защиты информации технологии виртуализации не могут быть использованы как основополагающий способ построения модели объекта защиты. Обозначенные инструменты виртуализации могут быть использованы с целью получения наборов данных для обучения средств ЗИ или отладки различных программных решений. Рассмотренные технологии не позволяют работать с каналом передачи данных и средой распространения сигнала в случае использования в эмулируемой сети специфических технологий передачи данных (RS-232 или радиоканал). Наиболее известные проекты по виртуализации конечных устройств направлены в первую очередь на эмуляцию одного устройства с возможностью подключения базового виртуального периферийного оборудования, но не множества таких устройств с целью их объединения в рамках единой среды взаимодействия. Отдельным ограничением является невозможность эмулирования каких-либо отказов или нарушений штатного функционирования виртуализируемых устройств, к примеру, падение напряжения в цепи питания конечного устройства, или вмешательство в радиоэфир злоумышленника.

Список использованных источников:

1. Картак В.М., Махмутов А.Р. Моделирование сетей промышленного Интернета вещей при модернизации системы защиты информации // Вопросы защиты информации. – 2024. – №1. – С. 32-37.

2. What is Simuli? // simuli.co URL: https://docs.simuli.co/ (дата обращения: 01.04.24).

3. Connect Raspberry Pi to Azure IoT Hub // microsoft.com URL: https://learn.microsoft.com/en-us/azure/iot-hub/raspberry-pi-get-started (дата обращения: 02.04.24).
4. Autodesk Tinkercad // tinkercad.com URL: https://www.tinkercad.com/ (дата обращения: 02.04.24).
5. Ellul, Joshua & Debono, Carl. (2022). TinkercadNetConnector: Connecting emulated IoT devices to the outside world. SoftwareX. 20. 10.1016/j.softx.2022.101218.
6. Lemay A., Fernandez J.M. Providing SCADA network data sets for intrusion detection research. 9th Workshop on Cyber Security Experimentation and Test (CSET 16). Austin, TX: USENIX Association, Aug. 2016.

УДК 004.5

Д.Т. Набиев
Уфимский университет
науки и технологий, Уфа, Россия

Научный руководитель:
Н.Г. Миронова
Уфимский университет
науки и технологий, Уфа, Россия

СЕТЕВАЯ БЕЗОПАСНОСТЬ: ЭВОЛЮЦИЯ КИБЕРАТАК
NETWORK SECURITY: THE EVOLUTION OF CYBER ATTACKS

Аннотация: В статье выполнен анализ новых, актуальных видов кибератак и методы противодействия им.

Abstract: The article analyzes new, current types of cyber attacks and methods to counter them.

Ключевые слова: информационная безопасность.

Key words: information security.

Кибератаки, т.е. взлом компьютерных систем, сетей, сетевых устройств с целью получения НСД к ним для раскрытия, хищения, порчи конфиденциальных данных, постоянно множатся и усложняются. На сайте https://cybermap.kaspersky.com, показывающем киберугрозы в реальном времени, Россия, как объект кибератак, оказалась на 1 месте среди всех

стран мира. В 2023 г. число ИБ-инцидентов в России увеличилось на 60%, причем, по оценке Лаборатории Касперского, в 26% случаев хакеры атаковали производственные предприятия, 16% атак пришлось на сферу услуг, чуть меньше - на ИТ-сектор и телеком, 10-15% атак – на государственную информационную инфраструктуру, ЦОДы [1], [2]. Группы хакеров при этом обычно мотивированы одной из целей:

- получение финансовой выгоды (для атаки применяется фишинг, вирусы-шифровальщики и смокеры); атаки, направленные на хищение конфиденциальной информации в 2023 году в среднем развивались 204 дня незаметно для служб безопасности, и требовали в среднем 73 дня для своего устранения.

- Вторая разновидность групп хакеров – иностранные спецслужбы, преследующие политические и экономические цели; они используют DDoS-атаки, фишинг, социальную инженерию и т.п., - причем участились атаки социальной инженерии с применением ИИ (дипфейки) для подмены доверенных лиц.

Все чаще фиксируются кибернападения с нарушением доступности мобильной связи и банковских услуг, нарушения в работе предприятий. Каждая IT-инновация создает новые возможности для злоумышленников. Так, бурное распространение мобильных устройств и облачных технологий создало хакерам новые каналы атак; IoT и мобильные устройства все чаще становятся особым объектом для хакеров, потому что могут дать доступ к конфиденциальной информации и служат входными точками в корпоративные сети, могут быть использованы для создания бот-сетей для развития широкомасштабных атак и заметания следов хакеров. Прогнозируется увеличение частоты т.н. атак на цепочки поставок (supply chain attack), используя инфраструктуру жертвы для развития атаки на ее контрагентов и клиентов через цифровое оборудование, ПО, облачную инфраструктуру, электронные документы, почту, зараженные OpenSource-решения и т.п. Растет активность атак новых видов, в т.ч. с использованием технологий искусственного интеллекта; усложняются сценарии и технологии атак. Хакеры быстро включили в арсенал своих инструментов сервисы машинного обучения для прощупывания и эксплуатации уязвимостей своих жертв (например, атака с использованием автоматического эксплойта, который сам сканирует сети в поисках незащищенных устройств, быстро проводит атаку на уязвимые узлы, − так что традиционные системы защиты не успевают своевременно отреагировать на атаку). Еще один тип сложных для обнаружения атак связан с эксплуатацией «скрытых каналов» утечки (хакеры инициируют неочевидные процессы передачи информации между системами и их компонентами, обходя защитные механизмы, получая НСД к критичным процессам и конфиденциальным данным, нанося ущерб, но не вызывая

подозрений); обнаружение таких атак требует специализированных систем обнаружения скрытых каналов.

Специалисты по безопасности совершенствуют технологии распознания атак и защиты от них. Для противодействия кибератакам используются антивирусные системы со встроенной изолированной средой, SIEM-решения, межсетевые экраны (WAF), средства глубокого анализа сетевого трафика (для отслеживания сложных целевых атак); снизить ущерб от кибератак позволяет резервное копирование критичных данных, возможно, киберстрахование и т.д. Одним из перспективных направлений развития технологий киберзащиты становятся технологии машинного обучения для анализа и обнаружения аномального поведения в сети [3]. Они позволяют быстро анализировать большие массивы данных, помогать в фильтрации сетевого трафика, обнаруживать неизвестные формы и признаки вредоносной активности, длительно развивающихся атак. Для эффективной борьбы с атаками требуется непрерывное обновление и адаптация систем безопасности сетей с учетом новых угроз и технологий.

Список использованных источников:

1. Аверьянова В. Виртуальный шторм: как изменились кибератаки на российскую инфраструктуру // Известия. – URL: https: // www.comnews.ru/content/232930/2024-04-26/2024-w17/1009/ virtualnyy-shtorm-kak-izmenilis-kiberataki-rossiyskuyu-infrastrukturu (дата обращения: 26.04.2024).

2. Назаров Е. На предвыборной платформе: какие кибератаки могут ударить по госсектору и бизнесу // comnews.ru; Forbes. – URL: https: // www.comnews.ru/content/232055/2024-03-14/2024-w11/1009/ predvybornoy-platforme-kakie-kiberataki-mogut-udarit-gossektoru-i-biznesuк (дата обращения: 26.04.2024).

3. Аменецкий, А.В. Кибербезопасность. Новые угрозы эпохи искусственного интеллекта и больших данных / А.В. Аменецкий, И.В. Рухович, Л.А. Аменецкая, Д.А. Аменецкий // Наука, инновации, образование: Актуальные вопросы и современные аспекты. – Пенза: Издательство: Наука и Просвещение (ИП Гуляев Г.Ю.), 2024. – С. 198-211.

УДК 004

А.С. Неттов
Уфимский университет
науки и технологий, Уфа, Россия

Научный руководитель:
Ф.Т. Байрушин
Уфимский университет
науки и технологий, Уфа, Россия

СОВРЕМЕННЫЕ ПРОБЛЕМЫ В ОБЛАСТИ КИБЕРБЕЗОПАСНОСТИ
MODERN PROBLEMS IN THE FIELD OF CYBERSECURITY

Аннотация: В статье рассматриваются современные проблемы в области кибербезопасности. Особое внимание уделено роли искусственного интеллекта в кибератаках и перспективам развития систем кибербезопасности с учётом внедрения новых технологий. Также статья рассматривает искусственный интеллект (ИИ), который находит всё большее применение в сфере кибербезопасности.

Annotation: The article discusses current problems in the field of cybersecurity, which include. Special attention is paid to the role of artificial intelligence in cyber attacks and the prospects for the development of cybersecurity systems, taking into account the introduction of new technologies. The article also examines artificial intelligence (AI), which is increasingly being used in the field of cybersecurity.

Ключевые слова: Кибербезопасность, искусственный интеллект, защита, угроза, атака, хакеры.

Keywords: Cybersecurity, artificial intelligence, protection, threat, attack, hackers.

Кибербезопасность — это комплекс мер, направленных на защиту от киберугроз. Под киберугрозами понимаются различные виды атак, целью которых является кража данных, нарушение работы систем или получение несанкционированного доступа к информации.

В современном мире, где информационные технологии играют ключевую роль во всех сферах жизни, кибербезопасность становится одним из важнейших аспектов национальной безопасности[1].

Кибербезопасность включает в себя защиту компьютерных систем, сетей, приложений и данных от различных видов киберугроз, таких как вирусы, программы-вымогатели, фишинг, DDoS-атаки и другие.

Для обеспечения кибербезопасности используются различные методы и технологии, такие как шифрование данных, антивирусное ПО, системы обнаружения и предотвращения вторжений, а также обучение пользователей основам кибербезопасности [2].

В современном мире информационные технологии играют ключевую роль во всех сферах жизни. Однако вместе с преимуществами, которые они предоставляют, информационные технологии также создают новые вызовы и угрозы в области кибербезопасности.

Вот некоторые из основных проблем кибербезопасности:

1. Рост киберугроз. С каждым годом количество кибератак и их сложность возрастают. Это связано с развитием технологий и увеличением числа пользователей интернета.
2. Уязвимость систем. Современные системы и сети становятся всё более сложными и взаимосвязанными. Это делает их более уязвимыми для кибератак.
3. Недостаточная защита данных. Многие организации и компании не уделяют должного внимания защите данных своих клиентов и сотрудников. Это приводит к утечкам данных и другим инцидентам.
4. Отсутствие единых стандартов. В области кибербезопасности нет единых стандартов и правил, которые бы применялись во всём мире. Это затрудняет международное сотрудничество в борьбе с киберугрозами.
5. Человеческий фактор. Одной из основных причин кибератак является человеческий фактор. Пользователи часто не соблюдают правила безопасности, что приводит к уязвимости систем.
6. Фишинг и социальная инженерия. Мошенники используют методы социальной инженерии и фишинга для получения доступа к личным данным пользователей.
7. Кибертерроризм. Кибертеррористы используют кибератаки для нанесения ущерба или запугивания населения.
8. Зависимость от технологий. Развитие технологий приводит к появлению новых уязвимостей и угроз.
9. Нехватка специалистов. В области кибербезопасности не хватает квалифицированных специалистов. Это затрудняет борьбу с киберугрозами.
10. Правовые аспекты. Правовые аспекты кибербезопасности ещё не до конца разработаны. Это затрудняет привлечение к ответственности за кибератаки [3].

Для решения этих проблем необходимо принимать комплексные меры, включающие в себя повышение осведомлённости пользователей, разработку новых технологий и стандартов, а также международное сотрудничество.

Искусственный интеллект может быть использован как для защиты от киберугроз, так и для их создания. В руках злоумышленников ИИ может стать мощным инструментом для проведения кибератак.

Вот некоторые способы использования ИИ для кибератак:

– автоматизация атак- ИИ может использоваться для автоматизации процессов обнаружения уязвимостей, разработки эксплойтов и проведения атак;

– генерация вредоносного ПО − ИИ может быть использован для создания новых видов вредоносного ПО, которые будут трудно обнаружить антивирусным программам;

– фишинг и социальная инженерия − ИИ может помочь злоумышленникам в создании более убедительных и персонализированных фишинговых писем;

– анализ данных − ИИ может использоваться для анализа данных о пользователях и организациях с целью выявления уязвимостей и слабых мест в системах безопасности;

– обход систем обнаружении − ИИ может помочь злоумышленникам в разработке методов обхода систем обнаружения вторжений и других средств защиты;

– создание ботов − ИИ может быть использован для создания ботов, которые будут выполнять различные задачи, такие как распространение вредоносного ПО или проведение DDoS-атак;

– анализ трафика - ИИ может анализировать сетевой трафик с целью выявления аномалий, которые могут указывать на кибератаку;

– распознавание образов − ИИ может быть использован для распознавания образов, которые могут быть использованы для идентификации пользователей и их устройств;

Таким образом, использование искусственного интеллекта может помочь в решении некоторых проблем кибербезопасности, но также может быть использовано злоумышленниками для проведения кибератак. Для защиты от кибератак, основанных на использовании ИИ, необходимо применять комплексные меры.

Список использованных источников:

1. Белоус, А. И. Основы кибербезопасности. Стандарты, концепции, методы и средства обеспечения: учебник/ А.И. Белоус. – М.: Техносфера, 2021. – 483 с.

2. Иерархическая динамическая система управления информационной безопасностью информационной системы предприятия / С.С. Валеев, Н.В. Кондратьева, М.Б. Гузаиров, А.С. Исмагилова // Инженерный вестник Дона. – 2023. – № 11(107). – С. 154-164.

3. Щербак, А.В. Информационная безопасность: учебник / А.В. Щербак. – М.: Издательство Юрайт, 2023. – 259 с. – ISBN 978-5-534-15345-3.

4. Байрушин, Ф.Т. Информационная безопасность как фактор обеспечения социальной стабильности в российском обществе / Ф.Т. Байрушин, И.В. Салов, И.Р. Абрамов // Евразийский юридический журнал. № 8(183). 2023. С. 427-429

5. Байрушин, Ф.Т. Информационная безопасность в современном многополярном укладе общественного устройства/ Ф.Т. Байрушин, И.В. Салов, И.Р. Абрамов // Евразийский юридический журнал. № 8(183). 2023. С. 416-417.

УДК 004.056.53

А.К. Полышева
Уфимский университет
науки и технологий, Уфа, Россия

Научный руководитель:
М.Р. Шафиков
Уфимский университет
науки и технологий, Уфа, Россия

АНАЛИЗ СОВРЕМЕННЫХ ТЕХНИЧЕСКИХ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ
ANALYSIS OF MODERN TECHNICAL CHANNELS OF INFORMATION LEAKAGE

Аннотация: В данной статье представлен анализ современных технических каналов утечки информации, создающих серьезную угрозу для безопасности данных. В статье рассматриваются различные сценарии и методы, используемые злоумышленниками для сбора и передачи конфиденциальной информации в обход существующих механизмов защиты.

Abstract: This article analyses modern technical information leakage channels that pose a serious threat to data security. The article discusses various scenarios and methods used by attackers to collect and transmit sensitive information to bypass existing security mechanisms.

Ключевые слова: Информация, данные, охраняемые сведения, безопаность, конфиденциальность, утечка информации, технические каналы утечки информации, аутентификация, защита информации.

Keywords: Information, data, secured information, security, confidentiality, information leakage, technical channels of information leakage, authentication, information protection.

В условиях стремительного развития информационных технологий и активного использования компьютеров и мобильных устройств защита конфиденциальных данных становится все более важной задачей в современном мире. Одним из способов нарушения безопасности таких данных является их утечка по техническим каналам. [1]

В современном информационном пространстве злоумышленники используют различные средства и методы для получения неправомерного доступа к конфиденциальным данным.

Среди наиболее распространенных сценариев реализации данной угрозы – это утечка через сети передачи данных, каналы физического доступа, мобильные приложения, электронную почту и облачные сервисы.

Утечка информации через сети передачи данных является одной из наиболее серьезных угроз для безопасности информации, которая ведет к необоснованному доступу к корпоративным или персональным сетям. Это происходит из-за недостаточно защищенных точек доступа Wi-Fi, слабых паролей, необновленного программного обеспечения, из-за ошибок в настройках сетевого оборудования, передачи информации через ненадежные сети или применения небезопасных протоколов передачи данных. [2]

Согласно аналитическому отчету экспертно-аналитического центра InfoWatch на долю утечек по каналам передачи данных приходится 95,4% на 2023 год. [3] Остальные случаи утечки конфиденциальных данных встречаются реже либо таких случаев и вовсе не было зарегистрировано.

Потеря или кража физических устройств, а также их неправильная утилизация способствуют несанкционированному доступу к содержащейся на них информации, особенно если они не защищены паролем или иными способами. Кроме того, наличие камер позволяет вести нелегальные аудио- и видеозаписи, фотографировать документы, записывать важные переговоры и передавать их в сеть в режиме реального времени для нанесения ущерба организации.

Многие мобильные приложения по своей природе очень уязвимы и для них характерна более обширная поверхность атаки, чем для их веб-аналогов, так как они скачиваются с публичных площадок и содержат огромное количество пользовательской информации [2]. Несоблюдение рекомендаций при разработке приложений со стороны разработчиков,

передача данных в незашифрованном виде [3], небезопасные аутентификация и авторизация – все эти уязвимости в мобильных приложениях ведут к утечке конфиденциальной информации.

Основную долю получения данных через электронную почту составляет рассылка фишинговых писем – до 92% атак проводятся именно таким способом. [4] Такие письма легко определить по общим признакам: грамматические и орфографические ошибки, срочность действий, просьба подтвердить ваш адрес или другие персональные данные, универсальные, неличные обращения по типу «Уважаемый клиент», наличие приложенных документов или ссылок с искаженным доменным именем, по которым необходимо перейти.

Преобладающая часть фишинговых сайтов находятся в доменной зоне .com (52%), на втором месте идет домен .ru (13%), далее – .xyz, .site и другие малоизвестные доменные зоны (8%).

Удобство облачных хранилищ бесспорно является их большим преимуществом, однако настройки безопасности пока не гарантируют полной защиты данных. Основная проблема утечки информации через облачные сервисы – игнорирование правил информационной безопасности при работе с облачными сервисами со стороны администраторов и предоставление ими же высокого уровня доступа группам пользователей для выполнения рабочих задач, которые в реальности используют лишь малую часть своих возможностей. Если учетные данные таких пользователей попадут в руки третьих лиц, злоумышленники получат неправомерный доступ к охраняемым данным.

Так как технические каналы утечки информации имеют свои особенности, ниже представлен их сравнительный анализ (таблица 1). [1]

Таблица 1 – Сравнительный анализ технических каналов утечки информации

Технический канал утечки информации/ Критерии сравнения	Каналы передачи данных через сети	Каналы физического доступа	Мобильные приложения	Электронная почта	Облачные сервисы
Сложность реализации	Требуются технические знания по сетевым протоколам и методам атак	Требуется физический доступ к устройствам и помещениям	Требуются знания в разработке приложений и социальной инженерии	Требуются знания в фишинге и разработке вредоносных писем	Требуются знания в облачных технологиях и методах атак на облака
Возможность обнаружения	Возможно обнаружение с помощью систем мониторинга сети и анализа сетевого трафика	Возможно обнаружение с помощью систем видеонаблюдения, контроля доступа и аудита физической безопасности	Возможно обнаружение с помощью антивирусного программного обеспечения и мониторинга активности приложений	Возможно обнаружение через применения спам-фильтров, анализ писем и обучения сотрудников	Обнаружение канала утечки информации через облачные сервисы может быть сложно из-за абстракции облачной инфраструктуры
Возможность внедрения защитных мер	Использование фаерволов (межсетевых экранов), системы обнаружения вторжений, VPN	Использование системы контроля доступа, видеонаблюдения, блокирования USB-портов	Регулярное обновление приложений, использование антивирусного программного обеспечения и защиты данных на уровне приложений	Использование шифрования писем, обучения сотрудников правилам информационной безопасности, фильтрация вложений	Использование шифрования данных, многофакторной аутентификации, мониторинг активности пользователей
Потенциальные последствия	Утечка больших объемов данных, нарушение конфиденциальности, доступ к критической информации	Физическое уничтожение или кража устройств, доступ к личным данным и документам	Доступ к личным данным пользователей, телефонным звонкам, сообщениям и т.д.	Доступ к конфиденциальным данным, утечка личной информации	Утрата контроля над обрабатываемыми данными, нарушение конфиденциальности
Скорость передачи данных	Высокая скорость передачи данных через сеть	Скорость ограничена физической пропускной способностью устройств	Высокая скорость передачи данных через мобильные сети	Высокая скорость передачи	Скорость зависит от качества и скорости интернет-соединения

Текущие данные и накапливаемая статистика нарушений безопасности информации является фундаментом для принятия решений по ее защите и оценке рисков реализации угроз.

Таким образом, анализ современных технических каналов утечки информации позволяет выявить основные уязвимости и улучшить системы защиты данных.

Список использованных источников:

1. Бузов, Г.А. Защита информации ограниченного доступа от утечки по техническим каналам: справочное пособие / Г.А. Бузов. – Москва: Горячая линия-Телеком, 2018. – 586 с. – ISBN 978-5-9912-0424-8. – Текст: электронный // Лань: электронно-библиотечная система. – URL: https://e.lanbook.com/book/111027 (дата обращения: 26.02.2024).

2. Исмагилов, Р.Ф. Конструирование модели обучающей нейронной сети для биометрической многофакторной аутентификации пользователя информационной системы / Р.Ф. Исмагилов, Н.Д. Лушников, А.С. Исмагилова // Вопросы защиты информации. – 2023. – № 1(140). – С. 19-23. – DOI 10.52190/2073-2600_2023_1_19.

3. Основы защиты информации от утечки по техническим каналам: учебное пособие / А.А. Евстифеев, В.И. Ерошев, А.П. Мартынов [и др.]. – Саров: РФЯЦ – ВНИИЭФ, 2019. – 267 с. – ISBN 978-5-9515-0426-5. – Текст: электронный // Лань: электронно-библиотечная система. – URL: https://e.lanbook.com/book/243473 (дата обращения: 23.02.2024).

4. Аналитический отчет. Россия: утечки информации ограниченного доступа, 2022-2023 годы / [Электронный ресурс] // Информационная безопасность в цифровой экономике: [сайт]. – URL: https://www.infowatch.ru/sites/default/files/analytics/files/utechki-informatsii-ogranichennogo-dostupa-v-rossii-za-2022-2023.pdf (дата обращения: 22.03.2024).

УДК 004

Б.Ф. Сабиров
Уфимский университет
науки и технологий, Уфа, Россия

Научный руководитель:
С.С. Валеев
Уфимский университет
науки и технологий, Уфа, Россия

СОВЕРШЕНСТВОВАНИЕ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ В СФЕРЕ НЕДВИЖИМОСТИ
IMPROVING THE INFORMATION SECURITY SYSTEM IN THE REAL ESTATE SECTOR

Аннотация: В статье рассматривается важная проблема совершенствования системы защиты информации в сфере недвижимости. Проводится анализ текущего состояния систем защиты информации, выявляются основные угрозы и риски, с которыми сталкиваются компании в данной отрасли, а также обсуждаются современные технологии и методы защиты. В качестве примера выбран подкласс информационных систем – CRM-системы.

Abstract: The article discusses the important problem of improving the information security system in the real estate sector. The current state of information security systems is analyzed, the main threats and risks faced by companies in this industry are identified, and modern technologies and methods of protection are discussed. As an example, we chose a subclass of information systems – CRM systems.

Ключевые слова: Недвижимость, технологии защиты информации, угрозы безопасности, риски, CRM-система.

Key words: Real estate, information security technologies, security threats, risks, CRM system.

В настоящее время система защиты информации в сфере недвижимости находится под угрозой из-за растущего числа кибератак и утечек данных [1]. Многие компании в сфере недвижимости сталкиваются с проблемой надёжной защиты конфиденциальных данных о клиентах, сделках и финансовых операциях [2].

Компании подвергаются разнообразным угрозам и рискам в области информационной безопасности. [3]. К числу ключевых угроз и рисков в этой области относятся [4]:

1. Кибератаки: Преступники могут атаковать информационные системы компаний, работающих в сфере недвижимости, чтобы завладеть конфиденциальными данными, финансовой информацией или нанести ущерб.

2. Утечки данных: Риск утечки конфиденциальных данных о сделках, клиентах или финансовых операциях может вызвать серьёзные проблемы, например потерю доверия клиентов, денежные потери и юридические трудности.

3. Фальсификация информации: Возможность изменения или фальсификации данных о недвижимости или сделках может привести к юридическим спорам и финансовым потерям.

4. Несанкционированный доступ: Если информация и данные были недостаточно защищены специалистами, то это может привести к несанкционированному доступу к защищаемой информации, что угрожает её конфиденциальности, а также её целостности.

5. Социальная инженерия: Методы социальной инженерии позволяют преступникам манипулировать сотрудниками компаний, чтобы получить доступ к информации или совершить мошенничество.

Для совершенствования системы защиты информации в сфере недвижимости необходимо использовать современные технологии и различные методы информационной безопасности. Алгоритмические методы криптографии, многофакторная аутентификация [5], различные системы мониторинга и обнаружения угроз. Все это обеспечивает повышение уровня безопасности данных [6].

Рассмотрим, например, CRM-системы, которые важны при автоматизации обработки информации в сфере недвижимости. Они обеспечивают повышению эффективности работы с клиентами, улучшать коммуникативные связи, увеличивают продажи и повышать эффективность обслуживания. Примером одной из популярнейших рассматриваемых систем является Bitrix24 [7]. Программа Bitrix24 занимает лидирующие места в рейтингах программ занимающихся планировкой задач и управлением проектов.

В программе Bitrix24 есть все необходимые инструменты для эффективной и качественной организации работы над проектом, для эффективного управления персоналом организации, средства разработки документов и решения других задач. Например, функция фокусировки внимания будет ежедневно информировать вас о статусе проекта, что облегчит выполнение краткосрочных задач. Методики Kanban, диаграмма Ганта и Scrum упрощают постановку задач. Также программа позволяет самостоятельно выбирать параметры для выполнения задач вашей организации.

Разработчики системы предусмотрели специальные рабочие поля для того, чтобы пользователь легко ориентировался в системе. Так в данной программе можно найти такие папки как: [Задачи], [Календарь], [Живую ленту], [Чат и звонки], [Группы], [Документы онлайн] и другие полезные разделы. Кроме того, эта система предлагает удобные инструменты для продаж через мессенджеры, включая различные тарифы, интеграцию с 1С, оценку клиентов для более тщательной обработки запросов и инструменты продаж через социальные сети.

Так CRM-система упрощает сбор и анализ данных о клиентах, их основные предпочтения, отмечает в журнале взаимодействия с агентами, а также отслеживать этапы сделок. Благодаря этому агенты могут легко находить информацию о клиентах, управлять активными сделками, устанавливать напоминания и совершать действия для максимизации продаж. Также они обеспечивают улучшение работы с клиентами.

Агенты могут быстро реагировать на запросы и обращения клиентов, предоставлять персонализированное обслуживание, а также следить за обратной связью. Все это помогает удерживать основных клиентов и поддерживать долгосрочные отношения.

Из этого можно сделать вывод, что CRM-системы в сфере недвижимости является важным средством управления отношениями с основными клиентами и повышения уровня сервиса и увеличения продаж. Эти системы позволяют быть компаниями конкурентоспособными, результативными и успешными на рынке недвижимости.

Как известно, CRM-системы относятся к классу открытых информационных систем, тем самым, необходимо обеспечивать противодействие кибератакам, утечке данных, возможной фальсификации информации, несанкционированному доступу к информации, технологиям социальной инженерии.

Рассматриваются основные подходы к совершенствованию защиты информации в данной предметной области.

Список использованных источников:

1. Угрозы социально-экономической безопасности в сфере жилищного строительства и направления ее обеспечения – URL: https://cyberleninka.ru/ article/n/ugrozy-sotsialno-ekonomicheskoy-bezopasnosti-v-sfere-zhilischnogo-stroitelstva-i-napravleniya-ee-obespecheniya/viewer (дата обращения: 29.04.2024).

2. Real estate cybersecurity: best practices to implement right now – URL: https://www.activerain.com/blogsview/5734818/real-estate-cybersecurity--best-practices-to-implement-right-now (дата обращения: 29.04.2024).

3. Understanding cyber risks in the real estate industry – URL: https://www.securitymagazine.com/articles/99023-understanding-cyber-risks-in-the-real-estate-industry (дата обращения: 29.04.2024).
4. ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации.
5. Исмагилова, А.С. Комплексная биометрическая аутентификация пользователей информационной системы с применением нейронных сетей / А.С. Исмагилова, Н.Д. Лушников // Инженерный вестник Дона. – 2024. – № 1(109). – С. 178-188.
6. ГОСТ Р ИСО/МЭК 27002-2021 Методы и средства обеспечения безопасности.
7. Bitrix24 – URL: https://www.bitrix24.ru/ (дата обращения: 29.04.2024).

УДК 004.056.53:34.096

А.В. Садыкова
Уфимский университет
науки и технологий, Уфа, Россия

Научный руководитель:
Э.Р. Гиззатова
Уфимский университет
науки и технологий, Уфа, Россия

ПРИМЕНЕНИЕ БИОМЕТРИЧЕСКИХ ДАННЫХ ДЛЯ ИДЕНТИФИКАЦИИ СОТРУДНИКОВ
THE USE OF BIOMETRIC DATA TO IDENTIFY EMPLOYEES

Аннотация: В условиях современной конкурентной борьбы защита интеллектуальной собственности занимает ключевую роль в обеспечении защиты режима коммерческой тайны. В связи с этим, в систему защиты информации специалисты внедряют все новые и новые способы идентификации пользователей. Метод идентификации с помощью биометрических данных не является новым, однако на сегодняшний день значительно изменилось законодательство в сфере их защиты, хранения и использования. В работе рассматривается вопрос подключения информационной системы организации к Единой биометрической системе.

Abstract: In the context of modern competition, the protection of intellectual property plays a key role in ensuring the protection of the trade secret regime. In this regard, specialists are introducing more and more new ways of identifying users into the information security system. The method of identification using biometric data is not new, but today the legislation in the field of their protection, storage and use has changed significantly. The paper considers the issue of connecting an organization's information system to a Single biometric system.

Ключевые слова: Безопасность, коммерческая тайна, биометрические персональные данные, единая биометрическая система.

Keywords: Security, trade secret, biometric personal data, unified biometric system.

В условиях современной конкурентной борьбы главенствующую роль также занимает информация. Каждый день изобретаются все новые способы производства, технологии и материалы, в связи с чем перед владельцами информации и производств встает вопрос защиты интеллектуальной собственности. Секреты производства компаний в соответствии с федеральным законодательством принято называть коммерческой тайной (КТ), ее стоит хранить, обрабатывать и использовать надлежащим образом.

Термин КТ относится к режиму конфиденциальности и подразумевает под собой состояние защищенности от посягательств конкурентов, утечек и краж. Доказано на практике, что утечка 20% информации, составляющей КТ, приводит к разорению 65% компаний-владельцев данной информации. Внедрение режима КТ и превентивные меры по защите информации, составляющей КТ, позволяет избавить компании от финансовых и репутационных потерь, защитить организацию от разорения, занять стабильное положение и иметь преимущество перед конкурентами в условиях рыночной экономики [1].

Рассматривая нормативно-правовую защиту КТ стоит обратиться к статистике. Компания InfoWatch представила исследование судебной практики по делам, связанным с незаконным получением и разглашением сведений, составляющих коммерческую за 2021-2023г. В соответствии с исследованием за 3 года было рассмотрено 219 дел по ст. 183 УК РФ, 75% из которых были совершены путем компрометации данных через сеть Интернет. Более того, около 63% рассмотренных дел инкриминировались частью 3 ст. 183 УК РФ т.е. были совершены умышленно, группой лиц, в особо крупном размере.

Однако приведенная статистика не является полной, данный факт связан с тем, что 70% дел не были рассмотрены из-за нарушений организаций в сфере защиты КТ. В 30% случаев на сведениях, содержащих

КТ отсутствовал соответствующий гриф, в 44% случаев режим КТ вообще не был введен, в остальных же случаях в трудовом договоре сотрудников отсутствовало соглашение о неразглашении сведений, составляющих КТ. Подводя итог вышесказанному стоит отметить, что нормативно-правовая защита КТ является такой же важной составляющей, как и техническая защита информации. Для юридически-правильного оформления режима КТ в организации необходимы следующие нормативно-правовые акты, указанные в ФЗ от 29.07.2004 № 98-ФЗ «О коммерческой тайне».

Помимо нормативно-правовой защиты сведений, составляющих КТ организации необходимо организовать и техническую защиту информации [2]. На сегодняшний день данная сфера защиты информации более развита, разработаны различные программные и программно-аппаратные комплексы, которые применят широкий спектр методов идентификации и аутентификации сотрудников, снижающие риски утечки и кражи конфиденциальной информации.

Практически все организации так или иначе применяют различные технические меры идентификации и аутентификации сотрудников в корпоративных информационных системах, к ним можно отнести парольную аутентификацию, аутентификацию с помощью физического носителя и биометрическую аутентификацию [3].

В современном корпоративном мире все большую популярность набирает биометрическая аутентификация [4]. Данный факт связан с удобством использования, отсутствием возможности забыть или потерять свой уникальный идентификатор. Однако биометрическая аутентификация обрела ряд условий.

С 2023 года организации, хранящие на своих серверах биометрические данные сотрудников, обязали передать их в Единую биометрическую систему (ЕБС), созданную при участии Минцифры, Ростелекома и Центробанка. Ее оператором назначен АО «Центр Биометрических Технологий» (ЦБТ). Основным нормативно-правовым актом, регламентирующим функционирование ЕБС выступает приказ Минцифры от 12.05.2023 № 453.

В ЕБС хранятся биометрические данные в строго определенном формате – изображение лица, полученное путем фото-, видеосъемки и запись голоса, полученная с помощью звукозаписывающего устройства. Однако передавать или получать биометрические данные в первоначальном виде не нужно. Организация получает и передает биометрические данные сотрудников в цифровом виде (математический вектор), который без специализированного программного обеспечения расшифровать или использовать невозможно [5].

Для того, чтобы подключиться к ЕБС стоит выбрать роль организации: поставщик данных – та организация, которая создает

биометрические данные для ЕБС с помощью корпоративной ИС; пользователь данных – организация, получающая из ЕБС готовые векторы. В первом случае организации необходимо будет подключиться к ЕБС на ее официальном сайте ebs.ru, через вкладку «Бизнесу» и выбрать «Поставщик данных», пройти аккредитацию информационной системы, подобрать соответствующее программное обеспечение для защиты и шифрования биометрических данных, во втором случае необходимо выбрать вкладку «Пользователь данных». На сайте ЕБС есть пошаговые инструкции по подключению и рекомендации по выбору оборудования, программного обеспечения с учетом требований приказа Минцифры от 12.05.2023 № 453.

Таким образом, разработанное нововведение существенно облегчило процесс создания, использования и хранения биометрических данных в корпоративных системах. Для биометрической идентификации сотрудников необходимо установить соответствующее программное обеспечение, запросить данные из ЕБС и интегрировать полученные векторы в действующую систему защиты информации. Функции защиты, обработки, сопоставления биометрии конкретному человеку берет на себя государственная информационная система, напрямую связанная с федеральной государственной информационной системой «Единый портал государственных и муниципальных услуг (функций)».

Список использованных источников:

1. Дышекова, Д.А. Правовая защита коммерческой тайны / Д.А. Дышекова // Теория права и межгосударственных отношений. – 2022. – Т. 1, № 6(26). – С. 54-57.

2. Садыкова, А.А. Коммерческая тайна как разновидность информации с ограниченным доступом: отдельные аспекты классификации / А.А. Садыкова, Х.С. Меджидова // Евразийский юридический журнал. – 2022. – № 10(173). – С. 276-277.

3. Колкарева, И.Н. Единая биометрическая система: мировой опыт и особенности применения в России / И.Н. Колкарева, Е.П. Змеева // Сфера услуг: инновации и качество. – 2022. – № 59. – С. 97-108.

4. Исмагилова, А.С. Комплексная биометрическая аутентификация пользователей информационной системы с применением нейронных сетей / А.С. Исмагилова, Н.Д. Лушников // Инженерный вестник Дона. – 2024. – № 1(109). – С. 178-188.

5. Гузаиров, М.Б. Аутентификация пользователей информационной системы по изображению лица / М.Б. Гузаиров, А.С. Исмагилова, Н.Д. Лушников // Моделирование, оптимизация и информационные технологии. – 2023. – Т. 11, № 4(43). – DOI 10.26102/2310-6018/2023.43.4.017.

УДК 004

А.А. Сальникова
Уфимский университет
науки и технологий, Уфа, Россия

Научный руководитель:
И.А. Шагапов
Уфимский университет
науки и технологий, Уфа, Россия

ИНТЕГРИРОВАННЫЙ ЦИКЛ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ ДОКУМЕНТАЦИЕЙ: ОТ ХРАНЕНИЯ ДО ПЕРЕРАБОТКИ
INTEGRATED INFORMATION DOCUMENTATION MANAGEMENT CYCLE: FROM STORAGE TO PROCESSING

Аннотация: Обеспечение конфиденциальности информации организаций, которой ещё не обрабатывается в электронном документообороте, с помощью сторонней компании, которая возьмёт на себя роль хранения, уничтожения и переработки документов.

Abstract: Ensuring the confidentiality of information of an organization that has not yet been processed in electronic document management, with the help of a third-party company that will take on the role of storing, destroying and processing documents.

Ключевые слова: Электронный документооборот, хранение информации, конфиденциальная информация, сторонняя компания, экология, переработка бумаги.

Keywords: Electronic document management, information storage, confidential information, third-party company, ecology, paper recycling.

Благодаря электронному документообороту можно уменьшить количество распечатанных документов, что приведет к уменьшению потребления бумаги и, в свою очередь, к сокращению рубок лесов. Кроме того, электронные документы легче подлежат защите информации, чем бумажные документы, что позволяет эффективно управлять доступом к данным и соблюдать нормы безопасности.

Однако, несмотря на преимущество электронного документооборота, ещё не все полностью перешли на него [1].

Для хранения конфиденциальной информации в организации, помимо затрат на помещение и найма дополнительных работников, потребуется использование журналов учёта, дополнительных соглашений о неразглашении и много внутренних нормативно правовых актов

регулирования работы с конфиденциальной информацией. Не лучше ли будет избежать таких затрат и рисков с помощью сторонней организации?

Мы предлагаем создать организацию, которая будет заниматься хранение документов, в том числе с конфиденциальной информацией. Помимо этого, она также будет заниматься удалением ненужной, устаревшей для компании информацией в документах, а именно стирание (удаление) информации с носителя и как следствие её переработка.

Итак, поподробнее. Компания возьмёт на себя ответственность за хранения документов. Для этого между двумя компаниями будет подписан договор, и документы, необходимые для хранения, будут изъяты в архив нашей компании. При потребности в документации компания-наниматель извещает о необходимости в них. С нашей стороны необходимые документы доставляются на транспорте и выдаются под роспись. После, также возвращаются в архив хранения. Естественно, с нашей стороны подписывается соглашение о неразглашении конфиденциальной информации, и применяются меры по защите информации путём применения организационных и инженерно-технических мер.

Как только документ выходит из оборота, информация сразу удаляется. Для этого будет существовать процесс переработки.

Сначала необходимо пояснить, что тонер, который наносится на бумагу, состоит из смолы и магнитной окиси железа. Смолу можно растворить разными растворителями, но останется пятно от окиси железа, убрать которое поможет только кислота, но она разъест бумагу [2].

Поэтому единственным способ удалением информации с бумажного носителя это разработка Кембриджского университета. Они научились испарять тонер с белой бумаги. Исследования проводились с использованием лазерного принтера фирмы HP - LaserJet и наносился тонер на белую бумагу производства Canon. Оказывается под действием лазера определённой волны (оптимальная длина волны составила 532 нм) с пульсацией (частота которой 4 нс) можно испарить тонер, не повредив при этом бумагу [3].

Учёные выяснили, что обрабатывать такую бумагу можно неоднократно, но чем чаще она проходит такую процедуру, тем дальше она от своего белого цвета. Всё просто – бумага начинает выцветать (желтеть).

К сожалению, такая бумага, судя по рисунку 1, всё же оставляет некий след от текста, а значит подходит только для черновиков.

Рисунок 1 – Обработанная бумага под микроскопом

Стоит учитывать, что для таких черновиков не подходит документы с конфиденциальными данными, а так же документы, на которых были использованы чернила (их вывести можно только химическим методом).

Поэтому мы предлагаем вторую стадию удаление информации – химическая обработка.

Так как неровный слой тонера убирается и остаётся поверхность листа без повреждений, то вполне можно повторно окрасить бумагу в белый цвет, дабы полностью избавиться от информации. Таким образом, мы получим белый лист, который в принципе будет соответствовать безопасности для конфиденциальной информации.

Не все листы с информацией сохраняют свой первоначальный вид. Где-то закреплены степлером, где-то помялись, порвались, существуют по половинке и на них есть подписи и печати. Таки документы тоже можно подвергнуть лазеру, если такие документы несут в себе сведения ограниченного доступа, но мы не видим в этом целесообразность, такая бумага не пригодиться повторно, а значит легче будет пустить её под нож.

Таким образом вторая категория документов с конфиденциальными данными или просто документация подлежит уничтожению через шредер. Далее её можно будет измельчить в мелкую массу, замешивать с водой, очистить несколько раз, подвергая химической обработке и отбеливанию, сформировать листы, высушить и нарезать.

К данному процессу будут допущены только определённый круг лиц, а мелко нарезанные документы и его переработка в одном помещении гарантирует полное уничтожение информации.

Существуют компании по внеофисному хранению документов, примером может послужить ОСГ [4]. Данная компания забирает документы на хранение (в том числе и конфиденциальные) и при необходимости сканирует их и отправляет в «е-Архиве» клиенту. Также она может уничтожить документы и отправить их на переработку в ближайший пункт сдачи макулатуры. Но насколько это безопасно?

Наша компания предлагает наиболее безопасный вариант в пределах своей территории. Мы лично привозим оригиналы документов под роспись ответственному лицу, что уменьшает риск перехвата информации через интернет. Так как собрать измельчённую информацию сложно, но возможно, мы предлагаем более защищённый вариант. Хранение и уничтожение конфиденциальной информации в пределах компании будет намного безопаснее, что уменьшит число каналов утечек информации, а также позволит сэкономить ресурсы.

Таким образом, мы помогаем компаниям повысить свою безопасность, и природе сохранить её леса.

Список использованных источников:

1. Минцифры России: официальный сайт. – URL: https://digital.gov.ru/ru/events/43644/ (дата обращения 22.04.2024).

2. Форум химиков на XuMuK.ru: официальный сайт. – URL: https://forum.xumuk.ru/topic/71388/ (дата обращения 23.04.2024).

3. Cnews: официальный сайт. – URL: https://www.cnews.ru/news/top/izobreten_lazernyj_antiprinter_dlya (дата обращения 23.04.2024).

4. ОСГ: официальный сайт. – URL: https://www.osgrm.ru/company/ (дата обращения 18.04.2024).

УДК 004

И.Р. Сахибгареев
Уфимский университет
науки и технологий, Уфа, Россия

Научный руководитель:
И.А. Шагапов
Уфимский университет
науки и технологий, Уфа, Россия

СИСТЕМА УПРАВЛЕНИЯ ЛОВУШКАМИ И ПРИМАНКАМИ
TRAP AND BAIT MANAGEMENT SYSTEM

Аннотация: Система предназначена для привлечения, выявления и фиксирования действий потенциальных нарушителей (злоумышленников), проникнувших в локальную сеть, путем размещения на объектах информатизации ложных целей компьютерных атак в виде

ловушек и приманок. Цель создания Системы – автоматизация деятельности по направлению информационной безопасности в части реализации ловушек для хакеров.

Abstract: The system is designed to attract, identify and record the actions of potential intruders (intruders) who have penetrated the local network by placing false targets of computer attacks in the form of traps and baits on informatization facilities. The purpose of creating the System is to automate information security activities in terms of implementing traps for hackers.

Ключевые слова: Выявление фиксирования действий потенциальных нарушителей, реализация ловушек для хакеров.

Keywords: Identification of fixing the actions of potential violators, implementation of traps for hackers.

Одним из ключевых аспектов обеспечения безопасности в локальных сетях является способность привлекать и выявлять действия потенциальных нарушителей. Традиционные методы защиты, такие как брандмауэры и антивирусные программы, могут быть недостаточно эффективными против хитрых и продвинутых атак [1].

В данной статье мы рассмотрим эффективные методы привлечения и выявления действий нарушителей в локальной сети через использование ложных целей компьютерных атак. Создание ловушек и приманок на объектах сети все более популярными стратегиями для обнаружения потенциальных угроз.

Внедряемое решение предоставляет злоумышленникам обманчивое представление о сети. Ложные цели размещаются на серверах-ловушках. На компьютерах пользователей и сервера распространяются приманки в виде учетных данных и ссылок на ложные цели. Попытки использовать ловушку или приманку фиксируются системой и сведения передаются на сервер управления, который в реальном времени запускает процесс сбора аналитики и отображает данные в консоли [2-3]. Сервер управления поддерживает интеграцию с SIEM-системами и отправку уведомлений по электронной почте. Общие принципы работы отражены на Рисунке 1.

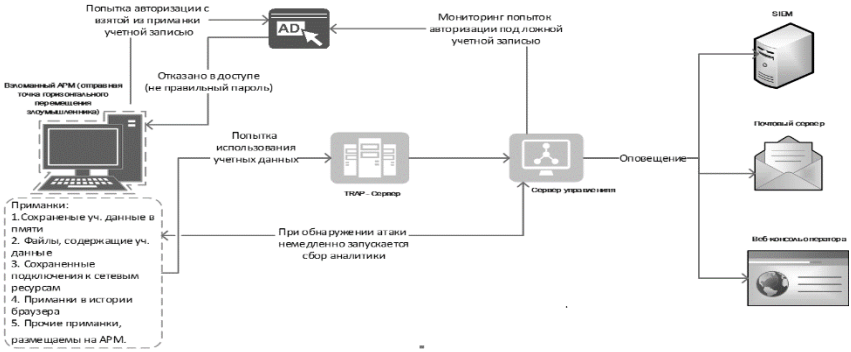

Рисунок 1 – Функциональная схема СУЛП

В состав системы управления ловушками и приманками входят следующие компоненты:

- единый централизованный модуль управления;
- модуль размещения приманок;
- модуль эмуляции устройств;

Единый централизованный модуль управления несет функционал распространения приманок, сбора статистики, анализа сетевого окружения и прав на объекты активного каталога, интеграции со смежными системами и управления по средствам веб-консоли.

Модуль размещения приманок определяет попытки сканирования сети и эмулирует на реальной операционной системе (Windows server) следующие сервисы:

- сервисы удаленного доступа к файлам (SMB);
- сетевые файловые ресурсы (FTP, SFTP);
- веб-сервисы (HTTP, HTTPS);
- сервисы удаленного управления (SSH);
- службы удаленных рабочих столов (RDP);
- различные СУБД (Postgresql, MySQL и т.д.).

Модуль эмуляции устройств представляет из себя гипервизор, где на платформе «docker» размещаются различные устройства:

- сервер;
- рабочая станция;
- сетевое оборудование;
- контроллерное оборудование и мобильные устройства.

После внедрения системы у администраторов безопасности появиться возможность выявлять и фиксирования действий потенциальных нарушителей (злоумышленников), проникнувших в локальную сеть, путем

размещения на объектах информатизации ложных целей компьютерных атак в виде ловушек и приманок.

Хочется отметить, что в современном цифровом мире, где угрозы кибербезопасности становятся все более сложными и разнообразными, важно иметь эффективные методы привлечения и выявления действий нарушителей в локальной сети. Создание ложных объектов, использование хонипотов, мониторинг сетевой активности, применение систем обнаружения вторжений и анализ журналов событий - все эти методы играют ключевую роль в обеспечении безопасности информации и защите сетевой инфраструктуры.

Путем использования современных технологий и методов кибербезопасности администраторы информационной безопасности могут активно привлекать нарушителей, выявлять и анализировать их действия на ранних стадиях, что позволяет предотвратить возможные атаки и укрепить защиту данных.

Список использованных источников:

1. Шагапов, И.А. Защита коммерческой тайны на предприятии: учебное пособие / И.А. Шагапов. – Уфа: Башкирский государственный университет, 2018. – 128 с. – ISBN 978-5-7477-4831-6.

2. Шагапов, И.А. Производство качественной безопасной информации – основа цифрового общества / И.А. Шагапов // Информационные технологии обеспечения комплексной безопасности в цифровом обществе: сборник материалов Всероссийской молодежной научно-практической конференции с международным участием, Уфа, 07–08 июня 2018 года / Фролова И.В., отв. редактор. – Уфа: Башкирский государственный университет, 2018. – С. 60-63.

3. Исмагилова, А.С. Рекомпозиционный подход в создании систем защиты информации автоматизированной системы / А.С. Исмагилова, И.А. Шагапов, И.В. Салов // Информационные технологии обеспечения комплексной безопасности в цифровом обществе: сборник материалов IV Всероссийской молодежной научно-практической конференции с международным участием, Уфа, 21–22 мая 2021 года. – Уфа: Башкирский государственный университет, 2021. – С. 18-24. – DOI 10.33184/itokbco-2021-05-21.3.

УДК 004

М.Е. Сержанин
Уфимский университет
науки и технологий, Уфа, Россия

Научный руководитель:
Ф.Т. Байрушин
Уфимский университет
науки и технологий, Уфа, Россия

АНАЛИЗ ПОТЕНЦИАЛЬНО-ОПАСНОГО КОНТЕНТА В «TELEGRAM»
ANALYSIS OF POTENTIALLY DANGEROUS CONTENT IN «TELEGRAM»

Аннотация: В статье раскрыты особенности безопасности информации, связанные с использованием мессенджера «Telegram» и потенциальных угроз, которые в нем присутствуют. Особое внимание уделяется мерам безопасности при использовании мессенджера и анализу по защите от потенциально-опасного контента.

Abstract: The article reveals the features of information security related to the use of the Telegram messenger and the potential threats that are present in it. Special attention is paid to security measures when using the messenger and analysis to protect against potentially dangerous content.

Ключевые слова: Информация, информационная безопасности, мессенджер, «Telegram», чаты, чат-боты, утечка информации, контент.

Keywords: Information, information security, messenger, Telegram, chats, chatbots, information leakage, content.

Популярность мессенджеров растет с каждым годом и они становятся не просто сервисом для общения, но площадками на которых публикуется огромное количество информации, в том числе и потенциально-опасный контент. Telegram – это платформа для обмена сообщениями на базе протокола безопасности MTProto. В 2024 году Telegram вошел в 5 самых популярных сервисов общения. Так, каждый месяц в Telegram заходят почти 800 миллионов человек. Доля россиян, пользующихся сервисом, растёт. За последний год их количество увеличилось на 20% по сравнению с предыдущим. По статистике популярность сервиса в России наблюдается среди граждан от 12 до 35 лет.

С ростом популярности социальных сетей в них все больше возникает ресурсов, которые публикуют потенциально-опасный контент. Потенциально-опасной информацией можно назвать любые данные, которые могут нести негативный характер и последствия. Публикация такой информации несет вплоть до уголовной ответственности в зависимости от ущерба, поэтому очень важно уделять внимание мерам ИБ и цифровой гигиене.

Telegram стал одной из площадок, на которой публикуется потенциально-опасный контент, по ряду причин, которые касаются как технической составляющей сервиса, так и социальной составляющей (возраст аудитории). С технической стороны стать пользователем мессенджера может любой человек, который имеет SIM-карту. Следует отметить, что в России до сих пор существует рынок нелегальных SIM-карт, которые были приобретены без предъявления паспорта и установления личности покупателя. Это является огромной проблемой, т. к. личность пользователя не будет идентифицирована и профиль может быть использован в мошеннических целях.

Политика конфиденциальности Telegram предоставляет пользователям практически полную анонимность действий. Сетевой трафик приложения практически невозможно, как было отмечено ранее, применяется собственный протокол шифрования MTProto. Протокол позволяет применять одновременно 256 - битное симметричное шифрование AES, алгоритм RSA-2048, а также обмен ключами методом Диффи-Хеллмана, что практически исключает расшифровку передаваемых сообщений между пользователя Telegram.

Потенциально-опасный контент в Telegram можно классифицировать:

1. Вредоносное ПО. Вирусы, содержащиеся в файлах или ссылках в Telegram, могут быть загружены на устройство пользователя и получить доступ к данным, в том числе к конфиденциальной информации, хранящейся на устройстве. Что может нанести, как моральный, так и финансовый ущерб.

2. Спам. Представляет собой массовую рассылку сообщений в различных целях (рекламных и мошеннических). Многие Telegram-каналы осуществляют отправку спама пользователям, который может содержать не только рекламную рассылку, но и вредоносное программное обеспечение.

3. Контент, запрещенный законодательством РФ. Отправка информации, которая запрещена на территории России.В соответствии со статьей 5 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» запрещается распространение информации, которая направлена на разжигание

национальной, расовой или религиозной ненависти и вражды, а также иной информации, за распространение которой предусмотрена ответственность.

С социальной точи зрения, потенциально-опасным контентом для пользователя является реклама употребления наркотических и психотропных средств и их распространение, реклама незаконных казино, пропаганда экстремизма и незаконный поиск, использование и передача персональных данных. Одним из ярких примеров Telegram-ботов, которые незаконно предоставляют ПДн, является запрещенный сервис «Глаз Бога».

Передача потенциально-опасного контента стала очень распространённой в Telegram, как отмечалось ранее, из-за шифрования трафика и безопасного обмена информацией. Поэтому очень важны методы, которые способны обнаружить потенциально-опасную информацию. Основной способ обнаружения опасной информации – это аналоговый, т.е. поиск потенциально-опасных данных по ключевым словам. Стоит отметить, что когда Telegram-канал закрытый осуществить поиск достаточно проблематично. Также при обнаружении такого вида данных пользователю обязательно отправить жалобу, чтобы ее обработали, и данные были заблокированы.

Чтобы обезопасить себя в Telegram нужно:

– не открывать и не скачивать файлы и ссылки от незнакомых людей;

– не вступать в незнакомые Telegram-каналы;

– не использовать запрещенные Telegram-боты;

– применять антивирусное ПО на устройстве;

– использовать двухфакторную аутентификацию при входе в профиль;

– проверять активные сеансы (раздел «Устройства»).

Одним из способов поиска потенциально-опасного контента является разработка чат-бота, который на основании анализа сможет определять опасные данные на основании поиска по ключевым словам. Т.е. вся входящая информация будет распознаваться до того, как пользователь ее открыл.

В заключение стоит отметить, что мессенджеры плотно вошли в жизнь человека. В первую очередь Telegram – это средство общения, но не стоит забывать, что в нем существует потенциально-опасный контент. Правила администрирования должны ужесточаться, чтобы минимизировать риски безопасности информации пользователя.

Список использованных источников:

1. Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 12.12.2023) «Об информации, информационных технологиях и о защите информации» [Электронный ресурс] // КонсультантПлюс: справочно-правовая система / Режим доступа: / http://base.www.consultant.ru/ (дата обращения 10.04.2024).

2. Байрушин, Ф.Т. Информационная безопасность как фактор обеспечения социальной стабильности в российском обществе / Ф.Т. Байрушин, И.В. Салов, И.Р. Абрамов // Евразийский юридический журнал. № 8(183). 2023. С.427-429.

3. Байрушин, Ф.Т. Информационная безопасность в современном многополярном укладе общественного устройстватве / Ф.Т. Байрушин, И.В. Салов, И.Р. Абрамов // Евразийский юридический журнал. № 8(183). 2023. С.416-417.

4. Благов, А.В. Анализ социальных сетей: учебное пособие / А.В. Благов, И.А. Рыцарев. – Самара: Самарский университет, 2020. – 104 с. – ISBN 978-5-7883-1556-0. – Текст: электронный // Лань: электронно-библиотечная система. – URL: https://e.lanbook.com/book/188862 (дата обращения: 11.04.2024).

5. Давидюк, Н.В. Мониторинг безопасности информационных систем: учебное пособие / Н.В. Давидюк, И.М. Космачева. – Санкт-Петербург: Интермедия, 2020. – 116 с. – ISBN 978-5-4383-0204-9. – Текст: электронный // Лань: электронно-библиотечная система. – URL: https://e.lanbook.com/book/161352 (дата обращения: 13.03.2024).

УДК 004

Д.И. Тазетдинов
Уфимский университет
науки и технологий, Уфа, Россия

Научный руководитель:
Ф.Т. Байрушин
Уфимский университет
науки и технологий, Уфа, Россия

БЕЗОПАСНОСТЬ В ОБЛАКЕ: СОВРЕМЕННЫЕ ВЫЗОВЫ И СТРАТЕГИИ ЗАЩИТЫ ДАННЫХ
SECURITY IN THE CLOUD: CURRENT CHALLENGES AND STRATEGIES FOR DATA PROTECTION

Аннотация: В данной статье рассматриваются современные вызовы и стратегии защиты данных в облаке. Облачные технологии становятся все более востребованными в современном бизнесе, но с ростом их популярности возрастает и уровень угроз для безопасности данных. В статье рассмотрены различные аспекты безопасности в облаке, включая уязвимости, типы атак и методы защиты.

Abstract: This paper discusses the current challenges and strategies for data protection in the cloud. Cloud technologies are becoming more and more popular in today's businesses, but as their popularity increases, so does the level of threats to data security. This article discusses various aspects of security in the cloud, including vulnerabilities, types of attacks, and defense methods.

Ключевые слова: Безопасность данных, облачные технологии, кибербезопасность, угрозы в облаке.

Keywords: Data security, cloud technology, cybersecurity, threats in the cloud.

В современном информационном ландшафте облачные технологии играют ключевую роль, обеспечивая компаниям гибкость, масштабируемость и доступность данных. Однако с ростом популярности облачных сервисов возрастает их уязвимость перед различными видами кибератак. Защита данных в облаке становится неотъемлемой частью стратегии информационной безопасности организаций всех размеров. Вызовы, с которыми сталкиваются компании при обеспечении безопасности в облаке, включают в себя сложность многоуровневой инфраструктуры, динамическую природу облачных сервисов и необходимость соблюдения строгих нормативных требований по защите данных. Угрозы могут происходить как извне, так и изнутри, и включать в

себя атаки типа DDoS, фишинг, вредоносное программное обеспечение и утечки данных [1].

Эффективная стратегия защиты данных в облаке должна включать в себя комплексный подход, включающий в себя криптографическое шифрование, механизмы идентификации и аутентификации, мониторинг событий и угроз, а также постоянное обновление и адаптацию политик безопасности в соответствии с изменяющимся уровнем угроз.

Переход к облачным вычислениям создал динамичную среду, в которой традиционные модели безопасности могут оказаться недостаточными. Поскольку данные и приложения перемещаются по сетям, устройствам и облачным провайдерам, обеспечение безопасности этой цифровой экосистемы становится важнейшей задачей.

По мере того как организации используют возможности защиты данных в облачных вычислениях для обеспечения гибкости и инноваций, они также должны укреплять свою защиту от развивающегося спектра киберугроз. В этом подробном руководстве мы рассмотрим стратегические меры, которые не только обеспечат безопасность облака, но и возведут ее в ранг неприступной крепости.

1. Архитектура облачной безопасности. Основа стратегии безопасности облачных вычислений начинается с разработки тщательно проработанной архитектуры безопасности облака. Эта архитектура должна включать в себя протоколы шифрования, надежные системы управления идентификацией и доступом, а также тщательную сегментацию сети [2].

2. Многофакторная аутентификация (MFA). Повысьте уровень безопасности, внедрив многофакторную аутентификацию (MFA). Этот дополнительный уровень защиты требует использования нескольких форм проверки, что значительно усложняет злоумышленникам задачу проникновения в вашу систему. MFA - это щит, защищающий критически важные точки доступа.

3. Облачные инструменты безопасности. Поставщики облачных услуг предлагают набор инструментов безопасности, разработанных специально для мониторинга и защиты облачных ресурсов. Использование этих инструментов позволяет получать информацию в режиме реального времени и заблаговременно устранять угрозы, обеспечивая безопасность и соответствие облачной среды нормативным требованиям [3].

4. Регулярные аудиты безопасности. Бдительность - краеугольный камень надежных облачных сервисов безопасности. Регулярно проводимые аудиты и оценки безопасности позволяют тщательно изучить инфраструктуру на предмет уязвимостей. Оперативное выявление и устранение слабых мест не только укрепляет безопасность, но и обеспечивает постоянное соответствие отраслевым нормам [4].

5. Защита данных пациентов в облаке. История успеха в здравоохранении, где было поручено защищать конфиденциальные записи пациентов в "облаке", отправилась в путь, чтобы обеспечить безопасность облачных данных. Руководствуясь непоколебимой приверженностью принципам конфиденциальности, они тщательно разработали целостную стратегию безопасности облачных вычислений. Шифрование стало крепостью, защищающей данные пациентов, а строгий контроль доступа возвел цифровые барьеры [5].

В заключении следует подчеркнуть важность эффективной защиты данных в облаке для современных организаций в контексте постоянно эволюционирующих киберугроз. Облачные технологии продолжают проникать в различные отрасли, предоставляя компаниям невероятные возможности для развития и роста, однако с этим ростом приходят и новые вызовы в области безопасности. Решение этих вызовов требует не только технических решений, но и стратегического подхода, включая обучение персонала, разработку политик безопасности и сотрудничество с провайдерами облачных услуг. Компании должны постоянно обновлять свои практики безопасности, учитывая последние тренды в кибербезопасности и анализируя свои системы на предмет уязвимостей.

Безопасность в облаке – это непрерывный процесс, требующий внимания и вложений. Однако инвестиции в безопасность оправданы, учитывая потенциальные последствия нарушения безопасности данных, включая финансовые потери, утрату репутации и нарушение законодательства о защите данных. В конечном итоге, стратегии защиты данных в облаке должны быть гибкими, адаптивными и масштабируемыми, чтобы организации могли эффективно реагировать на изменяющиеся условия и угрозы. Развитие и реализация таких стратегий позволят компаниям использовать преимущества облачных технологий, минимизируя при этом риски потенциальных нарушений безопасности данных.

Список использованных источников:

1. Тонких А.С., Авксентьева Е.Ю. Угрозы безопасности в облачных технологиях и методы их устранения // Международный журнал гуманитарных и естественных наук. – 2024. – № 1-2 (88). – С. 232-238.

2. Масленников В.В. и др. Управление информационной безопасностью в условиях цифровой экономики // Международная научно-практическая конференция по компьютерной и информационной безопасности (INFSEC 2023). – 2023. – С. 119-126.

3. Беспалова Н.В., Нечаев С.В. Обеспечение информационной безопасности облачных хранилищ // Вопросы безопасности. – 2023. – № 2. – С. 19-26.

4. Такушинов Д.С.М. Основные угрозы информационной безопасности и способы ее защиты // Современные проблемы и перспективные направления инновационного развития науки. – 2021. – С. 30-34.

5. Байрушин, Ф.Т. Информационная безопасность как фактор обеспечения социальной стабильности в российском обществе / Ф.Т. Байрушин, И.В. Салов, И.Р. Абрамов // Евразийский юридический журнал. № 8(183). 2023. С. 427-429.

УДК 004

Т.У. Фарвазов
Уфимский университет науки
и технологий, Уфа, Россия

Научный руководитель:
И.В. Салов
Уфимский университет науки
и технологий, Уфа, Россия

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ БИОМЕТРИЧЕСКИХ ПЕРСОНАЛЬНЫХ ДАНЫХ
ENSURING THE SECURITY OF BIOMETRIC PERSONAL DATA

Аннотация: В статье раскрыты особенности защиты персональных данных. Описаны вопросы обеспечения безопасности биометрических персональных данных, а также методы и средства их защиты.

Abstract: The article reveals the features of personal data protection. The issues of ensuring the security of biometric personal data, as well as methods and means of their protection, are described.

Ключевые слова: Персональные данные, биометрия, биометрические персональные данные, защита информации, информационная безопасность, защита персональных данных.

Keywords: Personal data, biometrics, biometric personal data, information protection, information security, personal data protection.

Биометрические персональные данные все больше внедряются во все сферы жизни для идентификации личности: медицина, страхование, банковская сфера и др. Биометрические персональные данные представляют собой такие данные, которые могут охарактеризовать особенности (физиологические и биологические) личности, например, фотографии, отпечатки пальцев или голос человека. Основным

нормативно-правовым актом, регулирующим действия с биометрическими персональными данными, является Федеральный закон № 152-ФЗ «О персональных данных» [1]. Изучив положения закона к биометрическим данным можно отнести следующие сведения о личности: почерк; голос; отпечатки пальцев; черты лица; рисунок радужной оболочки глаз; результаты анализа ДНК и др.

Биометрия способна сопоставить цифровые записи к конкретному человеку, поэтому такого рода данные являются мишенью для мошенников и злоумышленников, которые могут использовать их в корыстных целях.

Стоит отметить, что биометрия человека достаточно часто находится в открытом доступе [2]. В сети Интернет есть возможность найти фото- и видеозаписи практически каждого человека. Также идентификация с помощью биометрических данных подразумевает то, что результат подтверждения личности не равен 100%, т.е. человек может отличаться от той модели, которая загружена в систему [3]. При этом взломать логин и пароль пользователя намного проще, чем подделать лицо или сетчатку глаза.

С помощью биометрических персональных данных можно не только разблокировать умный домофон или турникет, но и зайти в банковское приложение или открыть банковский сейф, поэтому мошенники все больше работают над методами взлома подобных систем и фальсификацией биометрических данных.

Еще одной острой проблемой, связанной с биометрией является то, что сбор данных одного человека может многократно повторяться различными организациями при этом качество собранных данных может очень сильно различаться. Некачественная техника по записи голоса или создания фотографий для биометрической модели может увеличить количество ложных идентификаций. Вероятность того, что система воспримет одного человека за другого, возрастает. Т.е. некачественные биометрические ПДн могут предоставить мошенникам больше возможностей для фальсификации.

Чтобы система не воспринимала за живого человека фотографию или маску, используются технологии для выявления и проверки, что перед камерой находится живой человек, которому, например, нужно повторить какие-то жесты, позы или выражения лица.

Обмануть биометрическую идентификацию возможно и примером тому являются крупные инденты. Так, в 2019 году преступникам удалось украсть более 240 тысяч долларов у британской энергетической компании с помощью подделки голоса генерального директора. Сгенерировали голос злоумышленники при помощи искусственного интеллекта.

В 2023 году компания VisionLabs сумела разработать технологию OneShot Liveness по защите биометрических данных, которая меньше чем за секунду и по одному фото с телефона или web-камеры без дополнительных действий может обнаружить попытку мошенничества. Продукт прошел тестирование компании iBeta на соответствие международному стандарту ISO 30107-3 (Level 1 и Level 2). В ходе тестирования было предпринято более 3 тысяч попыток взломать технологию, процент успешных попыток равен 0.

Одной из особенностей государственного контроля и регулирования является создание в 2022 году единой системы биометрических данных (ГИС ЕБС). С помощью данной системы каждый гражданин РФ может получить государственные услуги безопасно. По официальным данным точность распознавания личности оставляет практически 100% (99,999%), а при использовании логина и пароля от «Госуслуг» взлом системы становится практически невозможным для злоумышленников.

Самой большой проблемой, с которой столкнулись компании в 2023 году, стал переход на автоматизированную обработку биометрических ПДн [4]. Так, с 1 июня 2023 года все предприятия, которые ранее обрабатывали биометрические данные, должны были передавать данные своих клиентов и сотрудников в систему ГИС ЕБС. Но чтобы передать биометрию - это не просто передать флешку с записанными данными, для этого нужно: заключить договор с «Центром биометрических технологий», чтобы подключить организацию к системе; купить специальное оборудование и ПО; перевести все биометрические данные в формат по приказу Министерства цифрового развития РФ от 12.05.2023 № 453; уничтожить все изображения лица и записи голоса, которые не выгружены в ЕБС.

Также одной из проблей при переходе на ЕБС стало то, что пользователь не знал находятся его данные в системе или нет, а также не было четких инструкций, что делать в случае если пользователь хочет удалить свои данные. Только с 1 января 2024 года гражданам РФ предоставили возможность просмотра биометрических данных через «Госуслуги», там же можно отказаться от использования данных.

В заключение стоит отметить, что уровень внедрения биометрических данных растет с каждым годом и захватывает все больше сфер человеческой жизни, при этом существует проблема правовой регламентации данного вопрос. Государство при этом с каждым годом принимает все больше нормативно-правовых актов и мер по защите биометрических персональных данных, поскольку ущерб от утечки и разглашения может нанести огромный ущерб как для личности, так и для определенных отраслей и даже государства. Безопасность биометрических систем требует постоянного совершенствования алгоритмов, архитектур и

инфраструктур биометрии, а также применения положений нормативно-правовых актов.

Список использованных источников:

1. Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 06.02.2023) «О персональных данных». – URL: http: // www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения 15.03.2024).

2. Бычков, А.И. Проблемы защиты персональных данных / А.И. Бычков. – Москва: Infotropic Media, 2020. – 116 с. – ISBN 978-5-9998-0352-8. – Текст: электронный // Лань: электронно-библиотечная система. – URL: https://e.lanbook.com/book/234317 (дата обращения: 15.03.2024).

3. Исмагилова, А.С. Программный модуль хэширования биометрических данных пользователя / А.С. Исмагилова, Н.Д. Лушников // Автометрия. – 2023. – Т. 59, № 4. – С. 20-28. – DOI 10.15372/AUT20230403.

4. Петренко, В.И. Защита персональных данных в информационных системах. Практикум: учебное пособие для вузов / В.И. Петренко, И.В. Мандрица. – 5-е изд., стер. – Санкт-Петербург: Лань, 2024. – 108 с.

УДК 004.056

Э.И. Хаерова, Б.И. Гатауллин
Казанский национальный исследовательский технический университет им. А.Н. Туполева–КАИ, Казань, Россия

Научный руководитель:
М.В. Тумбинская
Казанский национальный исследовательский технический университет им. А.Н. Туполева–КАИ, Казань, Россия

ВИРТУАЛЬНЫЙ ТРЕНАЖЁР ПО ОБРАБОТКЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ НА ФИЗИЧЕСКИХ НОСИТЕЛЯХ
VIRTUAL SIMULATOR FOR PROCESSING CONFIDENTIAL INFORMATION ON PHYSICAL MEDIA

Аннотация: В статье предложено современное цифровое решение, основанное на технологии виртуальной реальности, и выявлены формы

использования компьютерных технологий в рамках обучения. Виртуальный тренажер предназначен для обучения по направлению «Информационная безопасность» и представляет из себя набор интерактивных моделей в трехмерном виртуальном пространстве, позволяющий реализовать сценарии взаимодействия пользователей и специального программного обеспечения, по практическому применению задач защиты информации. В статье представлены результаты экспериментальных исследований по работе с виртуальным тренажером.

Abstract: The article proposes a modern digital solution based on virtual reality technology and identifies the forms of using computer technology in the framework of education. The virtual simulator is designed for training in the field of Information Security and is a set of interactive models in a three-dimensional virtual space that allows you to implement scenarios for user interaction and special software for the practical application of information security tasks. The article presents the results of experimental studies on working with a virtual simulator.

Ключевые слова: Цифровизация, образование, цифровые компетенции, виртуальный тренажер, цифровая среда

Keywords: Digitalization, education, digital competencies, virtual simulator, digital environment

Цифровые компетенции приобрели важное и ценное значение в образовательном контексте [1]. Качественное использование в своей деятельности цифровых технологий, соответствующих целям и задачам обучения в современных условиях, позволят сформировать цифровые компетенции у студентов. В работе предложен виртуальный тренажер для изучения дисциплины «Основы информационной безопасности» студентами направления подготовки «Информационная безопасность». Предложенный в работе виртуальный тренажер предназначен для теоретического и практического изучения обработки конфиденциальной информации на физических носителях.

Анализ литературных источников [2–8] показал, что на сегодняшний день существуют различные виды тренажеров и обучающих систем в области защиты информации. Так, например, в работе [8] рассматривается система и способ обучения модели обнаружения вредоносных контейнеров. На сегодняшний день существуют следующие виртуальные тренажеры: виртуальный тренажёр «Системы контроля и управления доступом» (ПО) фзи-трен-скуд, который предназначен для демонстрации и изучения принципов работы, а также монтажа и настройки системы контроля и управления доступом [2], виртуальный учебник «Программ-ные средства криптографии» (ПО) крипто-теор-по [3], виртуальный комплекс «Защита объекта от утечек информации по техническим

каналам», (ПО) тзи-трен-ткуи [4]. Анализ показал, что существующие тренажеры являются узконаправленными программными средствами, которые не способны обеспечить работу со съемными носителями информации.

Для разработки виртуального тренажера была использована среда Unity языка программирования C#. Для обработки фотографий была использована программа Adobe Photoshop, для редактирования и создания качественного, профессионального видео был использовано программное средство «Sony Vegas Pro 17». Продукт «Mixamo» был использован для загрузки и анимирования собственных 3D-моделей. В качестве инструментария работы с виртуальным тренажером выбраны следующие программные продукты по шифрованию данных «VeraCrypt», «Picocrypt», «FinalCrypt», по гарантированному удалению данных «Active@KillDisk Freeware», «Eraser», «BleachBit», по безопасному восстановлению данных «R-Studio», «EaseUS Data Recovery Wizard», «R-Saver» так как они являются наиболее эффективными среди аналогов, представленных на рынке в настоящее время.

Проведено тестирование и апробация виртуального тренажера. Тестирование выполнялось под виртуальной машиной с использованием программного средства VMware. В тестировании виртуального тренажера участвовали студенты КНИТУ-КАИ им. А.Н. Туполева направлений подготовки 10.05.02 «Информационная безопасность телекоммуникационных систем», которые оценивали удобство и эффективность использования. VR-тренажер способен работать под управлением операционных систем Windows, Linux. В результате тестирования замечаний к функциональной части обнаружено не было. VR-тренажер работает в соответствии с заявленными требованиями, обладает интуитивно понятным интерфейсом.

Список использованных источников:

1. Барахсанова, Е.А. Формирование профессиональной ИКТ-компетентности бакалавров – будущих педагогов в условиях двуязычия / Е.А. Барахсанова, В.А. Варламова // Современные наукоемкие технологии. – 2015. – № 10. – С. 68-71.

2. Виртуальный тренажёр «Системы контроля и управления доступом» (ПО) ФЗИ-ТРЕН-СКУД – Текст: электронный // ООО НПП «Учтех-Профи»: [сайт]. – URL: https://labstand.ru/catalog/virtualnye-trenazhery-i-emulyatory-zashhita-informaczii/virtualnyj-trenazhyor-sistemy-kontrolya-i-upravleniya-dostupom-po-fzi-tren-skud-2 (дата обращения: 01.02.2024).

3. Виртуальный учебник «Программные средства криптографии» (ПО) КРИПТО-ТЕОР-ПО – Текст: электронный // ООО НПП «Учтех-Профи»: [сайт]. – URL: https://labstand.ru/catalog/kriptograficheskie-sredstva/virtualnyj-trenazhyor-programmnye-sredstva-kriptografii-scrypto-virt (дата обращения: 01.02.2024).

4. Виртуальный комплекс «Защита объекта от утечек информации по техническим каналам», (ПО) ТЗИ-ТРЕН-ТКУИ – Текст: электронный // ООО НПП «Учтех-Профи»: [сайт]. – URL: https: // labstand.ru/catalog/zashhita-informaczii-ot-utechek-po-tehnicheskim-kanalam/virtualnyj-kompleks-zashhita-obekta-ot-utechek-informaczii-po-tehnicheskim-kanalam-tzi-virt (дата обращения: 01.02.2024)

5. Виртуальный тренажёр «Системы видеонаблюдения» (ПО) ФЗИ-ТРЕН-ВИДЕО – Текст: электронный // ООО НПП «Учтех-Профи»: [сайт]. – URL: https://labstand.ru/catalog/sredstva-fizicheskoj-zashhity-informaczii/virtualnyj-trenazhyor-sistemy-videonablyudeniya-fzi-video-virt (дата обращения: 01.02.2024).

6. Гафурова, Н.В. Продуктивные практики компетентностного подхода в образовании: монография / Н.В. Гафурова. – Красноярск: Сиб. федер. ун-т, 2017. – 154 с.

7. Патент № 2621697. Электронный путеводитель по медиаконтенту: № 2015110992: заявл. 2013.08.30: опубл. 2017.06.07 / Шиндлер Йорг, Цир Томас, Мюллер-Леффельхольц Георг; заявитель, патентобладатель Функе Диджитал ТВ гайд ГМБХ – Электронная копия доступна на сайте Федерального института промышленной собственности // ФИПС: [сайт]. – URL: https: / /fips.ru/iiss/document.xhtml? faces-redirect=true&id=d3c1df3971bb273542cf6f32c7369edb (дата обращения:26.01.2024).

8. Патент № 2697955. Система и способ обучения модели обнаружения вредоносных контейнеров: № 2018104438: заявл. 06.02.2018: опубл. 06.08.2019 / Крылов Владимир Владимирович, Лискин Александр Викторович, Антонов Алексей Евгеньевич; заявитель, патентобладатель Акционерное общество "Лаборатория Касперского" – Электронная копия доступна на сайте Федерального института промышленной собственности // ФИПС: [сайт]. – URL: https://fips.ru/iiss/document.xhtml?faces-redirect=true&id=a65f183665f1450a46bc81c7c5dd14a7 (дата обращения: 28.01.2024).

УДК 004

Н.А. Хаматнуров
Уфимский университет
науки и технологий, Уфа, Россия

Научный руководитель:
И.В. Салов
Уфимский университет
науки и технологий, Уфа, Россия

АНАЛИЗ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ МОБИЛЬНЫХ УСТРОЙСТВ
ANALYSIS OF INFORMATION SECURITY OF MOBILE DEVICES

Аннотация: В статье раскрыты основные принципы обеспечения информационной безопасности мобильных устройств. Особое внимание уделяется проблемам защиты информации при использовании мобильных устройств и методам безопасности и конфиденциальные данные.

Abstract: The article reveals the basic principles of ensuring the information security of mobile devices. Special attention is paid to the problems of information protection when using mobile devices and security methods and confidential data.

Ключевые слова: Информация, конфиденциальная информация, персональные данные, информации, информационная безопасность, мобильные устройства, смартфоны, планшеты, Интернет.

Keywords: Information, confidential information, personal data, information protection rights, information security, mobile devices, smartphones, tablets, Internet.

В настоящее время возможности и мощности мобильных устройств также стремительно увеличиваются, а в связи с этим возникают уязвимости и угрозы защиты конфиденциальной информации, которая хранится на данных устройствах.

Операционные системы (ОС) для мобильных представлен на рынке достаточно широко, защищенность некоторых достаточно слаба. Версий операционных систем также достаточно много, с чем связана проблема безопасности. Сейчас возглавляют рынок Google Android и Apple iOS. Каждая из ОС имеет свой подход к организации безопасности информации.

Стоит отметить, что по сравнению с персональными компьютерами поиск уязвимостей и угроз происходит в меньшей степени. Не все

разработчики и производители своевременно выпускают обновления на мобильные устройства, которые могут закрыть новые возникающие уязвимости.

На мобильных устройствах хранится огромное количество информации о пользователях, которая способна нанести ущерб: контакты из адресной книги; SMS-сообщения; фотографии и видеозаписи; данные геолокации; история браузеров; сохраненные пароли и логины электронных почты, социальных сетей и других интернет-площадок; данные из мобильных банков и др.

Основными угрозами безопасности информации для мобильных устройств являются: вредоносные приложения и веб-сайты (наиболее популярны трояны, которые содержатся во вредоносных ссылках и рекламе);

фишинговые атаки (большинство атак осуществляются через смс-сообщения и сообщения в социальных сетях, которые содержат вредоносные ссылки, так же 15% атак происходит через электронную почту пользователей); шпионское ПО, используемое для кражи персональных данных и данных для финансового мошенничества; атаки типа «человек посередине» с цель прослушивания и перехвата данных и др.

Одной из громких утечек информации с мобильных устройств стала атака 2016 года. Был создан троян «ANDROIDOS_LIBSKIN.A», который собирал всю информацию об аккаунте и отправлял на специальный удаленный сервер. Обнаружен он был компанией Trend Micro. Чтобы вирус заработал, пользователю нужно было просто установить его на телефон. Всего за несколько дней вирус распространился практически в 170 странах мира, включая Российскую Федерацию. Огромная база данных стала известна злоумышленникам. Поэтому вопрос защиты мобильных устройств набирает все большую актуальность.

При заражении вирусной программой устройство становится мишенью для мошенников, также путями компрометации может стать потеря или хищение смартфона. Рассмотрим более подробно, какими методами можно защитить устройства, чтобы защитить конфиденциальные данные:

1. Блокирование мобильного устройства. Обязательно нужно установить стойкий к взлому пароль и двухфакторную аутентификацию (дополнительно использовать отпечаток пальца или сканирование лица), а также ограничить количество неудачных попыток входа до минимального, чтобы в случае подбора пароля устройство было заблокировано. По стойкому к взлому паролю стоит рекомендовать использование генераторов пароля российского производства, например, комплекс программ «Специализированный генератор паролей» производства АО

«НПО РусБИТех». Не стоит использовать легкие к взлому пароли. Нельзя сохранять пароли на устройстве и в браузере, а также своевременно менять пароли.

2. Применение средств криптографической защиты. Основные конфиденциальные данные, которые хранятся на мобильном устройстве, обязательно должны быть зашифрованы. Даже в случае несанкционированного доступа к устройству мошенникам будет сложно понять и расшифровать конфиденциальную информацию. Примером может служить использование шифрованной папки Knox в смартфонах Samsung.

3. Запрещение установки «сомнительных» приложений из неофициальных источников. Скачивать ПО следует только из фирменных магазинов приложений мобильных устройств (Google Play, App Store, RuStore и др.) и только от известных разработчиков.

4. Использование средств антивирусной защиты. Применение антивирусного ПО поможет пользователю защитить свое устройство множества угроз. Следует проводить диагностику и «лечение» устройства на постоянной основе. Самыми популярными в 2024 году являются антивирусы Kaspersky Internet Security для Android и Dr. Web Security Space.

5. Ограничение доступа к данным. Чем меньше приложение получает данных о пользователе, тем выше уровень безопасности данных. Следует открыть приложение «Настройки», выбрать пункт «Приложения» и для каждого приложения настроить доступ к данным. Чтобы изменить разрешения нужно нажать на него и выбрать «Разрешить» или «Запретить».

Мобильные устройства стали неотъемлемой частью жизни людей. В телефонах, планшетах хранятся огромные массивы информации, утечка которых может нанести как репутационный ущерб, так и финансовый. Зачастую пользователи не применяют даже базовые средства защиты информации и потом теряют конфиденциальные данные. Защита мобильных устройств должна осуществляться на таком же высоком уровне, как и ПК.

Список использованных источников:

1. Бычков, А.И. Проблемы защиты персональных данных / А.И. Бычков. – Москва: Infotropic Media, 2020. – 116 с. – ISBN 978-5-9998-0352-8. – Текст: электронный // Лань: электронно-библиотечная система. – URL: https://e.lanbook.com/book/234317 (дата обращения: 10.03.2024).

2. Краковский, Ю.М. Защита информации: учебное пособие / Ю.М. Краковский. – Ростов-на-Дону: Феникс, 2016. – 347 с. - ISBN 978-5-222-26911-4. – Текст: электронный // Лань: электронно-библиотечная

система. – URL: https://e.lanbook.com/book/102279 (дата обращения: 21.03.2024).

3. Леонтьев, А.С. Защита информации: учебное пособие / А.С. Леонтьев. – Москва: РТУ МИРЭА, 2021. – 79 с. – Текст: электронный // Лань: электронно-библиотечная система. – URL: https://e.lanbook.com/book/182491 (дата обращения: 21.03.2024).

4. Прохорова, О.В. Информационная безопасность и защита информации: учебник для спо / О.В. Прохорова. – 5-е изд., стер. – Санкт-Петербург: Лань, 2024. – 124 с. – ISBN 978-5-507-47517-9. – Текст: электронный // Лань: электронно-библиотечная система. – URL: https://e.lanbook.com/book/385082 (дата обращения: 21.03.2024).

УДК 004

А.Р. Цагалов
Уфимский университет
науки и технологий, Уфа, Россия

Научный руководитель:
И.В. Салов
Уфимский университет
науки и технологий, Уфа, Россия

ПРОБЛЕМЫ БЕЗОПАСНОСТИ ТЕХНОЛОГИЙ NFC
NFC TECHNOLOGY SECURITY ISSUES

Аннотация: В статье раскрыты основные принципы обеспечения информационной безопасности при применении технологий NFC. Особое внимание уделяется проблемам защиты информации при использовании технологий бесконтактной оплаты и методам безопасности данных.

Abstract: The article reveals the basic principles of information security in the application of NFC technologies. Special attention is paid to the problems of information protection when using contactless payment technologies and data security methods.

Ключевые слова: Бесконтактные платежи, технологии NFC, мобильное устройство, платежи, NFC-платежи, терминал, денежные средства, безопасность NFC-платежей, информационная безопасность.

Keywords: Contactless payments, NFC technologies, mobile device, payments, NFC payments, terminal, cash, NFC payment security, information security.

Создание новых технологий в банковской сфере всегда сопровождается разработкой новых положений информационной безопасности. Работа NFC-технологий связана с персональными данным (ПДн): паспортными данными пользователя, банковскими счетами, контактами и др.

Технологии NFC (Near Field Communication) – это технологии бесконтактной оплаты, которые поддерживаются в том числе мобильными устройствами. Чтобы осуществлять платежи с помощь смартфона, внутри устройства должна находиться специальный модуль с микросхемой, который работает с помощью электромагнитной индукции [4,52].

В настоящее время российские граждане могут оплачивать товары и услуги с помощью применения технологий NFC, можно получить в банке платежный стикер или подключить к смартфону Mir Pay, который поддерживается устройствами на базе операционной системы Android. Процедура оплаты очень проста: мобильное устройство подносится к терминалу на расстоянии не менее 10 см, и платеж происходит моментально.

Платежные стикеры от банков появились в России не так давно, лишь в 2022 году. Они быстро получили популярность, поскольку частично заменили международные платежные системы Apple Pay и Google Pay. В стикерах находится специальный чип, который встраивается в приложение банка. NFC-чип считывает информацию с платежного терминала и передает ее в приложение банка. Стоит отметить, что NFC-чип для защиты информации хранит персональные данные пользователя в зашифрованном виде.

Преимуществами технологий NFC по сравнению с физическими банковскими картами являются:

– NFC- чип встроен в устройства, информации о пользователе нет, как это сделано на карте;

– авторизация по отпечатку пальца или лицу клиента при оплате и др.

При оплате с помощью NFC-чипа применяется шифрование, однако часть информации находится в открытом виде в памяти чипа карты. К подобным данным можно отнести совершенные операции, данные карты и др. Есть возможность получить данные сведения, например, с помощью мобильного устройства, которое работает в режиме ридера, установив определенные приложения. Тем самым получить и раскодировать

информацию о банковской карте и счете для мошеннических действий [1,32].

Как было отмечено ранее, дальность для передачи данных должна быть менее сантиметров. Это дает возможность считывания информации, если поднести специальное устройство. Также существует угроза заражения вирусным программным обеспечением (ПО), которое делает мобильное устройство пользователя ретранслятором сигнала NFC. Так, зараженное мобильное устройство может отправить информацию о доступности транзакции злоумышленникам. То есть появляется возможность снятия средств с банковского счета или получения информации о карте пользователя.

В случае кражи или потери устройства возможно получение доступа к денежным средствам пользователя и ко всей информации, которая требуется для проведения несанкционированных банковских транзакций.

Обезопасить мобильное устройство с NFC, можно следующим образом:

– настройка аутентификации с помощью пароля, графического ключа или биометрических данных (отпечаток пальца, сканирование лица), включить данную функцию можно в приложении банка;

– установка лимитов (максимальной суммы списаний);

– выключение технологии NFC, активация модуля только перед совершением оплаты;

– оплата только в знакомых и проверенных местах и особое внимание на внешний вид NFC-меток, установленных на терминалах и банкоматах;

– установка платежных приложений только из официальных магазинов, например, RuStore, Google Play, App Store и др.

– регулярное обновление платежных приложений до последних версий;

– не хранить платежную информацию в открытом виде на смартфоне;

– установка антивирусного ПО, например, Dr.Web Security Space, Kaspersky Internet Security для Android, и регулярное сканирование устройства на наличие угроз.

Для защиты пользователей банки-эквайеры ограничили возможность покупок без ввода пароля до 1000 рублей.

Защитить от атак на технологии NFC также помогают специальные аксессуары, например, RFID - картхолдер или чехол на телефон с экранизирующей вставкой из специальных материалов (металлических нитей, платин, фольги), способных отражать или поглощать радиоволны любой частоты. Эффективность защиты будет завить от плотности

прилегания и прочности материалов. В число одних из лучших чехлов входят Vaultskin MANHATTAN и Leatherology [6,18].

Технологии NFC плотно вошли в жизнь банковских пользователей. Эта функция очень проста и комфортна, однако ее безопасность зависит в том числе от самого пользователя. Поэтому применение вышеуказанных методов защиты поможет максимально снизить иски утечки информации и несанкционированного получения денежных средств.

Список использованных источников:

1. Вдовина, Е.С. Цифровизация банковского сектора в современных условиях: монография / Е.С. Вдовина, М.А. Куликова. – Тамбов: ТГТУ, 2022. – 100 с. – ISBN 978-5-8265-2542-5. - Текст: электронный // Лань: электронно-библиотечная система. – URL: https://e.lanbook.com/book/355220 (дата обращения: 20.04.2024)
2. Груздева, Л.М. Защита информации: учебное пособие / Л.М. Груздева. – Москва: РУТ (МИИТ), 2019. – 144 с. – ISBN 978-5-7876-0326-2. – Текст: электронный // Лань: электронно-библиотечная система. – URL: https://e.lanbook.com/book/188703 (дата обращения: 15.04.2024).
3. Краковский, Ю.М. Защита информации: учебное пособие / Ю.М. Краковский. – Ростов-на-Дону: Феникс, 2016. – 347 с. – ISBN 978-5-222-26911-4. – Текст: электронный // Лань: электронно-библиотечная система. – URL: https://e.lanbook.com/book/102279 (дата обращения: 20.04.2024).
4. Ларионова, С.Л. Информационная безопасность дистанционного банковского обслуживания: учебное пособие / С.Л. Ларионова. – Москва: Прометей, 2022. – 296 с. – ISBN 978-5-00172-343-1. – Текст: электронный // Лань: электронно-библиотечная система. – URL: https://e.lanbook.com/book/290516 (дата обращения: 21.04.2024).
5. Таштамиров, М.Р. Основы современного банкинга: учебное пособие / М.Р. Таштамиров, З.К. Тавбулатова. – Грозный: ЧГУ им. А.А. Кадырова, 2022. – 115 с. – Текст: электронный // Лань: электронно-библиотечная система. – URL: https://e.lanbook.com/book/339848 (дата обращения: 21.04.2024).

УДК 004.8

К.Ш. Чахалян, А.А. Ихсанова
Уфимский университет
науки и технологий, Уфа, Россия

Научный руководитель:
Д.С. Юнусова
Уфимский университет
науки и технологий, Уфа, Россия

ВЛИЯНИЕ РАЗВИТИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА НА ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ
THE IMPACT OF THE DEVELOPMENT OF ARTIFICIAL INTELLIGENCE ON INFORMATION SECURITY

Аннотация: Статья исследует влияние быстрого развития искусственного интеллекта на информационную безопасность. Рассматриваются как положительные, так и отрицательные аспекты использования искусственного интеллекта в сфере кибербезопасности. Представлены стратегии защиты от угроз, связанных с применением искусственного интеллекта.

Abstract: The article explores the impact of rapid development of artificial intelligence on information security. Both positive and negative aspects of using AI in the field of cybersecurity are considered. Strategies for protection against threats related to the application of artificial intelligence are presented.

Ключевые слова: Искусственный интеллект, кибербезопасность, киберугрозы.

Keywords: Artificial intelligence, cybersecurity, cyber threats.

Искусственный интеллект становится все более важным в современном мире, оказывая значительное влияние на различные сферы человеческой деятельности [1]. На кибербезопасность искусственный интеллект (ИИ) оказывает двойственное влияние [2]. С одной стороны, ИИ помогает автоматизировать защиту, улучшить обнаружение угроз и прогнозировать кибератаки. С другой стороны, он создает новые риски, такие как разработка более изощренных атак и уязвимости самих систем ИИ. Для усиления защиты необходимо разрабатывать безопасные системы ИИ, повышать осведомленность пользователей о киберугрозах и сотрудничать в сфере обмена информацией и разработки решений. В целом, ответственное развитие и внедрение ИИ позволит укрепить кибербезопасность и создать более безопасное цифровое пространство [3].

Развитие искусственного интеллекта оказало значительное влияние на кибербезопасность, изменив как объем данных, так и методы кибератак. Давайте рассмотрим каждый из этих аспектов подробнее.

Достижения в области искусственного интеллекта привели к значительному увеличению объема собираемых, обрабатываемых и хранимых данных. Это связано как с увеличением количества устройств, способных генерировать данные (например, датчиков IoT), так и с развитием технологий сбора и анализа информации. Однако увеличение объемов данных также повышает уязвимость систем кибербезопасности. Это связано с тем, что большие объемы информации требуют более сложной защиты от утечек, взломов и других киберугроз.

С развитием искусственного интеллекта киберпреступники также активно используют новые технологии для совершения кибератак. Машинное обучение и другие методы искусственного интеллекта могут использоваться для создания более сложных и эффективных атак, которые обходят традиционные методы обнаружения и защиты. Например, атаки, основанные на алгоритмах машинного обучения, могут адаптироваться к изменениям в окружающей среде и эффективно обходить системы безопасности.

Искусственный интеллект также играет важную роль в киберугрозах. Киберпреступники могут использовать алгоритмы машинного обучения для обхода защитных механизмов и создания вредоносного ПО, способного нанести ущерб информационным системам. Кроме того, автоматизация процессов на основе искусственного интеллекта может стать причиной масштабных, скоординированных кибератак, способных нанести серьезный ущерб отдельным организациям или целым странам.

Искусственный интеллект может быть использован для совершенствования методов фишинга и социальной инженерии. Алгоритмы машинного обучения могут анализировать данные пользователей из социальных сетей, электронной почты, сообщений и других источников для создания персонализированных и убедительных мошеннических сообщений. Благодаря этому фишинговые атаки становятся более индивидуальными для потенциальных жертв, а значит, их сложнее обнаружить.

Машинное обучение позволяет киберпреступникам создавать более сложные и эффективные вредоносные программы. Алгоритмы машинного обучения помогают создавать вредоносные программы, которые обходят традиционные методы обнаружения и защиты. Например, атаки, основанные на алгоритмах машинного обучения, могут адаптироваться к изменениям в окружающей среде и эффективно обходить системы безопасности.

Искусственный интеллект также используется для автоматизации процесса кибератак. Киберпреступники могут использовать алгоритмы машинного обучения для создания автоматизированных систем, способных осуществлять масштабные, скоординированные атаки на информационные системы. Это может нанести ущерб отдельным организациям, целым секторам экономики или странам при минимальных усилиях.

Чтобы укрепить защиту от киберугроз в условиях развития искусственного интеллекта, необходимо использовать комплексный подход, включающий разработку специализированных систем мониторинга и обнаружения угроз, использование методов машинного обучения для создания адаптивных систем, внедрение систем реагирования на инциденты, развитие человеческих ресурсов в области информационной безопасности через обучение сотрудников и проведение учебных симуляций угроз, применение технологий искусственного интеллекта для анализа данных и создания систем прогнозирования угроз, разработку систем защиты на основе машинного обучения и использование методов искусственного интеллекта для анализа трафика и выявления аномалий в сетевой активности.

Таким образом, разработки в области искусственного интеллекта оказывают как положительное, так и отрицательное влияние на кибербезопасность. С одной стороны, применение ИИ позволяет создавать более эффективные системы мониторинга и обнаружения угроз, которые также могут заранее предсказывать потенциальные атаки. С другой стороны, киберпреступники также могут использовать технологии ИИ для совершенствования своих атак и обхода существующих мер безопасности.

Важно понимать, что развитие ИИ требует постоянного совершенствования методов защиты от киберугроз. Стратегии и технологии безопасности должны быть проактивно адаптированы к новым вызовам, возникающим в связи с использованием искусственного интеллекта в киберпреступности.

С быстрым развитием технологий киберугрозы становятся все более сложными и изощренными. Для эффективной защиты информации и данных от кибератак необходимо постоянно совершенствовать меры безопасности.

Комплексный подход к кибербезопасности, включающий разработку специализированных систем мониторинга, обучение персонала и применение методов искусственного интеллекта, позволит улучшить защиту от киберугроз и повысить общую безопасность [4].

Постоянное обновление и адаптация стратегий безопасности к новым вызовам, возникающим в результате развития технологий, - ключевой

элемент успешной борьбы с киберугрозами и обеспечения надежной защиты информации в современном мире.

Список использованных источников:

1. Попова Н.И., Стрельникова Т.И. Влияние искусственного интеллекта на национальную безопасность //Информационные технологии и информационная безопасность в профессиональной деятельности. – 2022. – С. 95-100.

2. Хусанова М., Ганиева Ш., Садирова Х. Технологические инновации и развитие угроз информационной безопасности // Conference on Digital Innovation:" Modern Problems and Solutions". – 2023.

3. Камалова Г.Г. Информационная безопасность и искусственный интеллект: организационно-правовые проблемы / Г.Г. Камалов, 2023. – С. 20.

4. Исмагилова, А.С. Особенности защиты информационной системы с применением искусственной нейронной сети / А.С. Исмагилова, Н.Д. Лушников // Информационная безопасность цифровой экономики: материалы XIX научно-практической конференции (в рамках X Пленума регионального отделения Федерального учебно-методического объединения в системе высшего образования по укрупненной группе специальностей и направлений подготовки 10.00.00 «Информационная безопасность» по Сибирскому и Дальневосточному федеральным округам (СибРОУМО)), Улан-Удэ, 07–11 июня 2023 года. – Новосибирск: Сибирский государственный университет телекоммуникаций и информатики, 2023. – С. 140-152.

УДК 004

Б.С. Шамсутдинов
Уфимский университет
науки и технологий, Уфа, Росси
Научный руководитель:
И.В. Салов
Уфимский университет
науки и технологий, Уфа, Россия

МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕЖЕЛАТЕЛЬНЫХ ПОЧТОВЫХ РАССЫЛОК, СПАМ-ЗВОНКОВ И СООБЩЕНИЙ
WAYS TO PROTECT INFORMATION FROM UNSOLICITED MAILINGS, SPAM CALLS AND MESSAGES

Аннотация: В статье раскрыты основные принципы обеспечения информационной безопасности пользователей при атаках спама.

Особое внимание уделяется проблемам защиты информации при почтовых рассылках, звонках и сообщениям.

Abstract: The article reveals the basic principles of ensuring the information security of users during spam attacks. Special attention is paid to the problems of information protection during mailings, calls and messages.

Ключевые слова: Спам, телефонный спам, почтовый спам, почтовые рассылки, звонки, СМС-сообщения, чат-боты, конфиденциальная информация, персональные данные, информации.

Keywords: Spam, phone spam, mail spam, mailing lists, calls, SMS messages, chatbots, confidential information, personal data, information protection rights.

В настоящее время вопрос защиты пользователей от спама становится как никогда актуальным. Почтовые рассылки, сообщения, звонки и СМС от злоумышленников с цель кражи персональных данных и доступа к банковской информации ежедневно получают миллионы пользователей.

Спам – это массовая рассылка информации, отправленная без согласия получателя в рекламных и мошеннических целях. По последней статистике TelecomDaily 2023 года около 70% полученных писем на электронную почту являются спамом и каждый 7 телефонный звонок (порядка 15% от общего числа) – спам. То есть стать жертвой мошенников может стать любой человек, который пользуется электронными ресурсами или мобильным телефоном.

Спам в основном представляет собой рекламные рассылки и предложения на покупку товаров и с услуг, если получатель не предоставлял согласие на получение рассылки. Рекламные предложения могут надоедать получателю, но стоит отметить, что в основном не угрожают безопасности данных [4,36].

Но существуют и спам, который может нанести ущерб для получателя, как материальный ущерб, так и утечка конфиденциальной информации и персональных данных. В основном данный вид спама злоумышленники используют при отправке фишинговых сообщений под видом банка или социальной сети, где просят ввести логин и пароль для подтверждения учетной записи, тем самым получая полный доступ к аккаунту пользователя и незаконному использованию данных в личных целях.

При взломе социальных сетей или мессенджеров участилась отправка спама с подозрительными ссылками, которые заражены вирусным ПО. Когда получатель открывает ссылку или вложение его устройство автоматически становится зараженным и подвергается угрозе утечки информации.

Существуют определенные способы для незаконного сбора контактов:

1. Парсинг. Специальное ПО, которое способно автоматически собирать и систематизировать данные из источников сети Интернет (номер телефона, адрес электронной почты). Сейчас большую популярность получили Telegram-чаты, найти участника и посмотреть его контактный номер телефона для злоумышленника в этом случае не составит труда.

2. Покупка или взлом баз данных. В случае, если базы данных не защищены или защита происходит на недостаточном уровне, хакеры могут получить доступ к информации. Так, в 2022 году была утечка базы заказов из «Яндекс.Еды». В сеть попали несколько миллионов данных о заказах, в том числе ФИО, телефонные номера и адреса доставок.

3. Случайная генерация. При помощи специального ПО злоумышленники путем генерации могут подобрать номер телефона или почтовый адрес, используя, например, в качестве ключевого слова распространённое имя или фамилию [1,32].

В настоящее время пользователи столкнулись с огромной проблемой, когда они попадают на спам-ботов, называемых SMS-бомбер. Особое распространение данные боты получили в Telegram. Данные сервисы осуществляют массовую рассылку на заданный номер. Рассылка спама доступна в нескольких режимах и может продолжаться от 5 до 60 минут. Самый расширенный режим подразумевает отправку почти 1,5 тысяч сообщений и непрерывных звонков. В одном из подобных чат-ботов за 2023 год под влияние спама попало порядка 370 тысяч номеров пользователей.

Рассылка спама влечет наложение штрафов. Штрафы на юридическое лицо за отправку навязчивой рекламы – до 500 тысяч рублей. С технической стороны – блокирование аккаунтов, которые осуществляют рассылки.

С каждым годом становится все больше сервисов, осуществляющих спам-рассылки, но есть и меры, которые помогут защитить себя и свои данные: включение антиспамовых фильтров в почтовых сервисах; нельзя отвечать на сообщения или письма, так как сервис увидит активность пользователя и спама будет еще больше; не размещать электронную почту и номер телефона на открытых веб-сервисах; обязательное прочтение условий при регистрации на сервисах, так в условиях подписки или регистрации может стоять согласие на рассылки по умолчанию; регулярное обновление операционной системы устройства, чтобы исключить появление новых угроз информационной безопасности; применение функции жалобы на спам, та сервис может пресечь незаконную отправку спама и заблокировать аккаунт; использовать специальные программы для фильтрации спама [2,15].

Каждую неделю 83% российских абонентов получают как минимум по одному спам-звонку, которые совершают как в рекламных целях, так и с целью мошенничества. Самыми популярными программами для защиты от спам-звонков и сообщений являются: Kaspersky Who Calls, определитель номера от «Яндекса», определитель номера от Тинькофф.

Все эти программы определяют, какой организации может принадлежать номер телефона. Присутствует функция проверки на жалобы на спам или мошенничество. База данных сервисов постоянно обновляется. Программы путем анализа собирают статистику о частоте звонков, их количестве и продолжительности разговоров, тем самым могут присвоить номеру статус «спама» или «подозрение на мошенничество». Помочь с незаконной рассылкой и звонками могут и операторы сотовой связи, в основном это платная услуга. Она присутствует практически у каждого крупного оператора сотовой связи: «МТС», «Мегафон», «Билайн» и «Tele2».

Методы спама становятся изощрёнными. Использовать специальные фильтры, программное обеспечение и цифровую гигиену необходимо каждому пользователю. Особое внимание стоит уделить посещаемым веб-ресурсам, получаемым подозрительным сообщениям, звонкам с незнакомых номеров и предоставлением информации непроверенным сервисам.

Список использованных источников:

1. Бычков, А.И. Проблемы защиты персональных данных / А.И. Бычков. – Москва: Infotropic Media, 2020. – 116 с. – Текст: электронный // Лань: электронно-библиотечная система. – URL: https://e.lanbook.com/book/234317 (дата обращения: 18.03.2024).

2. Романов, В.Г. Социальная инженерия мошенничества: монография / В.Г. Романов, И.В. Романова. – Чита: ЗабГУ, 2021. – 240 с. – ISBN 978-5-9293-2771-1. – Текст: электронный // Лань: электронно-библиотечная система. – URL: https://e.lanbook.com/book/271808 (дата обращения: 07.04.2024).

3. Соловьев, И.Н. Как не стать жертвой телефонного мошенничества. Практикум: учебное пособие / И.Н. Соловьев. – Москва: Проспект, 2022. – 21 с. – ISBN 978-5-392-35233-3. – Текст: электронный // Лань: электронно-библиотечная система. – URL: https://e.lanbook.com/book/280202 (дата обращения: 07.04.2024).

4. Известия: Разговорчивый жанр: спам-звонки и SMS регулярно получают 94% россиян: офиц. сайт. URL: https://iz.ru/1679696/iana-shturma-kseniia-nabatkina-valeriia-mishina/sredstvennye-deistviia-na-chto-shel-biudzhet-orska-vmesto-obsluzhivaniia-damby (дата обращения: 07.04.2024).

УДК 004

Э.Ф. Шарипова
Уфимский университет
науки и технологий, Уфа, Россия

Научный руководитель:
С.С. Валеев
Уфимский университет
науки и технологий, Уфа, Россия

МУНИЦИПАЛЬНЫЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ВОПРОСЫ ЗАЩИТЫ ИНФОРМАЦИИ
MUNICIPAL INFORMATION SYSTEMS AND INFORMATION SECURITY ISSUES

Аннотация: В статье обсуждаются основные особенности муниципальных информационных систем и их взаимосвязь с задачами защиты информации. Рассматривается состояние, развитие муниципальных информационных систем (МИС), их основные функции. Описываются основные угрозы, с которыми могут столкнуться МИС, а также методы и технологии защиты информации, которые могут быть использованы для обеспечения безопасности муниципальных данных.

Abstract: The article discusses the main features of municipal information systems and their relationship with the tasks of information protection. The state and development of municipal information systems (MIS), their main functions are considered. Described the main threats that IIAs may face, as well as information security methods and technologies that can be used to ensure the security of municipal data

Ключевые слова: Муниципальные информационные системы, местное самоуправление, защита информации, угрозы безопасности, риски, районная администрация.

Key words: Municipal information systems, local government, information protection, security threats, risks, district administration.

Муниципальные и государственные учреждения являются ключевыми структурами, отвечающими за управление и обеспечение различных услуг и функций в обществе. Хотя обе эти системы могут иметь некоторые общие функции, они обладают своими уникальными особенностями и отличаются в своей структуре, компетенции и источниках финансирования [1].

Муниципальные учреждения обычно имеют более узкую компетенцию, сосредоточенную на конкретных территориях и локальных проблемах. Они отвечают за обеспечение освещения, водоснабжения, уличного хозяйства, транспорта, образования и здравоохранения на своей территории. Муниципальные советы и мэры избираются на местных выборах и отвечают перед местным населением.

Государственные учреждения, в свою очередь, имеют более широкую компетенцию и отвечают за стратегическое планирование, национальную политику, экологию, безопасность, внешнюю политику и оборону. Государственные органы создаются и контролируются национальными законодательными и исполнительными органами. В настоящее время муниципальные информационные системы (МИС) являются ключевым инструментом для управления городом и обеспечения качества жизни его жителей. Они включают в себя различные компоненты, такие как системы управления документооборотом, системы управления проектами, системы управления финансами и системы управления персоналом [2].

Одним из информационных источников является веб-сайт организации. На официальном веб-сайте муниципальной администрации содержится вся необходимая информация. Там можно найти сведения о поселении и, например, воспользоваться интернет-приемной. Любой заинтересованный гражданин может обратиться с вопросом к администрации. Сайт ежедневно обновляется, а необходимые документы доступны для ознакомления. Использование официального сайта очень удобно, но требует организации мер обеспечения защиты информации.

Ограничение доступа к данным в муниципальном управлении и государственном секторе играет важную роль. Обеспечение конфиденциальности является основным принципом в управлении этими сферами.

В связи с растущим количеством злоупотреблений и кибератак, решение задачи обеспечения защиты информации становится все более важной.

Создание и поддержание безопасности МИС требуют внимания и ресурсов с обеих сторон – как от технических экспертов, так и от руководства муниципалитетов.

Далее рассмотрим основные аспекты защиты информации в муниципальных информационных системах.

Защита информации – это комплекс мер по защите информации от нежелательных пользователей [3]. Защита информации в МИС зависит от решения нескольких основных задач:

– определение конфиденциальности используемых данных. Определение уровня класса защищенности для данных зависит от того, насколько критичны данные для города и его жителей. Необходимо

выяснить, какие данные могут быть утеряны или украдены, и какой ущерб это может причинить;

– контроль доступа к данным. Предотвращение незаконного доступа к данным и предотвращение несанкционированного изменения или удаления данных;

– защита от кибератак. Защита от вирусов, шпионского ПО, DDoS-атак и других видов кибератак;

– комплексная защита. Решение задачи защиты информации должно быть комплексным, включая физическую защиту, техническую защиту и защиту возможных инсайдеров [4].

В качестве мер для решения перечисленных задач обеспечения информационной безопасности МИС можно выделить следующие шаги.

Анализ возможного ландшафта киберугроз предполагает, что по мере расширения цифровой экосистемы муниципалитета увеличивается и площадь атак, и общий ландшафт угроз. Муниципалитеты должны контролировать риски, связанные с цифровыми активами, хранящимися в облаке, взаимодействием между департаментами и удаленными сотрудниками.

Еще одна стратегия, которая может помочь муниципалитетам сосредоточить свои усилия на обеспечении безопасности, заключается в том, чтобы сравнивать показатели безопасности с аналогичными показателями в других городах. Это может помочь руководителям служб безопасности определить цели в области безопасности.

Также эффективной мерой является обновление политики безопасности для устройств сотрудников и удаленного доступа к ним. Следует поощрять пользователей к принятию простых в применении мер безопасности, таких как постоянное использование защищенных подключений, регулярное обновление программного обеспечения и соблюдение правил использования надежных паролей.

Для обеспечения безопасности данных в Российской Федерации применяются государственные законы «О конфиденциальной информации» и «О цифровизации, информации и ее защите». На уровне местных органов власти используются уставы и различные нормативно-правовые документы, касающиеся защиты информации [5].

Таким образом, можно сделать вывод, что защита информации в муниципальных информационных системах является комплексной задачей, решение которой требует применения технических, организационных и правовых мер.

Список использованных источников:

1. Перечень основных информационных систем, находящихся в ведении органов местного самоуправления – URL: http://radm.gtn.ru/administration/informsystem/ (дата обращения 25.04.2024).

2. Защита информации – URL: https://www.consultant.ru/document/cons_doc_LAW_61798/0e9ec16b786dcbdaaa7f44abfc4a15e601d5be22/?ysclid=lvoypsoddl621880813 (дата обращения 25.04.2024).

3. ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации.

4. Государственные и муниципальные учреждения – URL: https://infoculture.gitbook.io/opengovfinances/orgs/publicbodies (дата обращения 25.04.2024).

5. Федеральный закон об информации, информационных технологиях и о защите информации – URL: https://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения 25.04.2024).

СЕКЦИЯ 3. ОРГАНИЗАЦИОННО-ПРАВОВЫЕ АСПЕКТЫ ЗАЩИТЫ ИНФОРМАЦИИ

УДК 330.101.2

В.М. Антипова
Уфимский университет
науки и технологий, Уфа, Россия

Научный руководитель:
Б.К. Кушубакова
Уфимский университет
науки и технологий, Уфа, Россия

СОДЕРЖАНИЕ ИНФОРМАЦИИ О ДЕЯТЕЛЬНОСТИ ОРГАНИЗАЦИЙ, СОСТАВЛЯЮЩИХ КОММЕРЧЕСКУЮ ТАЙНУ И СПОСОБЫ ОБЕСПЕЧЕНИЯ ЕЁ ЗАЩИТЫ
THE CONTENT OF INFORMATION ABOUT THE ACTIVITIES OF ORGANIZATIONS THAT CONSTITUTE A TRADE SECRET AND WAYS TO ENSURE ITS PROTECTION

Аннотация: В статье рассмотрены риски потерь и существующие способы защиты конфиденциальной информации о деятельности организации, составляющей коммерческую тайну. Также показана необходимость градации информации и разработки системы дифференцированного доступа работников к информации, в целях усиления ее защиты от потерь.

Abstract: The article discusses the risks of losses and existing ways to protect confidential information about the activities of an organization that constitutes a trade secret. It also shows the need for gradation of information and the development of a system of differentiated access of employees to information in order to strengthen its protection against losses.

Ключевые слова: Коммерческая тайна, информация, защита информации организации.

Keywords: Trade secret, information, protection of trade secrets.

В современных условиях информация стала стержнем движения социально-экономического развития государства, которую необходимо защищать в целях обеспечения национальной безопасности. Особое значение имеет информация о деятельности организаций, которые составляют первичное звено экономики государства.

Часть информации о деятельности организаций отражается в системе бухгалтерского учета и отчетности и выступает общедоступной. Так, в

пункте 11 статьи 13 федерального закона «О бухгалтерском учете» от 06.12.2011 N 402-ФЗ установлено, что в отношении бухгалтерской (финансовой) отчетности не может быть установлен режим коммерческой тайны. [5]

Состав информации, которая относится к категории, защищенной зафиксирован в Федеральном Законе «О коммерческие тайны» №98-ФЗ от 29.07.2004 г. В п.1 ст.3 приведенного закона дано определение коммерческой тайны как «режима конфиденциальной информации, позволяющей её обладателям при существующих или возможных обстоятельствах увеличивать доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду». [4]

Из данного положения следует, что коммерческая тайна обладает следующими признаками:

– информация имеет конфиденциальный характер;

– информация имеет коммерческую ценность, в связи с неизвестностью третьими лицами;

– к коммерческой информации отсутствует свободный доступ;

– получение информации влечет за собой определенную выгоду.

– организация должна принять меры по её защите и конфиденциальности.

Информацию, составляющую коммерческую тайну можно разделить на 4 больших блока. Это сведения: 1) научно-технического характера, включающая патенты, ноу-хау, методы повышения эффективности, пароли, программное обеспечение; 2) технологического и производственного характера включающая чертежи, модели, документацию на оборудование, технологические карты; 3) финансового характера, включающая данные управленческого учета и отчетности и формирования цен, расчеты себестоимости и денежного потока; 4) бизнес-характера, с данными о поставщиках и подрядчиках, о клиентах, с планами по продажам и сбыту, анализ рынка и конкурентов.

Основной целью установления коммерческой тайны является минимизация рисков потерь вследствие незаконного доступа к ней.

Защита коммерческой тайны у организации выступает наиболее сложным участком, в силу ее специфичности. Специфичность этой работы заключается в наличии множества точек риска, обусловленного тем, что каждый работник производственного и административного уровня, владея определенной информацией, выступает носителем риска неопределенного уровня. Кроме того, любая организация работает так, что информационный обмен между работниками осуществляется спонтанно, и точное количество работников, которые становятся владельцами конфиденциальной информации неизвестно.

Для обеспечения защиты конфиденциальной информации необходимо установить уровни степени конфиденциальности и разработать систему дифференцированного доступа работников.

Нужно выделить следующие уровни конфиденциальности: информация высшей степени секретности, строго конфиденциальная информация, конфиденциальная информация и уровень сведений ограниченного доступа.

Существуют различные способы защиты конфиденциальной информации, в том числе: правовые, предполагающую наличие юридических норм, соблюдение которых создает условия для защиты информации [4,1,3,2]; административно-организационные (представляют собой введение режима коммерческой тайны); технические, включающую аутентификацию и управление доступом, фильтрацию и шифрование информации, программное обеспечение, позволяющую исключить хищение информации и выявлять угрозы; психологические, предполагающие проведение разъяснительной работы с персоналом, создание доверительных отношений в коллективе и с начальством, проведение регулярных проверок с выявлением неблагонадежных лиц. [6, С.55] Каждая организация разрабатывает систему индивидуально.

Для снижения угрозы утечки необходимо закрепить дифференцированный доступ к информационной системе управления организацией, с одновременным контролем за соблюдением режима доступа. Для этого необходимо применить и правовые, и административно-организационные и технические способы защиты информации. Например, дифференцированный доступ к цифровой информации, необходимо внедрить в документооборот наряду с оперативным отслеживанием выполнения требований каждым отдельным работником.

Решить эту задачу можно путем внедрения системы документооборота на основе программы класса IdM/IGA, которая позволит осуществить:

1. сбор информации из кадровых систем в режиме реального времени, что позволяет специалистам, отвечающим за сохранение коммерческой тайны, своевременного реагировать на события. Например, произвести блокировку пользователей, сделать запрос на корректировку прав доступа и т.д.;

2. автоматизацию документооборота, позволяющую быстро редактировать данные о пользователях и видеть кому открыты доступы в реальном времени, и включать в список доступа коммерческой тайны новых сотрудников;

3. исключить накопление в системах бесхозных аккаунтов и учетных записей с избыточными правами. Система документооборота в режиме

реального времени отслеживает «учетки», и при обнаружении отклонений оповещает об этом специалистов, ответственных за сохранность информации. [7, С.135]

Таким образом, для сохранения коммерческой тайны, необходимо использовать систему документооборота, в которой дифференцированный доступ сочетается с оперативным контролем за соблюдением режима, что позволяет оперативно отслеживать и нейтрализовать возникающие проблемы. Такая система позволит существенно снизить риск утечки конфиденциальной информации, снижая соответственно и риск потери выгод и преимуществ организации, связанных с владением конфиденциальной информации.

Список использованных источников:

1. Гражданский кодекс Российской Федерации от 30 ноября 1994 года N 51-ФЗ.
2. Трудовой кодекс Российской Федерации от 30.12.2001 N 197-ФЗ.
3. Федеральный закон «О коммерческой тайне» от 29.07.2004 N 98-ФЗ.
4. Федеральный закона «О бухгалтерском учете» от 06.12.2011 N 402-ФЗ.
5. Дышекова, Д.А. Правовая защита коммерческой тайны // Теория права и межгосударственных отношений. – 2022. – Т. 1, № 6(26). – С. 54-57.
6. Пономарев, Р.А. Особенности коммерческой тайны в организации // Моя профессиональная карьера. – 2023. – Т. 2, № 47. – С. 134-137.

УДК 004

Ахмадиева Вилена Ф., Ахмадиева Виола Ф.
Уфимский университет
науки и технологий, Уфа, Россия

Научный руководитель:
М.Р. Шафиков
Уфимский университет
науки и технологий, Уфа, Россия

ОТВЕТСТВЕННОСТЬ ЗА РАСПРОСТРАНЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ, СОДЕРЖАЩИХСЯ В БАЗАХ ПОИСКОВЫХ БОТОВ И СПОСОБЫ СКРЫТИЯ ЛИЧНОЙ ИНФОРМАЦИИ
RESPONSIBILITY FOR DISSEMINATION OF PERSONAL DATA CONTAINED IN THE DATABASES OF SEARCH BOTS AND METHODS OF CONCEALMENT OF PERSONAL INFORMATION

Аннотация: В настоящее время существует большое количество поисковых ботов, содержащих личную информацию из социальных сетей и различных сайтов, которые имеют базу данных, люди активно пользуются ботами, чтобы получать различную информацию или помощь. Пользователи ботов, таких как популярный поисковый Telegram-бот «Глаз Бога» несут аналогичную ответственность с теми, кто имеет доступ к государственным базам данных по трудовому договору и разглашают эти сведения.

Abstract: Currently, there are a large number of search bots containing personal information from social networks and various sites that have a database, people actively use bots to get various information or help. Users of bots such as the popular search Telegram bot "God’s Eye" have a similar liability to those who have access to government databases under a labour contract and disclose this information.

Ключевые слова: Личные данные, поисковый бот, социальная сеть, база данных, обработка персональных данных, защита персональных данных, идентификация, государственная система, утечка данных, ущерб.

Keywords: Personal data, search bot, social network, database, personal data processing, personal data protection, identification, government system, data breach, damage.

Сегодня вопрос защиты персональных данных как никогда актуален, ведь утечка личных данных несёт угрозу реализации тяжёлых последствий. Для гарантии безопасности конфиденциальных сведений

необходимо предпринимать шаги в области обеспечения информационной безопасности, а также контролированию соблюдения законодательства в сфере защиты персональных данных.

Гарантируя своим гражданам безопасность, государство заботится о защите и обеспечении конфиденциальности их личных данных. Федеральный закон №152 "О персональных данных" от 27.07.2006 года является основным нормативно-правовым актом, регулирующим защиту персональных данных. Этот закон определяет принципы и условия обработки персональных данных.

Информацию о себе человек оставляет в социальных сетях, на маркетплейсах, при регистрации на различных сайтах, которые имеют базу данных. Именно поэтому в настоящее время создаются и активно используются поисковые Telegram-боты, предназначенные для поиска информации о человеке. Они собирают данные, оставленные пользователем в интернет-пространстве, и таким образом формируют свою базу данных.

Один из таких ботов — "Глаз Бога". Он является официальным Telegram-ботом для поиска информации о людях по ограниченным данным. Платформу "Глаз Бога" разработал российский программист Евгений Антипов в январе 2020 года. За четыре года, канал платформы "Глаз Бога" достиг колоссального успеха. На сегодняшний день база данных этого бота насчитывает 45 674 500 телефонных номеров и 199 345 699 фотографий, что позволяет получить обратную связь на поисковый запрос практически мгновенно [1].

Обусловив нарушением российских законов в области персональных данных, распространяемых через бот «Глаз Бога», 12 марта 2021 Роскомнадзор потребовал от команды мессенджера Telegram заблокировать его.

За использование таких нелегальных сервисов, как «Глаз Бога» на сегодняшний день законодательством ответственность не предусмотрена. Но такие действия могут повлечь за собой уголовное или административное наказание. Согласно законодательству РФ, обработка, передача и распространение персональных данных третьим лицам требует согласия субъекта этих данных следовательно деятельность поискового бота нарушает ряд нормативных актов в области защиты персональных данных РФ.

Законодательством предусмотрена серьезная ответственность для администраторов нелегальных сервисов и лиц, представляющих данные для их использования. Эти деяния могут быть квалифицированы в соответствии со статьей 137 Уголовного кодекса Российской Федерации, где указывается нарушение неприкосновенности частной жизни [2].

Сотрудники, допустившие утечку персональных данных, могут быть привлечены к ответственности в административном порядке согласно положениям части 1 статьи 13.11 КоАП РФ в области персональных данных [3].

Сотрудники, работающие с государственными базами данных, которые содержат персональные данные, так же несут ответственность за разглашение этих данных в соответствии с законодательством о защите персональных данных. Например, медицинский работник, имеющий доступ к ЕГИСЗ (Единая государственная система здравоохранения), тем самым получает важные сведения о пациентах, распространение которых наказывается государством. В случае утечки персональных данных из-за недобросовестных действий сотрудников, им может быть предусмотрена административная ответственность по статье 13.14.1. «Незаконное получение информации с ограниченным доступом» КоАП РФ или уголовная ответственность в зависимости от характера нарушения и уровня ущерба, нанесенного лицам, чьи данные были разглашены. Кроме того, сотрудники могут быть подвергнуты дисциплинарным мерам со стороны своего работодателя. Важно соблюдать законодательные требования обработки персональных данных для предотвращения возможных нарушений [3].

При получении информации из ботов и использовании её в своих целях пользователи тоже нарушают закон. Нарушение вышеуказанных требований влечет за собой ответственность в соответствии со статьей 13.14 «Разглашение информации с ограниченным доступом» КоАП РФ. Они должны понимать серьезность последствий небрежного отношения к персональным данным [3].

Организации и разработчики таких ботов также несут существенную ответственность за защиту персональных данных пользователей. Они должны предпринимать все необходимые меры, чтобы обеспечить безопасность и конфиденциальность личной информации, хранящейся в их системах. В связи с этим, на основании статьи 10.3 Федерального закона №149-ФЗ от 27.07.2006 «Об информации, информационных технологиях и защите информации» оператор поисковой системы, распространяющий в сети "Интернет" информацию пользователя без его согласия, по требованию гражданина обязан прекратить выдачу сведений об указателе страницы сайта в сети интернет.

Таким образом, каждый пользователь поискового бота, в том числе упомянутого ранее Telegram-бота «Глаз Бога» имеет право отправить запрос на требование об удалении персональных данных из поисковых результатов.

Защита личной информации в интернете является важным аспектом в современном мире, так как они могут собирать и хранить персональные

данные пользователей, которые затем могут быть использованы в различных целях. Законодательством РФ предусмотрена ответственность в области защиты персональных данных и право пользователя самостоятельно обращаться к сервисам по удалению личной информации из баз данных поисковых систем.

Список использованных источников:

1. Официальный сайт сервиса "Глаз Бога" – URL: https://glazbog.ru/ (дата обращения: 05.03.2024).
2. "Уголовный кодекс Российской Федерации" от 13.06.1996 N 63-ФЗ (ред. от 14.02.2024). – URL: https: // www.consultant.ru/document/cons_doc_LAW_10699/4234a27af714cc608ea71b7bae9400f3613c8f60/ (дата обращения: 05.03.2024).
3. "Кодекс Российской Федерации об административных правонарушениях" от 30.12.2001 N 195-ФЗ (ред. от 25.12.2023) (с изм. и доп., вступ. в силу с 01.03.2024). – URL: https: // www.consultant.ru/document/cons_doc_LAW_34661/?ysclid=lucjytq6ts238571911 (дата обращения: 05.03.2024).

УДК 004

Ахмадиева Вилена Ф., Ахмадиева Виола Ф.
Уфимский университет
науки и технологий, Уфа, Россия

Научный руководитель:
Р.М. Яппаров
Уфимский университет
науки и технологий, Уфа, Россия

ЛИЦЕНЗИРОВАНИЕ ДЕЯТЕЛЬНОСТИ ПО ТЕХНИЧЕСКОЙ ЗАЩИТЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ
LICENSING OF ACTIVITIES ON TECHNICAL PROTECTION OF CONFIDENTIAL INFORMATION

Аннотация: В данной статье рассматриваются актуальные вопросы, связанные с развитием информационных технологий и защитой конфиденциальной информации. Лицензирование деятельности по технической защите конфиденциальной информации выступает ключевым инструментом обеспечения безопасности информации, именно его основные концепции будут рассмотрены нами в представленной статье.

Abstract: This article deals with topical issues related to the development of information technologies and protection of confidential information. Licensing of activities on technical protection of confidential information is a key tool for ensuring information security, and it is its basic concepts that will be considered in this article.

Ключевые слова: Лицензирование, конфиденциальная информация, информационная безопасность, лицензиат, законодательство, неправомерное вмешательство, электронные средства.

Keywords: Licensing, confidential information, information security, licensee, legislation, tampering, electronic media.

В индустриальном обществе быстрыми темпами набирает обороты развитие технологий и расширяется сфера применения электронных средств в качестве способа обмена информацией, растёт актуальность вопросов по защите конфиденциальной информации [4]. Лицензирование деятельности по технической защите конфиденциальной информации выступает ключевым инструментом обеспечения безопасности информации. Лицензирование и его основные концепции будут рассмотрены нами в представленной статье.

Лицензирование деятельности по технической защите конфиденциальной информации — это процедура, предусматривающая выдачу специального разрешения на осуществление определенных видов деятельности, которая направлена на обеспечение защиты конфиденциальной информации от неправомерного доступа, использования и распространения [1].

Согласно законодательству, такая лицензия выдается Федеральной службой по техническому и экспортному контролю, выполняющей функции контроля за соблюдением правил, установленных законодательством, в части обеспечения безопасности конфиденциальной информации с ограниченным доступом [2].

Важнейшим элементом концепции являются строгие требования, предъявляемые к лицензиату. Законодательство содержит определенные условия, которым необходимо удовлетворять в случае наличия лицензии на защиту конфиденциальной информации. Эти требования могут характеризоваться наличием трудового стажа и специального образования в сфере безопасности информации, наличием необходимого оборудования и соблюдением соответствующих стандартов и нормативов в сфере защиты информации. Для того чтобы получить лицензию на осуществление деятельности по технической защите информации, специалисты должны пройти соответствующее обучение и получить сертификаты, подтверждающие их квалификацию и уровень знаний.

Подача заявки на лицензирование, предоставление требуемых документов и данных о соответствии установленным требованиям, прохождение проверок со стороны компетентных органов, а также погашение соответствующих государственных налогов – это основные шаги, входящие в процедуру получения лицензии на деятельность по технической защите конфиденциальной информации. Лицензиат обязан соблюдать все требования, установленные законодательством, в отношении использования данной лицензии, и регулярно проходить проверки, проводимые контролирующими органами. Техническая защита конфиденциальной информации должна постоянно совершенствоваться, принимая во внимание возможные новые угрозы и уязвимости, а также изменения в законодательстве и стандартах. Возможно продление или обновление лицензии на деятельность по технической защите конфиденциальной информации при соблюдении всех необходимых условий и требований.

Одной из ключевых концепций является ответственность. За нарушение условий лицензии могут предусматриваться различные виды ответственности, включая штрафы, административные или уголовные наказания.

Эти концепции помогают обеспечить высокий уровень защиты конфиденциальной информации и эффективное функционирование системы лицензирования в данной области. Лицензирование технической защиты конфиденциальной информации играет важную роль в поддержке защищенности информации и безопасности интересов государства, бизнеса и граждан. Беспрекословное следование процедурам лицензирования позволяет создать эффективную систему безопасности конфиденциальной информации и предотвратить утечки и незаконное использование различных сведений [3].

Список использованных источников:

1. Шахалов Игорь Юрьевич Лицензирование деятельности по технической защите конфиденциальной информации // Вопросы кибербезопасности. 2013. №1. – URL: https://cyberleninka.ru/article/n/litsenzirovanie-deyatelnosti-po-tehnicheskoy-zaschite-konfidentsialnoy-informatsii (дата обращения: 07.11.2023).

2. Постановление от 3 февраля 2012 г. N 79 "О лицензировании деятельности по технической защите конфиденциальной информации" (с изменениями и дополнениями). – URL: https://base.garant.ru/70136258/?ysclid=loo6yhdtic71033358 (дата обращения: 07.11.2023).

3. Иванов Андрей Евграфович, Спрогис Иван Александрович, Шахалов Игорь Юрьевич особенности лицензирования деятельности

предприятий и организаций в интересах министерства обороны российской федерации // вопросы кибербезопасности. 2021. № 5 (45). – URL: https://cyberleninka.ru/article/n/osobennosti-litsenzirovaniya-deyatelnosti-predpriyatiy-i-organizatsiy-v-interesah-ministerstva-oborony-rossiyskoy-federatsii (дата обращения: 07.11.2023).

4. Яппаров, Р.М. Роль и значение автоматизированных информационных систем в правоохранительной деятельности / Р.М. Яппаров // Информационные технологии обеспечения комплексной безопасности в цифровом обществе: сборник материалов V Всероссийской молодежной научно-практической конференции, Уфа, 20–21 мая 2022 года. – Уфа: Башкирский государственный университет, 2022. – С. 48-53. – DOI 10.33184/itokbco-2022-05-20.12.

УДК 34.05

А.И. Зыков
Уфимский университет
науки и технологий, Уфа, Россия

Научный руководитель:
Р.М. Яппаров
Уфимский университет
науки и технологий, Уфа, Россия

АНАЛИЗ ПРАВОВЫХ НОРМ РОССИИ И ЗАРУБЕЖНЫХ СТРАН В ОБЛАСТИ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ
ANALYSIS OF THE LEGAL NORMS OF RUSSIA AND FOREIGN COUNTRIES IN THE FIELD OF PERSONAL DATA PROTECTION

Аннотация: В данной статье проанализированы требования Общего регламента по защите данных Европейского союза и Закона Калифорнии о защите персональных данных потребителей», выявлена актуальность применения указанных регламентов в российской практике. Методология работы основана на сравнительном анализе GDPR, CCPA и Федерального закона № 152 «О персональных данных», благодаря чему были сделаны выводы об общих чертах и различиях основных положений.

Abstract: In this article it is analyzed the requirements of the General Data Protection Regulation of the European Union and the California Consumer Privacy Act and it reveals the relevance of the application of these regulations in

the Russian practice. The methodology of work is based on comparative analysis of GDPR, CCPA and Federal Law № 152 «On Personal Data», which resulted in conclusions about the general features and differences of the main provisions.

Ключевые слова: Персональные данные, защита данных, GDPR, CCPA, информационная безопасность.

Keywords: Personal data, data protection, GDPR, CCPA, information security.

Каждая страна регламентирует защиту персональных данных своими законами. В России – это Федеральный закон № 152-ФЗ «О персональных данных» от 27.07.2006, в Европе — «Общий регламент защиты персональных данных» (GDPR). В США же нет единого НПА в области защиты ПДн. Самым полным в США НПА считается «Закон Калифорнии о защите персональных данных потребителей» (CCPA).

В российском законодательстве термин «персональные данные» определяется следующим образом: «Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)» [1]. В федеральном законе отсутствует конкретный перечень сведений, отнесенных к персональным данным. В GDPR персональные данные — это любая информация, относящаяся к «субъекту данных», то есть идентифицированному или поддающемуся идентификации физическому лицу [2]. Здесь также отсутствует определенный перечень персональных данных, причем законодательство расширяет область ПДн даже больше, чем 152-ФЗ. Согласно GDPR, к персональным данным относится даже закодированная (анонимная) информация, если она может быть связана с физическим лицом. В CCPA говорится следующее: «Персональная информация означает информацию, которая идентифицирует, касается, описывает, разумно может быть связана с конкретным потребителем или домохозяйством или может разумно быть связана, прямо или косвенно, с ними» [3]. В отличие от двух предыдущих, в Калифорнийском законе есть примерный перечень, что относится к персональным данным: настоящее имя, псевдоним, биометрические данные, геопозиция и т.д.

В РФ уполномоченным органом в области ПДн является Роскомнадзор, в Европе – надзорные органы каждой страны, входящей в ЕС, в Калифорнии – прокурор штата.

Деятельность операторов ПДн в РФ могут осуществлять как государственные и муниципальные органы, так и физические и юридические лица. Операторы обязаны обрабатывать ПДн только тех лиц, которые находятся на территории РФ, при этом неважно, из какой страны будет оператор. Чтобы иметь возможность обрабатывать персональные данные, оператор должен быть зарегистрирован в специальном реестре

Роскомнадзора и хранить сведения в базах данных на территории РФ, иначе придется платить штраф (в 2020 году Facebook за такое нарушение выплатила штраф в 4 млн рублей). В Европе операторами выступают такие же органы и лица, а сами данные должны храниться на европейских серверах. Однако операторам не нужно регистрироваться в надзорных органах, а также операторам необходимо отстаивать права своих клиентов даже тогда, когда люди находятся не на территории ЕС. Калифорнийский закон применим к компаниям, работающим в Калифорнии, если они ежегодно соответствуют хотя бы одному из следующих критериев: годовая выручка более 25 млн долларов; более 50% дохода – от продажи личных данных клиентов; покупка, продажа или предоставление доступа к данным более 50 тыс. потребителей.

По российскому законодательству, чтобы получить согласие на обработку ПДн, необходимо поставить подпись (если согласие в бумажном варианте), либо просто галочку в окошке (если согласие в электронном виде), при этом в согласии должна быть прописана сама политика обработки ПДн организации, либо дана ссылка на нее, поскольку политика обработки ПДн – документ с открытым доступом [4]. Согласно ч. 4 ст. 9 152-ФЗ, необходимым является отдельное согласие с каждой целью обработки персональных данных. Согласие также должно быть явным, полным и добровольным, поэтому в электронной форме согласия запрещается установление включенного флажка по умолчанию. В этом плане Европейский GDPR аналогичен российскому. Можно добавить, что в Европейском законе также запрещаются формулировки с частицей «не» в согласии, т.к. это может ввести в заблуждение пользователя. Согласно CCPA, пользователи согласны на обработку персональных данных по умолчанию. При этом необходимым условием является возможность пользователей отозвать свое согласие в любое время. Следует отметить, что продажа данных подростков моложе 16 лет запрещена без их согласия.

В России оператор обязан предоставить пользователю информацию о нем, обновить или удалить данные, или отозвать согласие на обработку в течение 30 дней после запроса. Запрос можно отправлять не чаще одного раза в 30 дней. В Европе пользователи могут запросить данные в зашифрованном виде, а операторы могут не отвечать или требовать плату за слишком частые запросы. В Калифорнии оператор должен отвечать на запросы в течение 45 дней и не продавать ПДн по запросу пользователя, который может подать запрос онлайн или по электронной почте.

Штрафы за нарушения в области персональных данных различаются по регионам мира. В РФ юрлица могут быть оштрафованы до 75 тыс. рублей, а за хранение данных на серверах вне России – до 6 млн рублей за первое нарушение и до 18 млн рублей за повторное. В Европе штрафы до 10 млн евро или 2% годовой выручки за небольшие нарушения, и до

20 млн евро или 4% выручки за серьезные. В Калифорнии штраф до 2,5 тыс. долларов за непреднамеренные нарушения и 7,5 тыс. долларов за умышленные, плюс 750 долларов за каждого пострадавшего в случае утечки данных.

Все законы о защите персональных данных имеют свои особенности и сильные стороны. Российский 152-ФЗ схож с американским CCPA, но отличается более четкой категоризацией данных и меньшей вариативностью операторов. GDPR близок к ФЗ-152, но более строг к операторам. При разработке более полного НПА о защите данных следует учитывать все основные законы и выбирать самые полные и рациональные требования.

Список использованных источников:

1. Федеральный закон «О персональных данных» от 27.07.2006 N 152-ФЗ / [Электронный ресурс] // Правовой сервис «КонсультантПлюс»: [сайт]. – URL: https://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения: 25.02.2024).

2. Общий регламент защиты персональных данных (GDPR) Европейского союза / [Электронный ресурс] // Интерактивный справочник GDPR-TEXT.COM: [сайт]. – URL: https://gdpr-text.com/ru/ (дата обращения: 25.02.2024).

3. California Consumer Privacy Act of 2018 [1798.100 - 1798.199.100] / [Электронный ресурс] // California Legislative Information: [сайт]. – URL: https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=CIV&division=3.&title=1.81.5.&part=4.&chapter=&article= (дата обращения: 25.02.2024).

4. Яппаров, Р.М. Информационные технологии обеспечения комплексной безопасности в цифровом обществе / Р.М. Яппаров [Текст] // Сборник материалов V Всероссийской молодежной научно-практической конференции. – Уфа: БашГУ, 2022. – С. 48-53.

УДК 004

Д.А. Клияненко
Уфимский университет
науки и технологий, Уфа, Россия

Научный руководитель:
Р.М. Яппаров
Уфимский университет
науки и технологий, Уфа, Россия

УКРЕПЛЕНИЕ ЗАЩИТЫ ИНФОРМАЦИИ В ЗАКОНОДАТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ В ЭПОХУ ЦИФРОВИЦАЗИИ ОБЩЕСТВА
STRENGTHENING INFORMATION PROTECTION LEGISLATION IN THE RUSSIAN FEDERATION IN THE ERA OF SOCIETY DIGITALIZATION

Аннотация: В свете активной цифровизации и повышения зависимости общества от информационных технологий, обеспечение безопасности персональных данных и информационных систем становится вопиющей необходимостью. Настоящая статья посвящена анализу последних изменений и дополнений в законодательстве Российской Федерации, рассматривающих вопросы защиты информации на различных уровнях.

Abstract: Amidst the active digitalization and increasing dependence of society on information technologies, ensuring the security of personal data and information systems has become an imperative need. This article is dedicated to analyzing the latest amendments and additions to the legislation of the Russian Federation that address issues of information protection at various levels.

Ключевые слова: Информационная безопасность, законодательство, Российская Федерация, личные данные, киберугрозы, критическая информационная инфраструктура.

Keywords: Information security, legislation, Russian Federation, personal data, cyber threats, critical information infrastructure.

Современное общество переживает переход к информационной цивилизации, что сопровождается беспрецедентным увеличением объемов создаваемых, передаваемых и хранимых данных. В этой связи растет и объем угроз, связанных с несанкционированным доступом, порчей или потерей данных. РФ активно реагирует на данные вызовы путем постоянного совершенствования инструментария правовой защиты информации.

Изменения в Федеральном законе "О персональных данных" (152-ФЗ): Ужесточены требования к обработке персональных данных; введены новые ограничения для передачи данных в иностранные государства; усилены штрафные санкции за нарушение законодательства.

Федеральный закон "О безопасности критической информационной инфраструктуры Российской Федерации" (187-ФЗ): Закон направлен на защиту объектов критической информационной инфраструктуры (КИИ) от киберугроз. Вводится понятие "субъекты КИИ", на которых возложена ответственность за безопасность данных.

Изменения в Федеральном законе "О связи" (126-ФЗ): Акцентируется внимание на обеспечение безопасности передачи данных в сетях связи, введение требований по использованию отечественного оборудования и программного обеспечения для критической инфраструктуры.

Федеральный закон "О информации, информационных технологиях и о защите информации" (149-ФЗ): Вводятся изменения, учитывающие новые информационные технологии и угрозы, а также усиливающие контроль за распространением информации.

Стратегия информационного общества РФ: Обновление стратегии включает разработку мер по противодействию информационному терроризму, укреплению информационной культуры и повышению уровня информационной безопасности граждан.

Тенденция укрепления законодательства в области информационной безопасности РФ отражает глобальные цифровые вызовы и важность защиты данных в современных условиях. Проводимые государством меры направлены на создание эффективной системы противодействия киберугрозам, обеспечение конфиденциальности данных граждан и сохранения информационного суверенитета страны в условиях цифровой реальности. Каждое изменение законодательства предполагает необходимость его оперативной адаптации и использования на практике для обеспечения устойчивого и безопасного развития в информационной сфере.

Список использованных источников:

1. Федеральный закон от 07.07.2003 № 126-ФЗ (ред. от 07.07.2003) "О связи" (с изм. и доп., вступ. в силу с 01.07.2016) [Электронный ресурс] // КонсультантПлюс: справочно-правовая система. Режим доступа: https://www.consultant.ru/document/cons_doc_LAW_43224/ (дата обращения 19.04.2024). Текст: электронный.

2. Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 27.07.2006) "Об информации, информационных технологиях и о защите информации" (с изм. и доп., вступ. в силу с 28.07.2023) [Электронный ресурс] // КонсультантПлюс: справочно-правовая система. Режим доступа:

https://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения 19.04.2024).

3. Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 27.07.2006) "О персональных данных" (с изм. и доп., вступ. в силу с 06.02.2023) [Электронный ресурс] // КонсультантПлюс: справочно-правовая система. URL: https://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения 20.04.2024).

4. Федеральный закон от 26.07.2017 № 187-ФЗ (ред. от 26.07.2017) "О безопасности критической информационной инфраструктуры Российской Федерации" (с изм. и доп., вступ. в силу с 10.07.2023) [Электронный ресурс] // КонсультантПлюс: справочно-правовая система. URL: https://www.consultant.ru/document/cons_doc_LAW_220885/ (дата обращения 21.04.2024).

5. Указ Президента РФ от 09.05.2017 № 203 (ред. от 09.05.2017) "О Стратегии развития информационного общества в Российской Федерации на 2017 – 2030 годы" (с изм. и доп., вступ. в силу с 09.05.2017) [Электронный ресурс] // КонсультантПлюс: справочно-правовая система. URL: https://www.consultant.ru/document/cons_doc_LAW_216363/ (дата обращения 21.04.2024).

УДК 004.056

Р.С. Нуриев, А.В. Садыкова
Уфимский университет
науки и технологий, Уфа, Россия

Научный руководитель:
А.А. Корнилова
Уфимский университет
науки и технологий, Уфа, Россия

ПРОБЛЕМЫ МОДЕЛИРОВАНИЯ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
PROBLEMS OF MODELING INFORMATION SECURITY THREATS

Аннотация: На сегодняшний день информация выступает ценным ресурсом любой организации и имеет ряд обязательных условий для безопасного хранения, применения и передачи. Организации, ответственно относящиеся к информационным активам рано или поздно сталкиваются с вопросом проектирования или совершенствования

системы защиты информации. В вопросе построения актуальной системы защиты методическим нормативно-правовым актом выступает методика ФСТЭК моделирования угроз безопасности информации. В работе рассматриваются некоторые принципиальные вопросы разработки модели угроз безопасности информации.

Abstract: Today, information is a valuable resource for any organization and has a number of mandatory conditions for safe storage, use and transmission. Organizations that are responsible for information assets eventually face the issue of designing or improving an information security system. In the issue of building an up-to-date protection system, the methodological regulatory act is the FSTEC methodology for modeling information security threats. The paper discusses some fundamental issues of developing a model of information security threats.

Ключевые слова: Безопасность, моделирование угроз, актуальные угрозы, нарушители, потенциал, информационная система.

Keywords: Security, threat modeling, current threats, violators, potential, information system.

Сегодня многие компании сталкиваются с угрозами защиты интеллектуальной собственности и соответственно построением собственной системы защиты информации. Угрозы и риски информационной безопасности не так очевидны, как, например, финансовые угрозы, однако могут нести за собой еще больший ущерб для компании. Столкнувшись с требованиями законодательства или угрозой кибербезопасности в первую очередь необходимо определить какими механизмами и нормативно-правовыми актами стоит руководствоваться при построении системы защиты информации.

В первую очередь необходимо провести процедуру моделирования угроз информационной безопасности, основываясь на Методику оценки угроз безопасности информации ФСТЭК России, принятую 5 февраля 2021г. данный документ подразумевает экспертную методику построения системы защиты информации. Стоит отметить, что без моделирования угроз существуют риски создания неадекватной системы защиты информации в организации, которая будет либо недостаточной (не охватывает все существующие угрозы информационной безопасности организации), либо избыточной (охватывает не актуальные или несуществующие для организации угрозы).

Построение системы защиты должно опираться на модель угроз, которая в свою очередь должна помочь специалисту ответить на следующие вопросы: «Какие информационные активы необходимо защитить?», «От чего необходимо защищать информационные активы?» и «Какой существует потенциальный ущерб компании?».

Первый и последний вопрос относится к разделу «Оценка и анализ рисков» моделирования угроз информационной безопасности. С помощью оценки рисков специалист определяет информационные активы компании, оценивает их стоимость, степень потенциального ущерба и степень важности актива. Оценка стоимости информационных активов помогает руководству компании оценить потенциальную стоимость системы защиты информации. Данный факт связан с тем, что помимо защиты информации как таковой необходимо так же учитывать и финансовую составляющую, соотносить затраты на построение системы и стоимость информационного ресурса.

После того, как было определено что необходимо защищать и какой последует ущерб при отказе от внедрения системы защиты информации открытым остается вопрос от чего необходимо защищать информационные ресурсы. На данный вопрос поможет отметить модель угроз безопасности информации. Модель угроз в перовую очередь способствует определению актуальных угроз информационной безопасности организации, дает возможность построить эффективную систему защиты информации, отвечающую современным вызовам. Существует ряд информационных систем, для которых моделирование угроз обязательно:

– информационная система персональных данных;
– государственная информационная система;
– информационная система, относящаяся к критической информационной инфраструктуре.

В остальных случаях моделирование угроз производится добровольно.

В соответствии с методикой ФСТЭК от 05.02.2021г. определение актуальных угроз состоит из следующих этапов: определение негативных последствий; определение объектов последствий; оценка возможности реализации угроз и их актуальность. В методике разработано ранжирование злоумышленников в зависимости от потенциала их воздействия. Выделяют 2 группы нарушителей – внутренние и внешние. В каждой из групп выделяют подгруппы нарушителей с различным потенциалом. Данный факт связан с тем, что потенциал и возможности воздействия на информационную систему условного системного администратора или хакера гораздо выше уровня воздействия на систему рядового сотрудника организации.

Следующим этапом необходимо провести оценку актуальности угроз безопасности информации. Актуальной угроза считается если от ее реализации создается реальный ущерб информационным активам, определен актуальный нарушитель и выработан сценарий реализации

потенциальной угрозы. Наиболее трудоемким процессом на практике специалисты считают разработку сценариев реализации угроз.

В методике приведены примеры разработанных сценариев реализации угроз в графическом виде, однако составление графического представления реализации угроз значительно усложняет процесс моделирования угроз. Поэтому на практике гораздо чаще применяют табличную форму составления сценариев реализации угроз.

Подводя итог стоит отметить, что процесс разработки модели угроз безопасности информации достаточно трудоемкий, требует высокого уровня знаний в области защиты информации, но при изучении дополнительной информации, законодательства и практик ведущих специалистов под силу каждому специалисту. Однако большинство организаций предпочитает привлечение более опытных сторонних специалистов для объективной оценки существующей системы защиты информации. На рынке представлено большое количество компаний, занимающихся вопросом моделирования угроз безопасности информации и разработкой системы защиты информации под ключ, что в большинстве случаев более рационально и актуально.

Список использованных источников:

1. Барыбина, А.З. Моделирование угроз информационной безопасности сценарным подходом / А.З. Барыбина // Естественно-гуманитарные исследования. – 2022. – № 42(4). – С. 35-44.

2. Миняев, А.А. Моделирование угроз безопасности информации в территориально-распределенных информационных системах / А.А. Миняев // Наукоемкие технологии в космических исследованиях Земли. – 2021. – Т. 13, № 2. – С. 52-65. – DOI 10.36724/2409-5419-2021-13-2-52-65.

3. Сорокина, А.Е. Сравнительный анализ методов моделирования угроз информационной системы / А.Е. Сорокина // Информационные технологии в науке, бизнесе и образовании. Проблемы обеспечения цифрового суверенитета государства: Материалы XIII Международной научно-практической конференции студентов, аспирантов и молодых ученых, Москва, 26 ноября 2021 года / под общей редакцией А.М. Прохорова, А.В. Царегородцева. – Москва: Московский государственный лингвистический университет, 2022. – С. 92-97.

УДК 657.633.5

Е.В. Поляков, Т.Д. Ивлева
Уфимский университет
науки и технологий, Уфа, Россия

Научный руководитель:
Б.К. Кушубакова
Уфимский университет
науки и технологий, Уфа, Россия

ВНУТРЕННИЙ КОНТРОЛЬ ЗА ОБЕСПЕЧЕНИЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИЙ
INTERNAL CONTROL OVER THE INFORMATION SECURITY OF ORGANIZATIONS

Аннотация: В статье показано значение систематического внутреннего контроля организаций для обеспечения ее информационной безопасности. Также предложен ряд требований к организации внутреннего контроля, которые могут обеспечить защиту информации о деятельности хозяйствующих субъектов.

Abstract: The article shows the importance of systematic internal control of organizations to ensure its information security of organizations. A number of requirements for the organization of internal control are also proposed, which can ensure the protection of information about the activities of business entities

Ключевые слова: Контроль, внутренний контроль, информационная безопасность, организации.

Keywords: Control, internal control, information security, organizations.

В экономической системе каждый хозяйствующий субъект составляет его основное звено. Поэтому для обеспечения экономической безопасности на национальном уровне необходимо обеспечить экономическую безопасность каждой действующей организации.

В свою очередь, экономическая безопасность организации не может быть обеспечена без создания условий информационной безопасности и организации ее защиты. Особое значение информационная безопасность организаций приобретает на современном этапе, в условиях геополитических изменений и нестабильности международных экономических отношений.

Защита информации о деятельности организации имеет правовую

основу. В частности, персонал организации, выполняя те или иные функции и владея определенной информацией должен соблюдать положения федерального закона «О коммерческой тайне» №98-ФЗ от 29.07.2004 г.

Организации обязаны создавать внутренние локальные акты, положения которого должны конкретизировать нормы данного закона, чтобы обеспечить в полном объеме защиту информации о деятельности организации.

Соблюдение нормативных положений по обеспечению защиты информации о деятельности организации напрямую зависит от системы и механизмов внутреннего контроля организации.

Внутренний контроль представляет собой набор действий, спланированных руководством организации и осуществляемых внутри нее с целью обеспечения наилучшего выполнения своих обязанностей всеми сотрудниками в процессе хозяйственной деятельности. Основной задачей внутреннего контроля является проверка законности и экономической целесообразности проводимых операций для успешной и безопасной деятельности организации.

Важным аспектом внутреннего контроля является обеспечение информационной безопасности. В современном быстро меняющимся мире, когда информация является одним из самых ценных и важных активов организации, защита ее от утечек, несанкционированного доступа и кибератак становится приоритетной задачей.

Постановка внутреннего контроля в организациях на современном этапе в целом не полной мере отвечает потребностям безопасной деятельности. Для обеспечения защиты информации организации о ее деятельности внутренний контроль должен соответствовать следующим требованиям (см. табл.1)

Таблица 1 – Требования к внутреннему контролю организаций для обеспечения ее информационной безопасности

Требование	Влияние на обеспечение защиты информации
1. Создание упреждающих мер контроля для минимизации влияния угроз и рисков	Создание упреждающих мер контроля позволит организации идентифицировать потенциальные угрозы и риски заранее, что поможет принять необходимые меры для предотвращения, инцидентов, благодаря заранее разработанным алгоритмам действий и процедурам, с помощью которых, организация сможет быстро и эффективно среагировать на угрозы, минимизировать тем самым или нейтрализуя возможные потери.

Продолжение таблицы 1

2. Контроль доступа к данным	Позволит ограничить доступ к конфиденциальным данным, доступным только для пользователей с специальным разрешением, что предотвратит несанкционированный доступ к информации и ее дальнейшую утечку. Выполнение данного требования существенно снизит риск утраты важной информации и последующее негативное влияние на результаты деятельности.
3. Оперативный мониторинг и аудит информационных систем	Проведение оперативного мониторинга и аудита информационных систем направлен на точечное обнаружение уязвимых мест в системе, ее слабых точек в структуре защиты и потенциальные риски для безопасности данных. Мониторинг и аудит позволяет также принимать превентивные меры по устранению уязвимостей и разрабатывать дальнейшие улучшения для защиты информации.
4. Оперативное реагирование на инциденты	Данное требование направленно на то, чтобы минимизировать ущерб и последствия инцидента, предотвращая дальнейшее распространение угроз и защищая информацию от утечки или повреждения, а также способствует быстрому восстановлению работоспособности информационных систем и процессов после нарушения целостности и безопасности системы.
5. Повышение эффективности бизнес-процессов	Внутренний контроль позволит оптимизировать производственный процесс путем сокращения простоев оборудования, повышения производительности оборудования с помощью автоматизированных технологий, отслеживания в реальном времени производственного цикла, выявлять неэффективные операции, «мониторить» добросовестность выполнения обязанностей сотрудниками предприятия. [1, с. 455]
6. Исключение влияния человеческого фактора на результат	Одним из основных недостатков является человеческий фактор. Независимо от того, насколько хорошо разработаны политики и процедуры безопасности, ошибки и недосмотр со стороны сотрудников могут привести к компрометации информации.
7. Оптимизация затрат на проверочные мероприятия	Внедрение и поддержание системы внутреннего контроля в области информационной безопасности требует крупных финансовых и производственных затрат. Некоторые организации могут столкнуться с проблемой нехватки нужных ресурсов для реализации всех необходимых мер обеспечения безопасности.
8. Обеспечение чувствительности механизмов контроля к ошибкам	Ошибки в процессе реализации внутреннего контроля могут создать серьезную угрозу информационной безопасности организации и повлиять на результат ее деятельности. Некорректно настроенные системы, недостаточное обучение персонала или некачественный мониторинг могут стать причиной образования уязвимостей и угроз внутри организации.

В современной экономической системе важно понимать, что каждая

действующая организация играет ключевую роль в обеспечении экономической безопасности на национальном уровне. Для достижения этой цели необходимо обеспечить надежную информационную безопасность каждой организации, так как она является неотъемлемой частью общей экономической безопасности.

Внутренний контроль в данном контексте играет значительную роль в обеспечении информационной безопасности организации при условии выполнении приведенных выше требований к ее организации.

Таким образом, внутренний контроль, в части обеспечения информационной безопасности, играет ключевую роль в поддержании стабильности и защиты интересов организации в условиях современного бизнес-окружения. А внедрение эффективных мер и стратегий обеспечения внутреннего контроля поможет не только укрепить позиции компании на рынке, увеличив конкурентоспособность, но и обеспечить ее устойчивое развитие в будущем.

Список использованных источников:

1. Федеральный закон "О коммерческой тайне" от 29.07.2004 N 98-ФЗ – URL: https://www.consultant.ru/document/cons_doc_LAW_48699/ (дата обращения 27.04.2024). – Текст: электронный.

2. Хулхачиева Г.Д. Развитие внутреннего контроля в условиях цифровизации экономики / Текст: электронный // Индустриальная экономика. – 2021. – № 5. – URL: https://cyberleninka.ru/article/n/razvitie-vnutrennego-kontrolya-v-usloviyah-tsifrovizatsii-ekonomiki (дата обращения: 27.04.2024).

УДК 004.056.53

Э.К. Сагилова
Уральский федеральный университет имени первого Президента России Б.Н. Ельцина, Екатеринбург, Россия

А.А. Христолюбова
Уральский федеральный университет имени первого Президента России Б.Н. Ельцина, Екатеринбург, Россия

О ВЫЯВЛЕНИИ КРИТИЧЕСКИХ ПРОЦЕССОВ У ОРГАНИЗАЦИЙ, ЯВЛЯЮЩИХСЯ СУБЪЕКТАМИ КИИ
IDENTIFICATION OF CII FACILITIES IN THE FIELD OF DEFENSE INDUSTRY

Аннотация: В статье рассматривается проблематика выявления критических процессов в организациях в ходе исполнения требований

Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». Основываясь на результатах анализа методик идентификации и управления рисками, правового анализа требований законодательства сформирован повторяемый и измеряемый подход определение критичности процессов организации-субъекта КИИ.

Abstract: In the article, the solution to the problem determines the consequences of processes in organizations when fulfilling the requirements of the Federal Law of July 26, 2017 No. 187-FZ “On the security of critical information activities of the Russian Federation.” On solving the problem of determining methods of analysis and risk management, legal analysis of the requirements established by law, a repeating and research approach to determining the criticality of the processes of the organization-subject of CII.

Ключевые слова: Критическая информационная инфраструктура, субъект КИИ, управление рисками, процессный подход.

Keywords: Critical information infrastructure, CII subject, risk management, process approach.

Критический процесс является одним из ключевых терминов законодательства о безопасности КИИ, наравне с такими понятиями как субъект и объект КИИ. И от правильной интерпретации данного термина напрямую зависит формирование перечня объектов КИИ и как следствие последующие результаты категорирования [5].

Выявление критических процессов у субъекта КИИ представляет собой важную задачу в процессе категорирования, поскольку это позволяет определить наиболее уязвимые компоненты информационной системы. Этот процесс необходим для эффективного управления рисками и разработки стратегий защиты от потенциальных угроз. Идентификация критических процессов также способствует оптимизации распределения ресурсов и обеспечению непрерывности работы организации в условиях возможных компьютерных инцидентов.

Согласно п. 5б Постановления Правительства №127 [2] категорирование включает в себя выявление управленческих, технологических, производственных, финансово-экономических и (или) иных процессов в рамках выполнения функций (полномочий) или осуществления видов деятельности субъектов критической информационной инфраструктуры, нарушение и (или) прекращение которых может привести к негативным социальным, политическим, экономическим, экологическим последствиям, последствиям для обеспечения обороны страны, безопасности государства и правопорядка (далее - критические процессы).

С целью оценки критичности основных и вспомогательных процессов в данном исследовании используется методика оценивания, основанная на принципах количественного анализа воздействия каждого процесса на результат создания основной ценности. Методика подразумевает использование шкалы оценивания, которая включает в себя параметры времени, объема и качества продукции, с целью определения степени влияния каждого процесса на эффективность и результативность производственного процесса (выполнения плана производства). Используемая методика оценивания критичности процессов производства позволяет проводить оценку объективно и систематически. Шкала оценивания позволяет выразить уровень влияния каждого процесса на ключевые аспекты производства, учитывая их диапазон влияния от минимального до максимального в следующих границах:

0-20%, низкий уровень влияния: процессы, которые оказывают минимальное воздействие;

21-50%, умеренный уровень влияния: процессы, которые могут вносить изменения, но не имеют критического значения;

51-100% высокий уровень влияния: критически важные процессы, существенно влияющие на результативность и качество производства.

При реализации корректирующих мер вероятность реализации информационных рисков, связанных с компьютерными инцидентами, будет находиться на приемлемом уровне для риск-аппетита в отношении невозможности выполнения договорных обязательств организации в срок. Риск-аппетит определяется исходя из возможных численных значений длительности и объемов выполнения государственного контракта, а также с учетом времени восстановления выполнения критических процессов при применении корректирующих воздействий. Полученные значения оценки риска позволяют предположить численную оценку риск-аппетита Общества в части информационных рисков на уровне 200.

Таблица 1 – Качественные формулировки шкалы оценивания критичности процессов производства

Критерий оценивания		
Время	Качество	Объем
0-20%: Минимальное влияние на общее время производства.	0-20%: Минимальное влияние на качество, незначительные отклонения от стандартов.	0-20%: Незначительное влияние на объем производства.
21-50%: Умеренное влияние на время, может вызвать небольшие задержки.	21-50%: Умеренное влияние на качество, изменения могут влиять	21-50%: Умеренное влияние на объем, может немного изменить производственные показатели.

	на соответствие стандартам.	
51-100%: Сильное влияние на время, любая задержка здесь негативно отразится на всем производственном цикле.	51-100%: Сильное влияние на качество, любые изменения здесь существенно влияют на конечный продукт.	51-100%: Значительное влияние на объем, изменения здесь могут сильно повлиять на общий объем выпускаемой продукции.

Оценка критичности процессов проводится с использованием научных методов и инструментов, таких как анализ данных, моделирование и статистические методы.

Таким образом, основываясь на результатах анализа методик идентификации и управления рисками, правового анализа требований законодательства данный подход является повторяемым и измеряемым, что помогает определению критичности процессов организации-субъекта КИИ и способствует более точному обоснованию позицию комиссии перед регулятором с научной точки зрения.

Список использованных источников:

1. Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

2. Постановление Правительства от 8 февраля 2018 г. № 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».

3. Приказ ФСТЭК России от 25 декабря 2017 г. № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».

4. Указ Президента Российской Федерации от 1 мая 2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации».

5. Интернет ресурс «Критический процесс и его роль в процессе категорирования объектов КИИ» – URL: https: // www.securitylab.ru/blog/personal/plutsik/344890.php?ysclid=lweterzr8270921 5062 (дата обращения: 27.04.2024).

6. Сагилова, Э.К. Моделирование бизнес-процессов мониторинга субъекта критической информационной инфраструктуры / Э.К. Сагилова, А.А. Христолюбова // Весенние дни науки: сборник докладов международной конференции студентов и молодых ученых, Екатеринбург, 20–22 апреля 2023 года. – Екатеринбург: ООО Издательский Дом "Ажур", 2023. – С. 90-94.

УДК 004.056

А.А. Фаизов
Уфимский университет
науки и технологий, Уфа, Россия

Научный руководитель:
Н.Г. Миронова
Уфимский университет
науки и технологий, Уфа, Россия

ПЕРСОНАЛЬНЫЕ ДАННЫЕ КАК КАТЕГОРИЯ СВЕДЕНИЙ КОНФИДЕНЦИАЛЬНОГО ХАРАКТЕРА
PERSONAL DATA AS A CATEGORY OF CONFIDENTIAL INFORMATION

Аннотация: В статье даётся полное определение персональных данных. На основе анализа достоверных научных источников определяются категории персональных данных. Приводятся аргументы в пользу необходимости защиты персональных данных. Даётся полное заключение, основанное на выводах авторов статьи по теме персональных данных в рамках рассмотрения его как категории сведений конфиденциального характера.

Abstract: The article provides a complete definition of personal data. Based on the analysis of reliable scientific sources, the categories of personal data are determined. Arguments are given in favor of the need to protect personal data. A complete conclusion is given based on the conclusions of the authors of the article on the topic of personal data in the framework of considering it as a category of confidential information.

Ключевые слова: Персональные данные, информационная безопасность, конфиденциальность, интернет.

Keywords: Personal data, information security, privacy, Internet.

Персональные данные – это любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных). Они являются ценным активом в цифровую эпоху, но также и уязвимым объектом, требующим защиты.

В работе использованы возможности программы Microsoft Office Word. Использованы научные труды [1], [2].

Описаны категории персональных данных: идентификационные, контактные, финансовые, медицинские, биометрические, данные о местоположении и онлайн-активности. Риск дискриминации, репутационные и финансовые потери являются наибольшим риском в

вопросе хранения и передачи персональных данных. Выявлены существующие положения в законах о защите персональных данных и методы для защиты своих данных, заключающиеся в шифровании и аутентификации.

Существует ряд принципиальных категорий персональных данных [1]:

– Идентификационные данные: ФИО, дата рождения, адрес, паспортные данные, ИНН и т.д.

– Контактные данные: Телефон, адрес электронной почты, адрес проживания и т.д.

– Финансовые данные: Банковские реквизиты, данные о доходах и расходах, кредитная история и т.д.

– Биометрические данные: Отпечатки пальцев, распознавание лица, ДНК и т.д.

– Данные о местоположении: Геолокация, данные GPS, информация о передвижениях и т.д.

– Онлайн-активность: История посещений сайтов, поисковые запросы, данные о взаимодействии с социальными сетями и т.д.

Почему персональные данные нуждаются в защите – один из основных вопросов данной статьи. Риск дискриминации: Неправомерное использование персональных данных может привести к дискриминации по различным признакам. Финансовые потери: Утечка данных может привести к краже личных средств, мошенничеству и другим финансовым потерям. Репутационный ущерб: Распространение личной информации может нанести ущерб репутации и вызвать социальные проблемы.

Методы защиты персональных данных:

– Шифрование: Шифрование данных делает их нечитаемыми для неавторизованных лиц.

– Аутентификация: Использование паролей, двухфакторной аутентификации и других методов для обеспечения доступа к данным только для авторизированных пользователей (если речь идет о защите данных в сети Интернет).

– Контроль доступа: Ограничение доступа к персональным данным только для тех, кому это необходимо для выполнения служебных обязанностей. [2]

– Обучение сотрудников: Обучение сотрудников правилам обработки персональных данных и мерам безопасности.

Защита персональных данных – это общая ответственность. Организации и государство должны создавать эффективные механизмы защиты, а каждый человек должен быть осознанным и ответственным при обращении со своей личной информацией.

Список использованных источников:

1. Буянов Д.С. Информационная безопасность в интернете // Молодой ученый. 2017. № 36.
2. Экштайн К. Основные права и свободы: учеб. пос. для вузов. – М.: NOTA BENE. 2004.

УДК 004

Г.Ф. Хаматова
Нефтекамский филиал
Уфимского университета, Нефтекамск, Россия

Научный руководитель:
Н.Г. Миронова
Уфимский университет
науки и технологий, Уфа, Россия

О ЗАЩИТЕ IT-ИНФРАСТРУКТУРЫ УЧРЕЖДЕНИЙ ЗДРАВООХРАНЕНИЯ
ON THE PROTECTION OF HEALTHCARE ORGANIZATIONS

Аннотация: В статье изложены предложения по усовершенствованию защиты информации в учреждениях здравоохранения.

Abstract: The article outlines proposals for improving information security in healthcare institutions.

Ключевые слова: Кибербезопасность, здравоохранение.

Keywords: Cybersecurity, healthcare.

Информационные технологии (и проблемы, с ними связанные) стали неотъемлемой частью работы учреждений здравоохранения, отрасль переживает цифровую трансформацию по нескольким направлениям (растет уровень цифровизации мед.документооборота, складывается телемедицина; растет сложность информационной инфраструктуры и ИС отрасли). По оценке Positive Technologies, в 58% случаев в результате целевых атак на учреждения государственной власти, здравоохранения и др. происходят утечки конфиденциальной информации, в 41% таких атак нарушается работа деятельности организации; в последние годы на медучреждения участились атаки с применением вирусов-вымогателей. Важна разработка специальных нормативно-правовых актов, которые бы

помогали регламентировать защиту информации для учреждений здравоохранения, которые относятся в объектам критической инфраструктуры.

Минздрав России разработал Концепцию информационной безопасности в сфере здравоохранения, в которой, в частности, отмечено [1 - С. 16-17], что в ГИС здравоохранения используется недоверенное ПО, аудит и анализ защищенности носит в учреждениях отрасли нерегулярный характер; специалистов по ИБ недостаточно; средства защиты применяются фрагментарно и несистемно, их архитектура «разнородна»; безопасность ИС в учреждениях здравоохранения не всегда подтверждена. Среди проблем, с которыми сталкиваются медицинские учреждения после ужесточения санкций – отказ иностранных разработчиков ПО для мед.аппаратуры и цифрового медицинского оборудования от поддержки российских потребителей; быстрый переход на российские аналоги затруднен (например, из-за проблем совместимости операционных системы российской разработки с там оборудованием и приложениями); недостаточная или плохо исследованная совместимость к тому же порождает неочевидные уязвимости в работе ИС. Угрозы, актуальные для учреждений здравоохранения, перечислены в приказе Министерства здравоохранения от 3 июля 2023 г. № 340н [2] (угрозы утечки, НСД, угрозы воздействия на программные и аппаратные компоненты). Защите подлежат врачебные записи в цифровом формате, обрабатываемые в медицинских ГИС, информация ограниченного доступа органов власти, ПДн и врачебная тайна; иное. Проблемы безопасности цифровой медицины усугубляются тем, что медоборудование и ПО создавалось без особого учета требований к защите информации. Для защиты информационной инфраструктуры учреждения здравоохранения уже рекомендуется [3] (н на практике не всегда может быть реализовано по ряду причин) комплекс мер безопасности, в т.ч.: криптографическая защита медицинской информации (в т.ч. перс. данных, критичных и учетных данных) при хранении и передаче по сетям информации, многоуровневую защиту и механизмы контроля доступа к информации; регулярное обновление антивирусного и антихакерского программного обеспечения для предотвращения вредоносных атак; защита сетей передачи данных между компонентами ГИС; регулярные аудиты состояния безопасности информационной инфраструктуры для выявления уязвимостей и устранения их; разработка плана реагирования на инциденты, плана резервного копирования данных; обучение сотрудников учреждений здравоохранения правилам безопасности информации и проч.

Помимо перечисленных традиционных направлений защиты информации, могут быть такие предложены (возможно, в порядке регламента деятельности по ИБ) следующие усовершенствования защиты

учреждений здравоохранения: должна быть создана ведомственная структура при министерстве здравоохранения или при Минцифры, которая бы помогала учреждениями здравоохранения исследовать указанные уязвимости, а также рекомендовала проверенные и совместимые компоненты медицинской IT-инфраструктуры. В 2022 г. был создан Центр информационной безопасности и импортозамещения программного обеспечения на базе ФГБУ «ЦНИИОИЗ», который может участвовать в этой работе. Актуальна, на наш взгляд, разработка некой «типовой» для медучреждений политики информационной безопасности, на базе которой ведомственные учреждения могли бы адаптировать политику ИБ к своим обстоятельствам. Важно более тесное сотрудничество с органами кибербезопасности для двустороннего обмена информацией о потенциальных угрозах для раннего обнаружения и пресечения кибератак.

Список использованных источников:

1. Концепция информационной безопасности в сфере здравоохранения (от 10 марта 2022) – URL: https://minzdrav.gov.ru/news/2022/06/22/18919-minzdrav-rossii-razrabotal-kontseptsiyu-informatsionnoy-bezopasnosti-v-sfere-zdravoohraneniya (дата обращения: 25.04.2024).

2. Приказ Министерства здравоохранения РФ от 3 июля 2023 г. № 340н «Об определении угроз безопасности ПДн … в ИСПДн, эксплуатируемых в сферах деятельности, нормативно-правовое регулирование которых осуществляется Министерством здравоохранения РФ».

3. Приказ Министерства здравоохранения РФ от 24 декабря 2018 г. № 911н «Об утверждении Требований к государственным информационным системам в сфере здравоохранения субъектов РФ, медицинским информационным системам медицинских организаций и информационным системам фармацевтических организаций».

УДК 004

А.Р. Хусаинова
Уфимский университет
науки и технологий, Уфа, Россия

Научный руководитель:
Р.М. Яппаров
Уфимский университет
науки и технологий, Уфа, Россия

РАЗРАБОТКА МЕТОДОВ И ФОРМ РАБОТЫ С ПЕРСОНАЛОМ ОРГАНИЗАЦИИ, ДОПУЩЕННЫМ К КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ
DEVELOPMENT OF METHODS AND FORMS OF WORK WITH THE PERSONNEL OF THE ORGANIZATION ADMITTED TO CONFIDENTIAL INFORMATION

Аннотация: В статье раскрыты особенности защиты конфиденциальной информации. Описаны вопросы разработки методов и форм работы с персоналом организации, допущенным к конфиденциальной информации.

Abstract: The article reveals the features of protecting confidential information. The issues of developing methods and forms of work with the organization's personnel admitted to confidential information are described.

Ключевые слова: Конфиденциальная информация, защита информации, информационная безопасность, персонал, организационная защита информации.

Keywords: Confidential information, information protection, information security, personnel, organizational information protection.

Для предприятия в настоящее время очень актуальны вопросы работы с персоналом, допущенным к конфиденциальной информации. Конфиденциальная информация должна быть защищенной, чтобы утечка или другие мошеннические действия не могли привести к критическим последствиям для работы организации.

В ходе работы персонал получает, обрабатывает и хранит огромные массивы информации, в т.ч. и конфиденциальную информацию (например, коммерческую тайну или персональные данные), которая охраняется законом и может нанести как репутационный, так и финансовый ущерб для организации и самих сотрудников.

Стоит отметить, что уровень защиты информации напрямую зависит от того, какую ценность он предоставляет для организации и какой ущерб

может понести организация в случае несанкционированного доступа или утечки. Только при комплексной системе защиты, состоящей из организационных, правовых, технических мер, уровень защиты информации будет на соответствующем уровне и включать в различные средства защиты информации, меры и методы. Они могут позволить существенно уменьшить количество уязвимостей информационной безопасности.

Персонал – это начало и основа системы защиты конфиденциальной информации в любой организации. Поэтому так важно подобрать меры и методы работы с персоналом организации, допущенным к конфиденциальной информации. А организационные меры по защите стали приоритетными в организации. Именно сотрудники являются одними из главных распространителей конфиденциальной информации.

Доступ к конфиденциальной информации подразумевает под собой получение определенных сведений с учетом должностных обязанностей с разрешения руководителя.

Как было отмечено ранее, одно из важных мест в решении вопросов информационной безопасности занимает выбор методов работы с сотрудниками, допущенными к конфиденциальной информации. Основными методами по контролю качества работы и повышению уровня профессиональных знаний сотрудников является:

– регулярная аттестация персонала;

– регулярные проверки на соблюдение требований информационной безопасности;

– составление отчетов по работе сотрудников и состояния защищенности информации;

– самоконтроль сотрудников.

Также основными условиями для доступа к конфиденциальной информации являются:

– проведение инструктажей по работе с конфиденциальной информации;

– подписание персоналом соглашений о неразглашение конфиденциальной информации;

– ознакомление с ответственностью за разглашение конфиденциальной информации;

– наличие и ознакомление с должностными обязанностями работника, которые определяют объем разрешенной к пользованию информации в соответствии с кругом выполняемых задач и др.

Сотрудники должны строго соблюдать все требования по обращению с конфиденциальной информации в процессе всей работы, а также после увольнения с занимаемой должности. За нарушение данных требований в отношении сотрудника может быть применены меры ответственности.

Основная цель ограничения доступа, внедрения мер и форм работы с персоналом, допущенным к конфиденциальной информации, - это исключение и минимизация нанесения ущерба компании в случае разглашения конфиденциальных данных или утечки информации.

Стоит отметить, что контроль за действиями персонала может быть усилен путем внедрения специальных технических средств. Рынок систем контроля и мониторинга действий персонала достаточно широк. Причем российское ПО представляет серьезную конкуренцию зарубежному. Так применение программного комплекса «Стахановец: Полный контроль» позволит предотвратить утечки информации, выявить угрозы в действиях сотрудников, а также функция составление ежедневных отчетов о работе позволит обнаружить факторы, которые могут влиять на продуктивность работников.

Утечка конфиденциальной информации может нанести как ущерб для организации (репутационный, финансовый), так и привести к ликвидации компании. Поэтому следует уделять повышенное внимание методам и формам работы персонала, допущенному к конфиденциальной информации. Стоит отметить, чтобы обеспечить полноценную защиту нужно применять правовые и технические меры по защите информации.

Список использованных источников:

1. Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 12.12.2023) «Об информации, информационных технологиях и о защите информации». – URL: http://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения 15.03.2024).

2. Леонтьев, А.С. Защита информации: учебное пособие / А.С. Леонтьев. – Москва: РТУ МИРЭА, 2021. – 79 с. – Текст: электронный // Лань: электронно-библиотечная система. – URL: https://e.lanbook.com/book/182491 (дата обращения: 26.04.2024).

3. Прохорова, О.В. Информационная безопасность и защита информации: учебник для спо / О.В. Прохорова. – 5-е изд., стер. – Санкт-Петербург: Лань, 2024. – 124 с.

4. Тумбинская, М.В. Защита информации на предприятии: учебное пособие / М.В. Тумбинская, М.В. Петровский. – Санкт-Петербург: Лань, 2020. – 184 с.

СЕКЦИЯ 4. КОНЦЕПЦИЯ И МЕТОДЫ ИНЖЕНЕРНО-ТЕХНИЧЕСКОГО ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

УДК 004

Д.Д. Дмитриева
Уфимский университет
науки и технологий, Уфа, Россия

Научный руководитель:
Р.М. Яппаров
Уфимский университет
науки и технологий, Уфа, Россия

ПЕРЕДАЧА И ЗАЩИТА ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ
DATA TRANSMISSION AND PROTECTION IN INFORMATION SYSTEMS

Аннотация: Передача и защита данных в информационных системах являются важными аспектами современного цифрового мира. В меру того, как информационные технологии становятся все более распространенными, управление данными приобретает критическое значение, поэтому необходимо делать уклон на обеспечение безопасности при передаче и защите информации.

Abstract: Data transmission and protection in information systems are important aspects of the modern digital world. As information technology becomes more widespread, data management is becoming critical, so it is necessary to focus on ensuring security in the transmission and protection of information.

Ключевые слова: Передача данных, защита информации, информационная система, информационная безопасность.

Keywords: Data transmission, information protection, information system, information security.

Передача и защита данных в информационных системах являются важными аспектами современного цифрового мира. В меру того, как информационные технологии становятся все более распространенными, управление данными приобретает критическое значение.

Передача данных – это процесс передачи информации от одного узла или устройства к другому. В контексте информационных систем, это означает передачу данных от источника, будь то человек или другая система, к конечному получателю. Важно обеспечить надежное,

эффективное и безопасное передачу данных, чтобы предотвратить их потерю, повреждение или несанкционированный доступ.

Для высокоскоростной передачи данных предпочтительно создавать и использовать специальные каналы и сети передачи данных [2].

Одним из элементов современных структурированных кабельных систем является витая пара. Спектр передаваемого сигнала расширяется до более высоких частот в соответствии с требованиями к высокой и сверхвысокой четкости изображения.

Ассоциация производителей электронного оборудования и сервис-провайдеров разработала новый стандарт домашних сетей, использующих коаксиальный кабель, с целью его продвижения и распространения. Среди участников альянса такие компании, как Cisco, Alcatel и Westell. С помощью этой технологии к одной основной модели может быть подключено до 16 абонентских устройств.

Стандарт беспроводной связи называется технологией WiMAX. Даже на ранних этапах технологического развития и внедрения было ясно, что информационное покрытие на основе WiMAX расширит использование выделенных линий и DSL-соединений в качестве замены неэффективных средств соединения нескольких точек WI-FI и эффективно решит проблемы, связанные с этим.

Полнофункциональных аналогов высокоскоростного цифрового спутникового модема, разработанного томскими учеными, в России нет. Устройство имеет один канал с максимальной пропускной способностью 1 Гбит/с. Модем – это часть оборудования наземной станции, обеспечивающая двунаправленную связь со спутником. Он был создан научно-производственной компанией «Микран». Разработчики утверждают, что в то время как зарубежные спутниковые модемы могут развивать скорость до 314 Мбит/с, скорость российских спутниковых модемов в настоящее время составляет 155 Мбит/с. Кроме того, достижения в области современных технологий достигли скорости 800 Мбит/с во всем мире.

Американская компания ArrayComm разработала современную технологию под названием but, которая обеспечивает высокоскоростную беспроводную связь. Стоимость передачи информации невелика. В настоящее время беспроводные модемы портативных компьютеров являются единственными, которые поддерживают технологию пакетной передачи. Для каждого абонента пакетные системы, которые используются в настоящее время, обеспечивают передачу данных со скоростью до 1 Мбит/с. Ожидается, что в последующих версиях протокола эта скорость возрастет до 5 Мбит/с.

UWD – это беспроводная технология, обладающая высокой пропускной способностью (480 Мбит/с) и низким энергопотреблением,

которые позволяют передавать данные на короткие расстояния до 10 метров. Широкие диапазоны частот необходимы при использовании технологии ортогонального мультиплексирования несущей частоты в сочетании с несколькими диапазонами частот для передачи данных по СШП-радиоканалам [1].

На сегодняшний день, самой передовой и быстрой технологией беспроводной передачи данных является использование световых вихрей. Эта инновационная методика позволяет достичь скорости передачи данных до 2,5 Тбит/с, что делает её невероятно эффективной для передачи огромных объемов информации. Принцип работы заключается в использовании электромагнитных волн, которые формируются в специфические вихри, обеспечивая стабильную и быструю передачу данных. Такой подход открывает новые возможности для передачи данных на сверхвысоких скоростях, внося революционные изменения в область беспроводных коммуникаций.

Защита данных – это набор мер и систем, разработанных для обеспечения конфиденциальности, целостности и доступности данных.

Для того чтобы более эффективно и безопасно происходили передачи и защиты в информационных системах используются различные методы и технологии. Защита данных особенно важна в наше время, и без нее организация может столкнуться со многими негативными последствиями.

Однако передача и защита данных в информационных системах не являются статическими понятиями. С развитием технологий и все более изощренных способов взлома, необходимо постоянное обновление и модернизация систем защиты данных. Ведь даже самые надежные методы шифрования могут быть взломаны, если не принимать во внимание новые угрозы и уязвимости.

Другим аспектом, который следует учитывать, является физическая безопасность средств хранения данных. Центры обработки данных и серверные помещения должны быть оборудованы строгими мерами контроля доступа, включая биометрическую аутентификацию и видеонаблюдение, чтобы не допустить получения посторонними лицами физического доступа к конфиденциальной информации. Избыточные системы резервного копирования и планы аварийного восстановления также служат в качестве мер на случай непредвиденных обстоятельств для обеспечения доступности и целостности данных в случае непредвиденных инцидентов [3].

В современном мире безопасность и надежность информационных систем становятся всё более критическими вопросами. Передача и защита данных играют важную роль в обеспечении этой безопасности, обеспечивая сохранность конфиденциальности, целостности и доступности информации. Акцент на этих аспектах не только гарантирует

защиту от угроз, но и способствует эффективной работе современных технологий, обеспечивая их стабильность и функциональность.

Список использованных источников:

1. Канатьев К.Н., Большаков В.Н., Куприков О.Д., Горошков Д.Б., Баулин Е.И. Анализ угроз безопасности беспроводной сети и разработка оптимальных методов их предупреждения // Инновации и инвестиции. 2022. №3. – Текст: электронный – URL: https://cyberleninka.ru/article/n/analiz-ugroz-bezopasnosti-besprovodnoy-seti-i-razrabotka-optimalnyh-metodov-ih-preduprezhdeniya (дата обращения: 22.04.2024).

2. Муртазина А.М., Савичев А.В. Современные средства передачи данных // Материалы IX Международной студенческой научной конференции «Студенческий научный форум» – Текст: электронный – URL: https://scienceforum.ru (дата обращения: 22.04.2024).

3. Рева В.В. Вопросы модернизации системы защиты сетевого канала передачи данных// Молодой исследователь Дона. 2023. № 2. – Текст: электронный – URL: https://cyberleninka.ru/article/n/voprosy-modernizatsii-sistemy-zaschity-setevogo-kanala-peredachi-dannyh (дата обращения: 22.04.2024).

УДК 004.056

Т.И. Кашапов, А.Х. Хаертдинов
Казанский национальный исследовательский технический университет им. А.Н. Туполева – КАИ, г. Казань, Россия

Научный руководитель:
М.В. Тумбинская
Казанский национальный исследовательский технический университет им. А.Н. Туполева – КАИ, г. Казань, Россия

РАЗРАБОТКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ПО ОБНАРУЖЕНИЮ УГРОЗ SQL ИНЪЕКЦИЙ В ИСХОДНОМ КОДЕ
DEVELOPMENT OF SOFTWARE TO DETECT SQL INJECTION THREATS IN SOURCE CODE

Аннотация: В данной статье разработан алгоритм проверки исходного кода программы и выработки рекомендаций по устранению уязвимостей. Предложенный алгоритм заложен в основу специального

программного обеспечения, реализующего предотвращение угроз в исходном коде на примере SQL-инъекций.

Abstract: This article develops an algorithm for checking the source code of a program and developing recommendations for eliminating vulnerabilities. The proposed algorithm underlies special software that implements the prevention of threats in source code using the example of SQL injections.

Ключевые слова: SQL-инъекция, уязвимость, программное обеспечение, исходный код.

Keywords: SQL injection, vulnerability, software, source code.

В настоящее время существует большое количество разновидностей уязвимостей. К самым распространенным уязвимостям относятся атаки на базе SQL-инъекции, при которых злоумышленник внедряет вредоносный код, написанный на SQL, в строки, отправляемые в СУБД. В марте 2024 года эксперты Positive Technologies отнесли к трендовым еще пять уязвимостей. Атаки с использованием SQL-инъекций занимают первое место в этом списке, что делает эту уязвимость лидером по частоте эксплуатации и нанесению ущерба.

Целью данной работы является разработка программного обеспечения для поиска SQL-инъекций в исходном коде.

Для реализации программы использовался язык программирования C# на .NET Framework с использованием Windows.Forms и библиотеки iText для генерации отчета. Пример части листинга кода приведен на рисунках ниже. Основной модуль:

```
namespace VulnerabilityScanner{
  public partial class MainForm : Form    {
    public MainForm(){
      InitializeComponent();       }
    private void browseButton_Click(object sender, EventArgs e){
      OpenFileDialog openFileDialog = new OpenFileDialog();
      openFileDialog.Filter = "Text files | *.txt";
      if (openFileDialog.ShowDialog() == DialogResult.OK){
        string filePath = openFileDialog.FileName;
        CreateReport(filePath);          }       }
    private void CreateReport(string filePath){
      SqlVulnerabilityScanner sql = new SqlVulnerabilityScanner();
     sql.FindSqlVulnerabilities(filePath);
      // Создание отчета в pdf формате
      string pdfFilePath = Path.ChangeExtension(filePath, "pdf");
      PdfWriter writer = new PdfWriter(pdfFilePath);
      PdfDocument pdf = new PdfDocument(writer);
      Document document = new Document(pdf);
      document.Add(new Paragraph("Отчет об уязвимостях"));
     AddVulner();
      document.Close();
      writer.Close();       }   }   }
```

Рисунок 1 – Фрагмент программного кода

В данном модуле формируется интерфейс и реализуется функция добавления уязвимостей отчет и сохранения отчета в PDF формате.

Часть листинга кода поиска уязвимости с использованием регулярных выражений:

```
public class SqlVulnerabilityScanner{
    public void FindSqlVulnerabilities(string filePath){
        try    {
            string fileContents = File.ReadAllText(filePath);
            string sqlQueryPattern = @"select\s+(?:(?!--|from|where|group by|order
by|hav¬ing|limit)[\s\S])*?\b(?:insert|update|delete|drop|alter|create|grant|truncate|(?:s(
?:e(?:t|l(?:e(?:c(?:t|ted)?)?|i(?:ze|on_identity))|r(?:v_(?:name|uid)|)(?:user|role)|tansacti
on_isolation_level))|grant|revoke)\b";
            MatchCollection matches = Regex.Matches(fileContents,
sqlQueryPattern, RegexOptions.IgnoreCase);    }
        catch (Exception ex){
            MessageBox.Show("Ошибка при выполнении сканирования на
уязвимости: " + ex.Message); }    }}
```

Рисунок 2 – Фрагмент программного кода

Таким образом, разработано ПО, которое можно применять для обучения студентов и начинающих программистов безопасному написанию кода.

Список использованных источников:

1. Мухаматханов Р.М., Михайлов А.А., Баянов Б.И., Тумбинская М.В. Классификация DDOS-атак на основе нейросетевой модели //Прикладная информатика. 2019. Т. 14. № 1 (79). С. 96-103.
2. Positive Technologies представила топ трендовых уязвимостей за март [Электронный ресурс]. 2024. URL: https://www.ptsecurity.com/ru-ru/about/news/positive-technologies-predstavila-top-trendovyh-uyazvimostej-za-mart/ (дата обращения: 02.04.2024 г.).
3. Тумбинская М.В., Баянов Б.И., Рахимов Р.Ж., Кормильцев Н.В., Уваров А.Д. Анализ и прогнозирование вредоносного сетевого трафика в облачных сервисах // Бизнес-информатика. 2019. Т. 13. No 1. С. 71-81.
4. Тумбинская М.В. Системный подход к обеспечению защиты от нежелательной информации в социальных сетях // Вопросы кибербезопасности. 2017. № 2 (20). С. 30-44.
5. Уязвимости и угрозы веб-приложений в 2020–2021 гг. [Электронный ресурс]. 2022. URL: https://www.ptsecurity.com/ru-ru/research/analytics/web-vulnerabilities-2020-2021/ (дата обращения: 03.04.2024 г.).

УДК 004

Т.И. Макаримов
Уфимский университет
науки и технологий, Уфа, Россия

Научный руководитель:
С.С. Валеев
Уфимский университет
науки и технологий, Уфа, Россия

ОРГАНИЗАЦИЯ ЗАЩИЩЕННОГО ОБМЕНА ДАННЫМИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ УПРАВЛЕНИЯ
ORGANIZATION OF SECURE DATA EXCHANGE IN AUTOMATED CONTROL SYSTEMS

Аннотация: Статья посвящена проблеме организации защищенного обмена данными в автоматизированных системах управления технологическими процессами. Рассматривается особенность реализации защищенного обмена данными с применением встраиваемых средств защиты информации.

Abstract: The article is devoted to the problem of organizing secure data exchange in automated process control systems. The peculiarities of implementing secure data exchange using built-in information security tools are considered.

Ключевые слова: АСУ, ПЛК, Modbus, АРМ, технологический процесс, SIES, SCADA.

Key words: Automated control system, PLC, Modbus, SIES, SCADA.

Защита информации в автоматизированных системах управления технологическим процессом (АСУ ТП) является актуальной задачей. Ведь именно в этих системах реализуются алгоритмы управления ключевыми производственными процессами современного промышленного предприятия. Потенциальные нарушители могут изменить передаваемые данные или нарушить их целостность, что может повлечь за собой как кратковременную, так и долговременную остановку производства, требующую значительных затрат на восстановление.

Однако защита АСУ ТП относится к классу сложно решаемых задач. Системы АСУ ТП, как правило, функционируют более 10-20 лет, и ранее им не уделялось должного внимания, касающиеся вопросам информационной безопасности. Технологии развивались менее активно, и важность обеспечения безопасности данных не была такой высокой, как

сейчас. В связи с этим возникают трудности при внедрении современных протоколов обмена данными и вычислительных технологий в системы управления [1].

Особенностью организации обмена данными в автоматизированных системах управления технологическими процессами является то, что передача данных в них осуществляется не по стандартному протоколу TCP/IP, а по разнообразным (включая устаревшие) протоколам, таким как Modbus и другие [2].

В связи с этим, более целесообразно обеспечивать защиту не на уровне каналов связи, так как организация защиты для разных протоколов может быть трудоемкой и затратной. Вместо этого, следует обеспечивать защиту на уровне данных, чтобы каналы связи оставались открытыми, а передаваемые данные были защищены.

В настоящее время, реализацию данной концепции предлагает компания АО «ИнфоТеКС» с помощью решения ViPNet SIES (Security for Industrial and Embedded Solutions). Данное решение предназначено для встраивания в АСУ ТП и обеспечивающее высокий уровень защиты данных.

Основными преимуществами комплекса является апробированная высокая эффективность реализации способов защиты информации в промышленных системах. Защита обмена данными на всех уровнях АСУ (как нижнего и среднего) реализуется на базе используемого модуля ViPNet SIES Core, встраиваемого в защищаемое устройство.

На верхнем уровне используется модуль ViPNet SIES Unit, реализованный в виде прикладной службы и обеспечивающий высокопроизводительное выполнение базовых операций защиты с целью защиты обмена данными в таких системах как SCADA-серверы, серверные системы сбора и мониторинга данных [3].

Концепция реализации предлагаемой организации защищенного обмена данными предоставлена на рисунке 1.

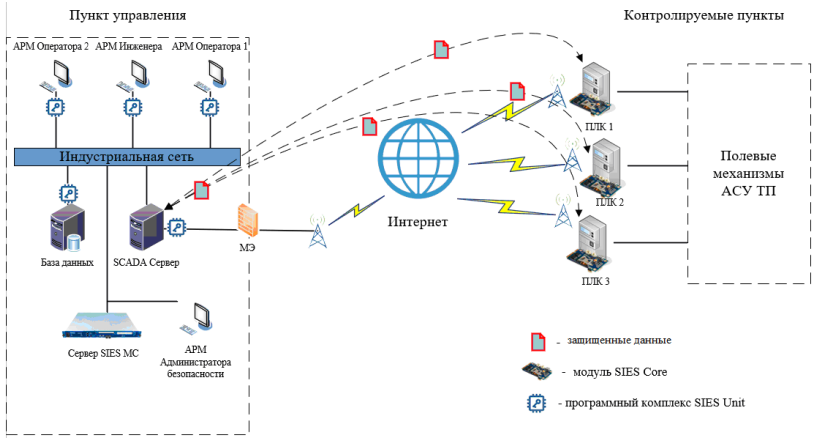

Рисунок 1 – Структурная схема организации защищенного обмена данными в АСУ ТП

На рисунке 1 представлена схема организации защищенного обмена данными в АСУ ТП, включающая АРМы инженера и операторов, SCADA сервер и базу данных – все это перечисленное оборудование является основой центра управления АСУ ТП.

Для защиты данных, используемых в пункте управления, используется программный комплекс ViPNet SIES Unit.

Данные, после реализации алгоритмов защиты информации операций, отправляются по сети до программируемых логических контроллеров (ПЛК). В контроллеры встроены модули защиты информации ViPNet SIES Core – именно они служат средством обработки защищенных данных, которые были получены по сети из пункта управления. После этого, данные поступают на сами конечные устройства (датчики, сенсоры, исполнительные механизмы).

Таким образом, при использовании предлагаемых технологий защиты информации, удается решить задачу обеспечения требуемого уровня защиты данных, которые циркулируют в АСУ ТП от одного технологического узла до другого.

В этом случае на всех уровнях обмена данными они защищены по определенному критерию защищенности.

Следует отметить необходимость решения всех организационных и технологических задач сопровождения данного способа защиты информации.

Список использованных источников:

1. Музипов, Х.Н. Системы управления технологическими процессами добычи, промысловой подготовки и транспорта нефти и газа / Х. Н. Музипов. – Санкт-Петербург: Лань, 2023. – 268 с.

2. Системы автоматизации в газовой промышленности: учебное пособие / М.Ю. Прахова, Э.А. Шаловников, А.Н. Краснов [и др.]; под общей редакцией М.Ю. Праховой. – Вологда: Инфра-Инженерия, 2019. – 480 с.

3. Техническая документация ViPNet SIES [электронный ресурс]. – URL: https://infotecs.ru/products/vipnet-sies-mc/ (дата обращения: 26.04.2024).

УДК 004

А.Н. Насертдинова
Уфимский университет
науки и технологий, Уфа, Россия

Научный руководитель:
И.А. Шагапов
Уфимский университет
науки и технологий, Уфа, Россия

ЗАЩИТА ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА В ОРГАНИЗАЦИИ
PROTECTION OF ELECTRONIC DOCUMENT MANAGEMENT IN THE ORGANIZATION

Аннотация: В статье рассматривается система электронного документооборота и ее основные цели. Основное внимание сосредоточено на преимуществах внедрения электронного документооборота в организации, а также проблемы безопасности информации и методы защиты электронного документооборота.

Abstract: The article discusses the electronic document management system and its main objectives. The main focus is on the advantages of implementing electronic document management in an organization, as well as information security issues and methods of protecting electronic document management.

Ключевые слова: Информация, документация, электронный документ, документооборот, электронный документооборот (ЭДО), системы электронного документооборота (СЭД), защита информации, информационная безопасность, защита электронного документооборота.

Keywords: Information, documentation, electronic document, document management, electronic document management (EDI), electronic document management systems (EDMS), information security, information security, electronic document management protection.

В настоящее время современный бизнес быстро развивается, и информатизация играет ключевую роль в его развитии. Информационные технологии тесно переплетаются в традиционных областях коммерческой деятельности, становясь неотъемлемой частью бизнес-процессов. Каждое предприятие сталкивается с необходимостью организации и оптимизации системы документооборота, а с увеличением документации возникает необходимость в переводе бумажного документооборота в электронную форму. Так создается концепция системы электронного документооборота.

Под системой электронного документооборота подразумевается организационно-техническая система, которая может обеспечить процесс формирования, управления доступом и отправки электронных документов, а также обеспечивает контроль и регулирование потока документации в компании. То есть СЭД - это автоматизированная корпоративная система управления электронными документами.

При использовании бумажного документооборота существует риск случайной потери документов организации, а также на процесс создания и редактирования документов затрачивается значительное время. В случае использования электронного документооборота автоматизация поможет уменьшить время на обработку, а также практически исключить риск случайной потери, поскольку документы хранятся на электронных устройствах (в том числе дисках и флеш-накопителях). Также СЭД помогает руководству более эффективно выполнять функции контроля управления.

Но с переходом на электронный формат работы с документами возникает вопрос безопасности информации, содержащейся в этих документах, граничения доступа, а также подлинности созданных документов. Стоит отметить, что подлинность документа можно подтвердить с помощью использования электронной подписи, имеющей полную юридическую силу, как и рукописная.

Настройка аутентификации и разграничение прав пользователей способны обеспечить безопасный доступ к данным внутри системы электронного документооборота. Самый популярный и доступный метод аутентификации – парольный. Но именно человеческий фактор влияет на надежность парольной защиты. Также существует способ аутентификации с помощью смарт-карты или USB-ключа. Но самый надежный способ – аутентификация с помощью биометрических данных (например, отпечаток пальца).

Для защиты конфиденциальной информации в СЭД применяются криптографические методы защиты информации. Шифрование не позволит нарушить конфиденциальность документа даже в случае несанкционированного доступа к нему злоумышленника.

Отношения в области электронного документооборота законодательно регулируются нормативно-правовыми актами, в том числе Федеральным законом «Об информации, информационных технологиях и о защите информации».

К техническим средствам защиты относится: применение антивирусного ПО, резервное копирование данных, криптографические средства защиты информации, своевременное обновление ОС устройства, установка прав разграничения доступа и др.

Одной из самых защищенных систем электронного документооборота является «Контур.Диадок». В данной СЭД используются следующие методы для защиты конфиденциальной информации:

– двухфакторная аутентификация при помощи электронной подписи, номера телефона, логина и пароля, что уменьшает угрозу несанкционированного доступа;

– использование программы «Крипто Про» для обработки сертификатов электронной подписи;

– резервное копирование данных на разных серверах Контура;

– неограниченный срок хранения документов на серверах.

Также стоит отметить, что при внедрении СЭД требуется проведение инструктажа и обучения сотрудников, а также курсы повышения квалификации. У каждого сотрудника нужно настроить определенные права доступа в зависимости от выполняемых должностных обязанностей.

Подводя итог, можно сказать, что автоматизированные системы документооборота все больше внедряются в компаниях. Положительный эффект от внедрения системы электронного документооборота заключается в сокращении времени работы с информацией, возможность хранения больших массивов данных без затрат на отдельные помещения (архивы), прозрачность управленческий действий и другие полезные функции.

Список использованных источников:

1. Анацкая, А.Г. Защита электронного документооборота: учебное пособие / А.Г. Анацкая. – Омск: СибАДИ, 2019. – 87 с. – Текст: электронный // Лань: электронно-библиотечная система. – URL: https://e.lanbook.com/book/149493 (дата обращения: 22.04.2024).

2. Грибков, Д.Н. Технологии электронного документооборота: учебное пособие / Д.Н. Грибков, А.В. Калянов. – Орел: ОГИИК, 2021. – 105

с. – Текст: электронный // Лань: электронно-библиотечная система. – URL: https://e.lanbook.com/book/261932 (дата обращения: 22.04.2024).

3. Котлярова, Л.Д. Делопроизводство и документооборот: практикум: учебное пособие / составитель Л.Д. Котлярова. – Пос. Караваево: КГСХА, 2020. – 44 с. – Текст: электронный // Лань: электронно-библиотечная система. – URL: https://e.lanbook.com/book/171710 (дата обращения: 22.04.2024).

4. Ульянова, Н.Д. Электронный документооборот: учебно-методическое пособие / Н.Д. Ульянова. – Брянск: Брянский ГАУ, 2021. – 24 с. – Текст: электронный // Лань: электронно-библиотечная система. – URL: https://e.lanbook.com/book/304610 (дата обращения: 22.04.2024).

УДК 004.056

Р.Р. Султанов
Уфимский университет
науки и технологий, Уфа, Россия

Научный руководитель:
С.С. Валеев
Уфимский университет
науки и технологий, Уфа, Россия

ПРИМЕНЕНИЕ ПРИНЦИПА НУЛЕВОГО ДОВЕРИЯ НА ПРИМЕРЕ УЧЕБНЫХ ЗАВЕДЕНИЙ
APPLYING ZERO TRUST PRINCIPLE ON THE EXAMPLE OF EDUCATIONAL INSTITUTIONS

Аннотация: В статье рассматривается принцип нулевого доверия, меры, необходимые для его внедрения и эффект от применения данной концепции в учебных заведениях.

Abstract: The article discusses the principle of zero trust, the measures necessary for its implementation and the effect of applying this concept in educational institutions.

Ключевые слова: Принцип нулевого доверия, архитектура нулевого доверия, защита информации, учебное заведение.

Keywords: Zero trust principle, zero trust architecture, information security, educational institution

В современном мире учебные заведения, будучи центрами знаний и обучения, активно используют разнообразные информационные

технологии для обеспечения учебного процесса и управления данными. Однако с ростом цифровых угроз становится крайне важным обеспечить надежную защиту информации от несанкционированного доступа и утечек. Концепция нулевого доверия может стать решением для обеспечения высокого уровня защиты информации.

Принцип нулевого доверия (Zero Trust) основывается на том, что никакое устройство или пользователь не должны автоматически получать доверие в сети, даже если они уже находятся внутри защищенной сети [1]. В рамках этого подхода каждый запрос на доступ к ресурсам должен проходить строгую аутентификацию, авторизацию и шифрование, независимо от местоположения пользователя или устройства. Концепция Zero Trust опирается на минимизацию привилегий и максимальное ограничение доступа к данным для снижения риска атак и утечек информации. Основная цель Zero Trust заключается в предотвращении несанкционированного доступа к данным и сервисам, а также в обеспечении максимально детализированного контроля доступа [2].

Эта концепция основывается на принципе минимизации привилегий и максимальном ограничении доступа к данным с целью снижения риска возможных атак и утечек информации. Целью Zero Trust является: «предотвращение несанкционированного доступа к данным и сервисам в сочетании с максимально детализированным обеспечением контроля доступа».

Учебные заведения обладают обширными информационными ресурсами, включая персональные данные студентов, учебные материалы, исследования, финансовую информацию и многое другое. Поэтому защита этой информации является актуальной конкретной задачей.

Для реализации концепции нулевого доверия необходимо внедрение следующих мер:

– строгой аутентификации и авторизации - каждый пользователь и устройство должны быть строго идентифицированы и аутентифицированы перед получением доступа к системе. Это позволяет предотвратить несанкционированный доступ даже в случае компрометации учетных данных;

– микросегментации сети - подразумевает разделение сетевых ресурсов на отдельные сегменты, доступ к которым предоставляется исключительно авторизованным пользователям. Этот подход способствует предотвращению распространения атак внутри сети и минимизации возможного ущерба.

– шифрования данных данных - все передаваемые по сети данные должны быть зашифрованы, чтобы защитить их от перехвата и утечки. Это особенно критично для персональной информации студентов и конфиденциальных исследовательских материалов.

– ограничения доступа – система защиты должна обеспечивать контроль доступа ко всем типам ресурсов [3,4].

Одним из вариантов внедрения концепции нулевого доверия может стать применение на оконечных устройствах специальных клиентских приложений, обладающими следующими функциями:

– защита устройств от внешних и внутренних атак;

– обеспечение конфиденциальности передачи информации и ее защиты на персональном устройстве;

– безопасная работа с корпоративными ресурсами через защищенные каналы с применением отечественных алгоритмов шифрования с большим ключом;

– многофакторная аутентификация пользователя;

– точечное применение политик безопасности для конкретного устройства или пользователя;

– создание защищенного канала коммуникаций для пользователей;

– фильтрация трафика.

Такой подход обеспечит многоуровневую защиту устройства и позволит точечную политику информационной безопасности для конкретного устройства или группы устройств.

Результатом применения концепции нулевого доверия в системе защиты информации университета может стать:

– конфиденциальность: строгая аутентификация, микросегментация и шифрование данных существенно повышают уровень безопасности и снижают риск утечек информации.

– соответствие нормативным требованиям: применение концепции нулевого доверия в системе защиты университетами способствует выполнению законодательных требований по защите данных и помогает избежать потенциальных штрафов;

– улучшенное управление доступом: система нулевого доверия позволяет администраторам точно контролировать доступ к ресурсам и минимизировать риски внутренних угроз;

– повышение доверия: защита конфиденциальных данных студентов и исследовательских материалов способствует укреплению доверия заинтересованных лиц, включая студентов, родителей, финансовых спонсоров и государственных органов.

Внедрение концепции нулевого доверия в системы информационной защиты учебных заведений позволяет эффективно защищать ценные данные от угроз и утечек, обеспечивая высокий уровень безопасности. Это не только укрепляет доверие, но и поддерживает стабильное функционирование учебного заведения в современной цифровой среде.

Список использованных источников:

1. Концепция Zero Trust: не доверяй - всегда проверяй – URL: https:// www.kaspersky.ru/ blog/zero-trust-security/28780/?ysclid=lvqexsu7y0477804 184 (дата обращения: 25.04.2024).
2. С.С. Валеев, Н.В. Кондратьева, М.Б. Гузаиров, А.В. Мельников. Этапы реинжиниринга информационной системы предприятия в рамках технологии нулевого доверия. [Электронный ресурс]: vestnik-rosnou.ru– 2023 – Режим доступа: https://vestnik-rosnou.ru/sites/default/files /136_Сложные%20системы%20№%203%20ПРОСМОТРОВЫЙ.pdf (дата обращения: 30.04.2024).
3. С.С. Валеев, Н.В. Кондратьева. Особенности проектирования систем безопасности на базе архитектуры нулевого доверия. [Электронный ресурс]: ivdon.ru– 2023 – Режим доступа: http://www.ivdon.ru/uploads/article/pdf/IVD_68__8_valeev_kondratyeva_v2.p df_72458b243f.pdf (дата обращения: 30.04.2024).
4. Валеев С.С., Кондратьева Н.В., Мельников А.В. Архитектура предприятия и архитектура нулевого доверия [Электронный ресурс]: info-secur.ru– 2023 – Режим доступа: https://www.info-secur.ru/index.php/ojs/article/download/413/371/ (дата обращения: 30.04.2024).

УДК 004.056

Н.А. Федосеев
Магнитогорский государственный технический университет им. Г.И. Носова, Магнитогорск, Россия
Научный руководитель:
И.И. Баранкова
Магнитогорский государственный технический университет им. Г.И. Носова, Магнитогорск, Россия

ОБЗОР РЕШЕНИЙ АППАРАТНЫХ КРИПТОШЛЮЗОВ ДЛЯ ПОСТРОЕНИЯ ЗАЩИЩЕННЫХ КОРПОРАТИВНЫХ СЕТЕЙ
OVERVIEW OF HARDWARE CRYPTOGRAPHIC GATEWAY SOLUTIONS FOR BUILDING SECURE CORPORATE NETWORKS

Аннотация: В данной статье рассматриваются методы организации защиты корпоративных сетей, так же поднята проблема использования программного VPN. Кратко сделан обзор на существующие на рынке России решения криптографической защиты информации. Описана

проблематика их использования и предложены возможные решения данной проблемы.

Abstract: This article discusses the methods of organizing the protection of corporate networks, as well as the problem of using a software VPN. A brief overview of the existing cryptographic information protection solutions on the Russian market is made. The problems of their use are described and possible solutions to this problem are proposed.

Ключевые слова: Криптошлюзы; программный VPN; VPN-шлюзы; корпоративные сети; VipNet; Континент; С-Терра

Keywords: Cryptographic gateways; software VPN; VPN gateways; corporate networks; ViPNet; Continent; C-Terra

Защита конфиденциальной информации является важнейшим компонентом успеха на всех этапах развития деятельности компании в быстро меняющейся бизнес-среде. По мере того как организации внедряют новые стратегии и инновационные технологии, вопрос безопасности и стабильности работы внутри компании остается на первом плане. В рамках данной статьи рассмотрим средства и способы защиты информации в корпоративных сетях.

В основе сетевой защиты лежит использование виртуальных частных сетей (VPN). Эти безопасные соединения стали жизненно важным инструментом для работы удаленных сотрудников, которым необходим доступ к корпоративным ресурсам. Так же сети VPN могут быть использованы для объединения и изоляции отделов внутри компаний, так как отделы могут разделены на офисы и разнесены друг от друга на расстоянии.

Возникла проблематика использования программного VPN, так как стремясь сохранить стабильность, безопасность и целостность своей коммуникационной сети, Российская Федерация приняла меры для устранения потенциальных угроз. В августе 2023 года Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) инициировала масштабные изменения ограничений. В конце октября 2023 года число заблокированных программных VPN превысило отметку 170 единиц, а также более 200 почтовых сервисов были ограничены. Блокировки стали проводиться не по IP-адресам VPN сервисов, а по протоколам, в частности речь идет о таких популярных протоколах, как OpenVPN, IKEv2 и Wireguard.

Эти действия имеют серьезные последствия, создавая неудобства для компаний, использующих программный VPN основанный на данных протоколах или любых других, которые так же уязвимы для блокировки. Для решения данной проблемы можно рассмотреть внедрение программно-аппаратных комплексов для криптографической защиты

трафика передаваемого при помощи «туннельных соединений» между компьютером пользователя и компьютером-сервером организации вместо использование программного VPN основанного на общеизвестных протоколах подверженных блокировке.

В число основных пользователей входят самые разнообразные организации, начиная от небольших компаний, занимающихся частным бизнесом, и заканчивая государственными органами. Решающим фактором при выборе криптографического шлюза является наличие у него действительных сертификатов от регулирующих органов, таких как ФСБ и ФСТЭК России, которые выдают сертификаты только для решений, которые используют отечественные алгоритмы шифрования, такие как ГОСТ 28147-89. Рассмотрим особенности трех российских криптошлюзов, применяемых в государственных органах России.

Известная Российская компания «ИнфоТеКС» предлагает продукт ViPNet Coordinator HW, который является программно-аппаратным комплексом. Данный продукт является сертифицированным криптографическим шлюзом и межсетевым экраном с поддержкой функций L3 и L2. Это решение обеспечивает защиту данных путем их шифрования в соответствии с ГОСТ 28147-89, как в режиме гаммирования, так и в режиме гаммирования с обратной связью. Программно-аппаратный комплекс работает на адаптированной операционной системе Linux и применяет проприетарный протокол IPlir, однако это применение осуществляется только в том случае, когда смежные шлюзы могут без проблем найти друг друга. Когда устройства находятся в разных подсетях, то блок данных инкапсулируется в UDP или в TCP.

Второй аппаратно-программный комплекс шифрования АПКШ "Континент" 3.9 (IT компания «Код Безопасности»), работает под управлением ОС FreeBSD и обеспечивает защиту данных при межсайтовом шифровании в соответствии со стандартами ГОСТ 28147-89. Из особенностей продукта можно выделить функции сжатия IP-пакетов по алгоритму Deflate, с возможностью ручной настройки длины шифрования.

И третий продукт С-Терра Шлюз (IT компания «С-Терра СиЭсПи») представляет собой программный комплекс, который адаптируем к различным аппаратным платформам. Комплекс позволяет шифровать данные в соответствии с ГОСТ 28147-89 и обеспечивать безопасность трафика по открытым каналам связи с использованием протокола IPSec. Так как комплекс использует операционную систему Debian Linux с криптомодулем, то оно поддерживает набор алгоритмов ГОСТ, в том числе блочные шифры из ГОСТ Р 34.12-2015 – «Магма» и «Кузнечик.

Каждый из представленных выше систем, используемые в качестве

криптомаршрутизаторов и VPN-шлюзов, имеют сертификацию по классам защиты КС1, КС2 и КС3. Все эти решения отвечают требованиям о защите информации, утвержденные приказом ФСБ России и ФСТЭК России и позволяют компаниям в кратчайшие сроки пересмотреть коммуникационные стратегии, а специалистам данной области сосредоточиться на технических аспектах, критериях выбора криптошлюза для своей организации и решение проблемы несовместимости криптошлюзов разных вендоров.

Возможным решением проблемы можно предложить встраивание в существующие криптошлюзы еще одного протокола совместимого между собой, с сохранением всех существующих. Можно предположить, что класс защиты для этого протокола будет ниже, но такое решение позволит при сохранении инвестиций в существующие защищенный сети обеспечить без покупки дополнительного оборудования, например, передачу отчетности, взаимодействие на местном уровне, когда класс защиты допустимо может быть ниже. Так же возможным решением проблемы может быть включение требование к отечественным криптошлюзам дополнительного модуля квантовой криптографии или дополнительного алгоритма или протокола, который взаимодействует не по существующим защищенным сетям, а взаимодействует над ними, как вариант через единое государственное облако.

Список использованных источников:

1. Криптошлюзы и корпоративные VPN-решения: особенности российского рынка. [Электронный ресурс]. – URL: https://www.anti-malware.ru/analytics/Market_Analysis/VPN-Gateway-AM-Live (дата обращения: 12.05.2024).

2. Шесть устройств для сетевого шифрования: плюсы и минусы. [Электронный ресурс]. – URL: https://systempb.ru/company/articles/shest-ustroystv-dlya-setevogo-shifrovaniya-plyusy-i-minusy/ (дата обращения: 12.05.2024).

3. Документация Континент 3.9.3 КС. [Электронный ресурс]. – URL: https://www.securitycode.ru/products/apksh_kontinent/?tab=support, (дата обращения: 12.05.2024).

4. С-Терра Шлюз: характеристики, технология и эксплуатация. [Электронный ресурс]. – URL: https://www.s-terra.ru/products/catalog/s-terra-shlyuz-4-3/?tab=2 (дата обращения: 12.05.2024).

5. VipNet Coordinator HW Шлюз безопасности для защиты каналов связи. [Электронный ресурс]. – URL: https://infotecs.ru/products/vipnet-coordinator-hw-4/ (дата обращения: 12.05.2024).

УДК 659.443

Е.Д. Хорольская
БИП – Университет права и социально-информационных технологий, Минск, Беларусь

Научный руководитель:
А.П. Ковалёв
БИП – Университет права и социально-информационных технологий, Минск, Беларусь

ПОСТ-КЛИК ОПТИМИЗАЦИЯ В ОБЕСПЕЧЕНИИ БЕЗОПАСНОСТИ ПОСЕЩЕНИЙ ВЕБ-СТРАНИЦ
POST-CLICK OPTIMIZATION TO ENSURE SAFE WEB PAGE VISITS

Аннотация: В докладе рассмотрено влияние пост-клик оптимизации на информационную безопасность маркетинговых коммуникаций. Были выявлены наиболее используемые принципы реализации взаимодействий с брендом для единообразного и безопасного опыта посещений веб-страниц.

Abstract: The report examines the impact of post-click optimization on the information security of marketing communications. The most used principles for implementing brand interactions were identified for a consistent and secure web experience.

Ключевые слова: Пост-клик оптимизация, безопасность веб-страниц, маркетинговые коммуникации, маркетинг.

Keywords: Post-click optimization, web page security, marketing communications, marketing.

Оптимизация после клика (PCO) — это стратегия, направленная на улучшение качества обслуживания клиентов и их вовлеченности после нажатия на цифровое объявление. Цель оптимизации после клика — персонализировать опыт, предоставляя релевантную информацию в нужное время и в каждой точке взаимодействия с клиентом — от целевой страницы до завершения оформления заказа.

Целевая страница для безопасного перехода должна быть спроектирована как естественное продолжение объявления, на которое нажимают. Каждый элемент на странице должен сообщать посетителю, что он попал в нужное место и что нужное ему предложение находится всего в одном клике, чтобы совершить покупку или нужное действие. Оптимизация после клика направлена на предоставление

покупателям высокорелевантных целевых страниц и четких призывов к действию, а также распространяется на опыт после покупки.

Оптимизация после клика должна основываться на трёх основных направлениях для безопасного перехода:

1. Масштабируемое создание страниц. Масштабируемое создание — это создание нескольких целевых страниц после клика. Создание целевых страниц после клика в большом масштабе необходимо, потому что этим можно персонализировать и оптимизировать каждую страницу с учетом определенного сегмента аудитории или личности покупателя. Вместо того, чтобы направлять посетителей на загруженную страницу продукта с каждым элементом после клика по объявлению, лучше создать целевые страницы [1]. Где каждая целевая страница посвящена отдельному товару с копией, соответствующей сообщению, главным снимком товара и отзывами клиентов.

2. A/B-тестирование. Оно необходимо, чтобы определить, какие компоненты работают хорошо, а какие нуждаются в улучшениях. В постклик-маркетинге под оптимизацией понимают улучшение компонентов целевых страниц после клика посредством исследования и тестирования пользователей, например, посредством тепловых карт.

3. Персонализация. Персонализация предполагает повышение релевантности рекламы для определенной целевой аудитории. У пользователей, находящихся на стадии выбора товара, другие потребности, чем у потребителя, собирающегося совершить покупку. Удовлетворение обоих типов пользователей с помощью разных целевых страниц после клика эффективнее.

На рисунке 1 показана страница благодарности. На странице сообщается, что заявка принята сайтом и предлагается связь с ассистентом, для того чтобы задать интересующие вопросы, которые могли возникнуть в процессе создания заявки или для обратной связи с компанией. Это наиболее подходящий вариант для страницы благодарности. В случае если у потребителя будет негативный опыт, он сможет сразу сообщить об этом менеджерам, которые исправят ситуацию.

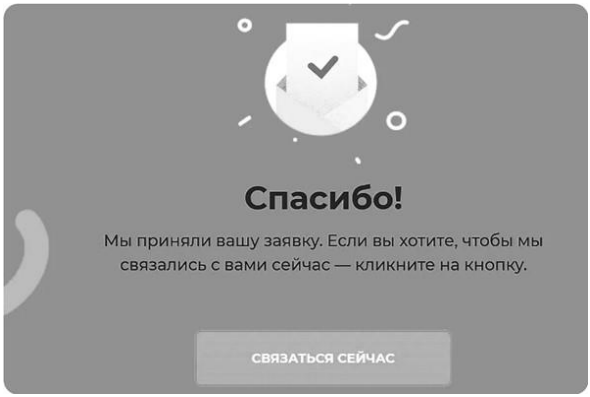

Рисунок 1 – Страница благодарности [2]

Когда потребитель нажимает на объявление, он не только обычно демонстрирует интерес к предложению, но также имеет ожидания относительно того, куда его приведет этот клик. Если целевая страница не соответствует объявлению, это может привести к путанице, разочарованию и потере возможностей продаж, а поисковые системы могут идентифицировать страницу небезопасной для перехода. Оптимизация после клика направлена на превращение как можно большего числа заинтересованных пользователей в клиентов посредством стратегических улучшений. Это достигается за счет масштабируемого создания технически оптимизированных страниц, релевантных/целевых копий целевых страниц с одним основным призывом к действию и несколькими путями выхода.

В случае, когда пользователь за 3-5 секунд понимает, что за организация, на сайт которой он пришёл, что предлагает и как это получить — полдела сделано. Этот принцип заложен в большинстве юзабилити-тестов. Однако сайт при этом тестирует не целевая аудитория, а поведение исполнителей, которых подбирает сервис. Она не совпадает на 100% с поведением реального покупателя [3].

Достаточно сверстать сайт без ошибок и выполнить следующие условия:

– использовать качественные изображения;

– проверить отсутствие грамматических ошибок;

– использовать контрастные конверсионные элементы (форма заявки, кнопка CTA);

– использовать минимум полей в форме заявки.

Методы оптимизации до клика обычно приводят к более высокому CTR объявлений, но если далее будет плохой опыт пост-клика,

то количество конверсий не удастся увеличить. Заставить клиентов нажимать на объявления по-прежнему имеет решающее значение, но уделить время завлечению потенциальных потребителей после нажатия имеет важное значение для увеличения количества кликов, приводящих к конверсиям. Когда целевая страница не соответствует объявлению, на которое нажал клиент, в лучшем случае это может привести к некоторой путанице, а в худшем – может показаться обманом.

Оптимизация после клика помогает создать единообразный и безопасный опыт взаимодействия с брендом, где каждый шаг после клика работает в сочетании с оригинальным сообщением, которое привлекло внимание покупателей.

Список использованных источников:

1. Масштабируемое создание целевых страниц. [Электронный ресурс]. – URL: https://clck.ru/3AE5VU (дата обращения: 20.04.2024).

2. Страница благодарности. [Электронный ресурс]. – URL: https://petr-panda.ru/primery-stranic-spasibo/ (дата доступа: 20.04.2024).

3. Постклик анализ и оптимизация. [Электронный ресурс]. – Режим доступа: https://clck.ru/3AVrZU (дата доступа: 20.04.2024).

СЕКЦИЯ 5. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ И РАЗВИТИЯ ДЕТЕЙ В ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ

УДК 004

И.М. Вагабов, К.А. Моисеева
Уфимский университет
науки и технологий, Уфа, Россия

Научный руководитель:
А.Ф. Фатхелисламов
Уфимский университет
науки и технологий, Уфа, Россия

ОСНОВНЫЕ УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ ДЕТЕЙ ПРИ ИСПОЛЬЗОВАНИИ ГОСУДАРСТВЕННЫХ СЕРВИСОВ
MAIN THREATS TO INFORMATION SECURITY FOR CHILDREN WHEN USING GOVERNMENT SERVICES

Аннотация: Информационная безопасность в сфере государственных сервисов является важнейшей основой защиты личных данных граждан. Как правило, дети не всегда уверены в безопасности своих действий при использовании государственных порталов. В данной статье рассказывается об основных угрозах, связанных с государственными сервисами, а также о рекомендациях по противодействию им.

Abstract: Information security in the sphere of government services is the most important basis for the protection of citizens' personal data. As a rule, children are not always confident in the safety of their actions when using government portals. This article describes the main threats associated with government services, as well as recommendations on how to counteract them.

Ключевые слова: Государственные сервисы, фишинг, социальная инженерия

Keywords: Government services, phishing, social engineering

В данной работе в качестве примера государственных сервисов рассматривается «Портал государственных услуг Российской Федерации»,

«Госуслуги Культура», поскольку регистрация в этих сервисах доступна для граждан, не достигших совершеннолетия [1].

Дети подвержены следующим видам угроз: переход по фишинговой ссылке, наличие сниффера на устройстве, использование недостоверных приложений и социальная инженерия.

Начнём с использования web-версии данного портала. Переход на данный ресурс осуществляется по единственной ссылке. После начального протокола HTTPS, идёт доменное имя. В нём содержится информация о ресурсе. На официальном сайте это WWW, GOSUSLUGI и домен верхнего уровня: RU (Рис.1). Изменяя адресную строку, злоумышленники рассчитывают на невнимательность граждан (Рис.2). Подмена доменного имени, перенаправляет на фишинговый сайт, который визуально тяжело отличим от оригинального сайта.

Рисунок 1 – Адресная строка официального сайта

Рисунок 2 – Адресная строка неофициального сайта

Рекомендательный метод для молодых, а также неопытных пользователей довольно прост. Необходимо использовать браузеры, поддерживающие шифрование TLS по ГОСТу (Рис.3), данный стандарт обязывает браузеры использовать современное шифрование данных для защиты пользовательских данных [2].

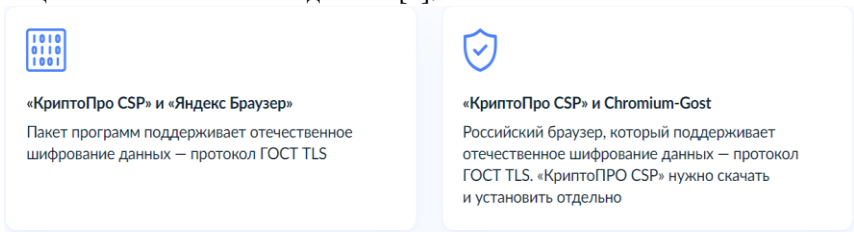

Рисунок 3 – Браузеры с шифрованием данных по ГОСТ TLS для безопасного соединения

Следующее, на что необходимо обратить внимание – это наличие сниффера на устройстве. Подключение к частым сетям позволяет пользователям пользоваться ресурсом вопреки санкциям. Однако тут может случиться следующее: ненадежная частная сеть, которая приводит к тому, что хакеры могут подменять записи в кэше DNS для дальнейшей кражи данных, внедрения вредоносных программ, фишинга и блокировки

обновлений. Такая же ситуация обстоит и с VPN-сервисами. Как правило, бесплатный VPN-сервис – это ненадёжный сервис. Актуальным источников снифферов являются некачественные и бесплатные VPN сервисы. Новые и никому неизвестные VPN сервисы могут предоставлять третьим лицам трафик с устройства пользователя сайта. Как правило, они продают информацию о пользователе, в том числе и его cookie-файлы [3].

Методы борьбы с данной угрозой:

1. Не стоит подключаться к неизвестным сетям, поскольку они могут быть заражены;
2. Используйте проверенные DNS-сервера и VPN-сервисы
3. Не используйте бесплатные ресурсы
4. Не пользуйтесь государственными порталами, во время подключения к зарубежным серверам

В настоящее время существует проблема, что наши отечественные приложения удаляются из магазина приложений различных платформ.

Самый верный способ убедиться в подлинности приложения «Госуслуги» – это скачать через официальный сайт. На выбор будет предложены актуальные версии приложения, а также соответствующие источники.

Есть несколько факторов, на которые нужно обратить внимание при скачивании приложения:

1. Разработчик.

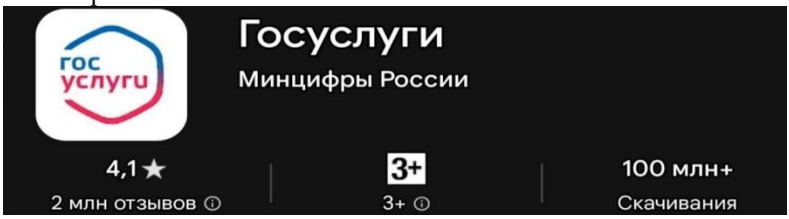

Рисунок 4 – Имя разработчика приложения в Google Play соответствует официальному наименованию государственной службы

2. Количество скачиваний.
3. Рейтинг и отзывы.

Рекомендация для детей: будьте внимательны при скачивании приложения и не переходите по первой ссылке. Придерживайтесь основных правил безопасной работы, в противном случае, Ваши данные окажутся в руках мошенника [4].

Таким образом, с развитием информационного пространства взрослые и дети должны знать какие потенциальные угрозы могут возникнуть, если они используют сторонние приложения при работе с государственным сайтом. Самое главное – понимание взрослых и детей,

что не все сайты сделаны на сохранение безопасности Ваших данных. Важно проявить бдительность.

Список использованных источников и литературы:

1. Портал государственных услуг Российской Федерации: официальный сайт. – Москва. – URL: https://www.gosuslugi.ru/help/faq/lk/102380 (дата обращения: 19.04.2024).

2. Поддержка протоколов TLS по ГОСТу: официальный сайт по браузеру Яндекс Яндекс Справка. – URL: https://yandex.ru/support/browser-mos/tls/tls.html (дата обращения: 23.04.2024).

3. Олег Галимов, Егор Соловьёв «Екатерина Мизулина заявила о возможной блокировке VPN в 2024 году» – URL: https://www.ural.kp.ru/daily/27562/4887505/ (дата обращения: 23.04.2024).

4. Смирнов, И.А. Цифровая грамотность, как способ защиты в интернете / И.А. Смирнов, Д.А. Козорез, Д.В. Редников // Информационные технологии обеспечения комплексной безопасности в цифровом обществе: сборник материалов VI Всероссийской молодежной научно-практической конференции с международным участием, Уфа, 19-20 мая 2023 года. – № 124. – С. 222-225. (дата обращения: 18.04.2024).

УДК 004

Р.В. Стенькина
Уфимский университет
науки и технологий, Уфа, Россия

Научный руководитель:
И.А. Шагапов
Уфимский университет
науки и технологий, Уфа, Россия

ЗАЩИТА ДЕТЕЙ В ЦИФРОВОМ ПРОСТРАНСТВЕ
PROTECTING CHILDREN IN THE DIGITAL SPACE

Аннотация: В данной статье проводится анализ проблем, связанных с защитой детей в цифровом пространстве. В первой части анализируется влияние интернета и мобильных устройств на подростков и детей, включая возможные угрозы и другие аспекты, которые могут негативно повлиять на их психологическое и физическое благополучие. Во второй части автор предлагает ряд рекомендаций и стратегий по защите детей в онлайн-среде.

Abstract: This article analyzes the problems associated with protecting children in the digital space. The first part analyzes the impact of the Internet

and mobile devices on adolescents and children, including possible threats and other aspects that can negatively affect their psychological and physical well-being. In the second part, the author offers a number of recommendations and strategies for protecting children in the online environment.

Ключевые слова: Киберграмотность, цифровая гигиена, информационная безопасность, веб-пространство, интернет.

Keywords: Cyber literacy, digital hygiene, information security, web space, Internet.

Цифровое пространство – это концепция, описывающая виртуальную среду, которая вышла за рамки физических границ и областей. Это совокупность информационных технологий, интернет-ресурсов, мобильных приложений, социальных сетей и цифровых платформ, где происходят взаимодействия, обмен данными, общение и деятельность пользователей.

Цифровое пространство охватывает все аспекты нашей жизни, связанные с использованием современных технологий, включая работу, образование, развлечения, медиа, социальные взаимодействия и даже финансовые операции. Здесь люди могут искать информацию, общаться, создавать контент, работать в онлайн-среде, покупать и продавать товары и услуги, участвовать в различных событиях и активностях.

Преимущества цифрового пространства включают доступность информации, глобальное взаимодействие, возможность обучения и развития, а также новые возможности для предпринимательства и инноваций [1]. Однако оно также включает в себя ряд проблем и вызовов, таких как кибербезопасность, защита данных, негативное воздействие соцсетей и дисбаланс информации.

Цифровое пространство продолжает развиваться вместе с технологиями, и его влияние на человеческую жизнь продолжает расти и меняться.

В настоящее время в России действует федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию», который направлен на защиту детей от травмирующих воздействий на психику негативной информацией. В данном законе нету упоминания прямых методов или рекомендаций для защиты детей в цифровом пространстве. Однако, он содержит общие положения о необходимости защиты детей от вредной информации, включая информацию, распространяемую через интернет.

Это значит, что родители и опекуны должны принимать дополнительные меры для обеспечения безопасности детей в цифровом пространстве, используя различные инструменты и методы, такие как

фильтрация контента, использование программного обеспечения для родительского контроля, обучение детей правилам безопасного поведения в интернете и т.д.

Для защиты в онлайн-среде детям важно следовать нескольким ключевым правилам и рекомендациям:

1. Не разглашать личные данные: Научите детей сохранять конфиденциальность своих личных данных в интернете, включая имя, адрес, номер телефона, школу и другие личные сведения.

2. Осмотрительность в общении: Учите детей быть осторожными в общении с незнакомыми людьми онлайн. Помогите им понять, что некоторые люди в сети могут быть недобросовестными и им не следует разглашать личные данные или доверять им.

3. Правила безопасности при использовании социальных сетей: Поговорите с детьми о правилах безопасности в социальных медиа, включая организацию приватных профилей, ограничение доступа к личной информации и обучение о блокировке и сообщении об опасных встречах в интернете.

4. Осторожность с контентом: Есть необходимость рассказать детям, что им следует быть бдительными при просмотре видео, фотографий и чтении текстов в сети, и что необходимо немедленно сообщать о неподходящем или оскорбительном контенте.

5. Обсуждение онлайн-опасностей: Поговорите с детьми о различных онлайн-опасностях, таких как неприемлемый контент, кибербуллинг, встречи с незнакомцами и мошенничество. Помогите им понять, как правильно реагировать на такие ситуации и куда обращаться за помощью.

Защита детей в цифровом пространстве может быть описана как создание безопасной "песочницы", где дети могут играть и учиться, не подвергаясь серьезным рискам или опасностям. Как и в обычной песочнице, где дети играют с песком, они взаимодействуют с окружающей средой, который может содержать микробы. Хотя это может быть рискованно, игра в песочнице помогает детям развивать навыки решения проблем и критическое мышление. Однако, если предпринять соответствующие меры предосторожности и обучить детей правилам безопасного поведения, эти риски можно свести к минимуму.

Позволяя детям делать маленькие ошибки в контролируемой среде, они могут научиться распознавать потенциальные опасности и развить навыки критического мышления. Это поможет им стать более осведомленными и осторожными при использовании интернета в будущем.

Сотрудничество между родителями, школами, правоохранительными органами и технологическими компаниями играет ключевую роль в

обеспечении безопасности и благополучия детей в онлайн-среде по многим причинам [2].

Сотрудничество позволяет обмениваться информацией об актуальных тенденциях и угрозах в интернет-пространстве, а также делиться полезными ресурсами и методиками обучения детей о безопасном поведении в сети. Совместные усилия позволяют создавать эффективные образовательные программы по кибербезопасности, которые могут быть внедрены в школьные учебные планы и семейное обучение.

Родители, педагоги и руководители школ могут получать консультации и ресурсы от правоохранительных органов и технологических компаний для разработки стратегий обеспечения безопасности детей.

Сотрудничество с правоохранительными органами позволяет создавать и улучшать законы и стандарты в области безопасности детей в онлайн-среде [3].

Совместное взаимодействие с технологическими компаниями способствует разработке и внедрению новых инструментов и технических решений для защиты детей в онлайн-среде, таких как фильтры, контроль доступа и мониторинг активности.

Эти формы сотрудничества помогают создать более эффективные стратегии и меры по обеспечению безопасности и благополучия детей в цифровом пространстве, что выходит за рамки индивидуального усилия и обеспечивает всеобъемлющий и комплексный подход к проблемам в онлайн-мире.

Список использованных источников:

1. Белоус, А.И. Основы кибербезопасности. Стандарты, концепции, методы и средства обеспечения: учебник / А.И. Белоус. – М.: Техносфера, 2021. – 483 с.

2. Городнова, А.А. Развитие информационного общества: учебник и практикум для академического бакалавриата / А.А. Городнова. – М.: Юрайт, 2019. – 243 с.

3. Гуриков, С.Р. Интернет-технологии: учебное пособие / С.Р. Гуриков. – М.: ФОРУМ: ИНФРА-М, 2019. – 184 с.

СЕКЦИЯ 6. ОБЕСПЕЧЕНИЕ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ ИНФОРМАЦИОННЫХ ВОЙН

УДК 004.056.53

Д.Ю. Гаврилов
Уфимский университет
науки и технологий, Уфа, Россия

Научный руководитель:
Н.В. Кучкарова
Уфимский университет
науки и технологий, Уфа, Россия

ИСКУССТВЕННОЕ ЗАНИЖЕНИЕ КАТЕГОРИИ ЗНАЧИМОСТИ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ – УГРОЗА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СТРАНЫ
MALICIOUS DOWNPLAYING OF CRITICAL INFORMATION INFRASTRUCTURE OBJECT CATEGORIES – A LOOMING THREAT TO NATIONAL CYBERSECURITY

Аннотация: В статье рассматривается необходимость усовершенствования процесса категорирования объектов КИИ, с целью исключения возможности намеренного занижения категории значимости и, соответственно, подвержения угрозе национальной безопасности.

Abstract: The article discusses the need to improve the process of categorizing Critical Information Infrastructure objects in order to eliminate the possibility of intentionally lowering their significance category and, consequently, exposing national security to threats.

Ключевые слова: Информационная безопасность, информационная война, критическая информационная инфраструктура, категорирование объектов критической информационной инфраструктуры, национальная безопасность.

Keywords: Information Security, Information Warfare, Critical Information Infrastructure, Critical Information Infrastructure Object Categorization, National Security.

В современном мире информация становится более ценным ресурсом и критическая информационная инфраструктура играет ключевую роль в обеспечении национальной безопасности. КИИ охватывает широкий спектр систем и объектов, которые являются жизненно важными для

функционирования общества и экономики страны, и их уязвимость перед кибератаками представляет серьезную угрозу национальной безопасности.

Понимание уязвимостей КИИ РФ имеет стратегическое значение для обеспечения национальной безопасности. В условиях текущей геополитической ситуации обеспечение безопасности объектов КИИ особенно актуально, в связи с необходимостью предотвращения влияния зарубежных стран.

Одной из проблем в сфере защиты КИИ является занижение категории значимости объектов. Это происходит по ряду причин, в том числе из-за недостаточной осведомленности субъектов КИИ о требованиях законодательства, желания снизить расходы на обеспечение безопасности.

Заниженная категория значимости объекта КИИ может иметь серьезные последствия. Самыми важными можно выделить:

1. Объект КИИ, отнесенный к более низкой категории, автоматически получает менее строгие требования к защите, что означает, что для него могут применяться менее совершенные методы защиты, устанавливаться менее стойкое к взломам оборудование и программное обеспечение, а также осуществляться менее тщательный контроль за системами безопасности.

2. Значимые объекты КИИ играют критическую роль в функционировании страны, и в случае занижения категории значимости таких объектов, повышается вероятность реализации кибератак, что может привести к катастрофическим последствиям функционирования общества и страны.

В условиях информационных войн рассматриваемая проблема может быть использована противником для нанесения значительного ущерба государству. Для решения проблемы можно предпринять следующие меры:

1. Усовершенствовать методику категорирования объектов КИИ: обязать субъекты КИИ включать в комиссию по категорированию независимых экспертов, что снизит заинтересованность участников комиссии в экономии и обеспечит более объективную оценку. Также привлечение независимых экспертов позволит предотвратить превращение мероприятий «внутреннего аудита» в формальность и обеспечит в полной мере выполнение мероприятий «внешнего аудита» (меры АУД. 10 и 11 приказа ФСТЭК России №239 [2]).

Также возможно сокращение максимально допустимого срока категорирования объектов КИИ с 1 года [3], за счет чего будет быстрее вноситься информация об объектах КИИ и применяться более адекватные

меры по их защите. Также это позволит снизить расходы субъектов КИИ на процедуру категорирования.

2. Проблема неосведомленности организаций о важности обеспечения безопасности КИИ можно решить проведением семинаров и конференций по вопросам категорирования объектов КИИ и обеспечения их безопасности. На них необходимо разъяснять, что возможный ущерб может оказаться больше суммы, сэкономленной на мерах защиты, а также разъяснять возможные административные и уголовные последствия.

3. Усилить государственный контроль в области КИИ: согласно Постановлению Правительства Российской Федерации №162 [4] срок плановых проверок ФСТЭК России равен трем годам, но при уменьши его, можно решить проблему не обновлении информация об объектах КИИ [6]. Также ужесточить [5] наказания за предоставление неверной информации о категории значимости объектах предусмотренные статьей 274.1. УК РФ [1].

В заключение можно сказать следующее: обеспечение защиты объектов КИИ является одним из важнейших направлений обеспечения национальной безопасности в условиях информационных войн. Для решения проблемы преднамеренного занижения категории значимости объектов КИИ требуется комплексный подход с участием и государства, и организаций.

Список использованных источников:

1. «Статья 274.1. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации» / [Электронный ресурс] // ИПО ГАРАНТ: [сайт] – URL: https://base.garant.ru/10108000/d441471697df2f4643c064f927a5f9f4/ (дата обращения: 25.05.2024).

2. Приказ ФСТЭК России от 25 декабря 2017 г. N 239/ [Электронный ресурс] // ФСТЭК России: [сайт] – https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-25-dekabrya-2017-g-n-239?ysclid=lvmkxrsvsq827850945 (дата обращения: 25.05.2024).

3. «Постановление Правительства Российской Федерации от 8 февраля 2018 г. №127» / [Электронный ресурс] // ФСТЭК России: [сайт] – URL: https://fstec.ru/dokumenty/vse-dokumenty/postanovleniya/postanovlenie-pravitelstva-rossijskoj-federatsii-ot-8-fevralya-2018-g-n-127?ysclid=lvmen9qxkh367816904 (дата обращения: 25.05.2024).

4. «Постановление Правительства Российской Федерации от 17 февраля 2018 г. №162» / [Электронный ресурс] // ФСТЭК России: [сайт] – URL: https://fstec.ru/dokumenty/vse-dokumenty/postanovleniya/postanovlenie -pravitelstva-rossijskoj-federatsii-ot-

17-fevralya-2018-g-n-162?ysclid=lvmj49p 8kn712550415 (дата обращения: 25.05.2024).

5. «С проблемой негласного умышленного «занижения» категории значимости объектов КИИ будут бороться на законодательном уровне» / [Электронный ресурс] // BIS JOURNAL: [сайт] – URL: https://ib-bank.ru/bisjournal/news/17667?ysclid=lvmedrsxw7887228402 (дата обращения: 25.05.2024).

6. «ФСТЭК: закон о защите критической инфраструктуры выполняется плохо, подключена прокуратура, усиливаются проверки» / [Электронный ресурс] // TADVISER : [сайт] – URL: https: // www.tadviser.ru/index.php/Статья:Безопасность_критической_информационной_инфраструктуры_РФ?ysclid=lvmev0gukj745315142 (дата обращения: 25.05.2024).

УДК 004.5

В.С. Кириллов
Уфимский университет
науки и технологий, Уфа, Россия

Научный руководитель:
Н.Г. Миронова
Уфимский университет
науки и технологий, Уфа, Россия

О СТРАТЕГИЯХ ПРОТИВОДЕЙСТВИЯ РФ ИНФОРМАЦИОННОЙ ВОЙНЕ
ON STRATEGIES TO COUNTER INFORMATION WAR

Аннотация: Сделан обзор направлений концептуальной деятельности по противодействию информационной войны в РФ. Предложены некоторые меры общего характера в этой сфере.

Abstract: A review of the directions of conceptual activities to counter information warfare in the Russian Federation is made. Some general measures in this area have been proposed.

Ключевые слова: Информационная война, кибербезопасность, национальная безопасность.

Keywords: Information war, cybersecurity, national security.

Информационные технологии с момента своего появления используются как инструмент ведения информационного противоборства

в информационной сфере и средствах массовой информации, а также для достижения различных политических целей. В распространения ИТ-технологий реализуются все новые угрозы национальной безопасности. Страны достаточно давно следуют своим военным кибер-доктринам и используют кибервойска, военные ведомства и спецслужбы, научно-исследовательские центры для информационного воздействия на коллективное сознание и информационную инфраструктуру противника как до активной вооруженной фазы военных действий, так и во время и вместо «горячей фазы» борьбы. Информационная война, ведущаяся против России в интернете, направлена, в частности, на разрушение традиционных ценностей и культурного кода (и внедрение новых символов, ценностей, моделей массового поведения для «перепрограммирования» мировоззрения и хаотизации социального взаимодействия), на дезинформацию населения и лиц, принимающих политические и экономические решения; продвижение иностранных агентов влияния, популяризация вредоносных идей и концепций; принуждение и навязывание принятия решений, выгодных противнику; подрыв доверия населений к национальным институтам власти; масштабные информационные кампании и спецоперации по подготовке революционных ситуаций и протестной деятельности; информационное зашумление и переключение внимания, отвлечение масс населения от полезной деятельности и пустое «сетевое бродяжничество»; сбор информации о пользователях интернета для усиления целевого воздействия на группы в дальнейшем; снижение способности государства возможности проводить самостоятельную информационную политику в национальном сегменте интернета. Интернет стал поистине «оружием массового поражения».

Арсенал методов информационного воздействия и противодействия обширен (разведка, кибершпионаж, пропаганда через СМИ и иные формы воздействия, кибератаки на инфраструктуру противника, создание альтернативных каналов воздействия электронной информационной среды – и их разрушение, блокирования информационной среды противника, террористические акты (в т.ч. с задействованием киберсферы)) [1]. Информационные войны между государствами ведутся в таких областях, как политика (манипуляция общественным мнением, дезинформация, нарушение работы ГИС), экономика (нарушение работы финансовых систем, АСУ, кража интеллектуальной собственности, промышленный шпионаж, устранение ученых), социальная сфера (разжигание социальной вражды и панических настроений, распространение экстремистских идей), военно-техническое противостояние (в т.ч. нарушение работы систем управления войсками, дезинформирование о военных действиях, кибератаки на военные и

социальные объекты). В последние годы активно применяются гибридные методы борьбы (политические, экономических целей с минимальным силовым воздействием на противника, с использованием подрывной деятельности в отношении военного и экономического потенциала) [2], чья эффективность поддерживается широким перечнем IT-технологий.

Обеспечение национальной безопасности в РФ–регулируется рядом законодательных актов и стратегических документов, среди которых: 149-ФЗ «Об информации, информационных технологиях и о защите информации» от 27.07.2006; Доктрина информационной безопасности Российской Федерации (утв. Указом Президента РФ от 5 декабря 2016 г. № 646), Стратегия национальной безопасности Российской Федерации (утв. Указом Президента РФ от 2 июля 2021 г. № 400), 390-ФЗ «О безопасности» от 28.12.2010. Эти документы регулируют такие аспекты безопасности, как ответственность за распространение ложной информации, защиту ГИС и объектов КИИ РФ, деятельность российских СМИ. Действуют уполномоченные органы и структуры (СовБез РФ, СВР, ФСБ и НКЦКИ, ФСТЭК, РКН, Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций), осуществляющие разработку и реализацию государственной политики в области национальной безопасности, координацию деятельности других органов власти в этой области, мониторинг и анализ информационных угроз.

Россия применяет арсенал технических средств и методы для противоборства в информационной сфере, направленный на обнаружение и предотвращение кибератак, на защиту информационной инфраструктуры органов госуправления и жизнеобеспечения, мониторинг и анализ информационных потоков в интернете и т.п. [2]. Тем не менее есть ряд направлений совершенствования и обеспечения национальной безопасности в условиях информационной войны:

1. Дальнейшее совершенствование законодательства: разработка и принятие новых законов, регулирующих информационные отношения, а также внесение изменений в существующие нормативные акты, в частности, по защите критической информационной инфраструктуры, противодействию распространению недостоверной информации.
2. Системная работа в интернет-пространстве, создание суверенного аналога интернету (как это делается, например, в Китае), исключающего саму возможность бесконтрольной антироссийской и экстремистской пропаганды и информационных операций против России.
3. Усиление контроля за распространением информации: механизмов контроля за распространением информации, которые позволят предотвратить распространение ложной и вредной информации.

4. Разработка и внедрение целостной системы обеспечения кибербезопасности ГИС (в т.ч. антивирусного ПО, системы обнаружения и предотвращения вторжений, систем резервного копирования данных).

5. Более активное проведение научных исследований по созданию эффективных методов и технологий защиты информации.

6. Всестороннее повышение информационной осведомленности и грамотности населения, чтобы лучше понимать информационные угрозы и способы противодействия.

7. Государство должно в целом прилагать больше усилий по повышению доверия населения к своим действиям, должно вести более активную работу по выявлению и противодействию вредоносному воздействию на массовое сознание (в частности на молодежь, другие социально активные группы населения группы) ложных, разрушительных, экстремистских идеологий. Стране нужна своя целостная объединяющая общество концепция развития, остро необходимо продвижение своих национальных исторических задач (вместо перманентного «ценностного переключения» и следованиями за чужими и чуждыми идеологиями, транслируемыми через сетевое информационное пространство).

Список использованных источников:

1. Миронова, Н.Г. Арсенал технологий и методов информационного противодействия / Н.Г. Миронова // Актуальные аспекты развития науки и общества в эпоху цифровой трансформации: сборник материалов V международной научно-практической конференции (шифр – МКАА), Москва, 27 февраля 2023 года. – Москва: Общество с ограниченной ответственностью "Издательство АЛЕФ", 2023. – С. 120-128. – URL: https://www.elibrary.ru/item.asp?id=50382855 (дата обращения: 02.04.2024).

2. Шабанов, А.Г. Готовность к информационному противоборству в условиях современной гибридной войны / А.Г. Шабанов, А.Л. Снигерев, А.Е. Мазурин // Гуманитарные проблемы военного дела. – 2020. – № 4(25). – С. 11-14. – URL: https://www.elibrary.ru/item.asp?id=45778256 (дата обращения: 02.04.2024).

УДК 004.732.056

Т.Е. Лисина
Уфимский университет
науки и технологий, Уфа, Россия

Научный руководитель:
В.Е. Кладов
Уфимский университет
науки и технологий, Уфа, Россия

РЕАЛИЗАЦИЯ МАНДАТНОГО РАЗГРАНИЧЕНИЯ ДОСТУПА В КОРПОРАТИВНОЙ СЕТИ НА БАЗЕ ЗАЩИЩЕННОЙ ОПЕРАЦИОННОЙ СИСТЕМЫ ASTRA LINUX SPECIAL EDITION
IMPLEMENTATION OF MANDATORY ACCESS CONTROL IN A CORPORATE NETWORK BASED ON THE SECURE OPERATING SYSTEM ASTRA LINUX SPECIAL EDITION

Аннотация: Статья посвящена задаче реализации мандатного разграничения доступа в корпоративной сети с использованием встроенного межсетевого экрана защищенной операционной системы Astra Linux Special Edition.

Abstract: The article is devoted to the task of implementing mandatory access control in a corporate network using the built-in firewall of the secure operating system Astra Linux Special Edition.

Ключевые слова: Межсетевой экран (МЭ), мандатное разграничение доступа, классификационные метки, защищенные операционные системы.

Keywords: Firewall, mandatory access control, classification labels, secure operating systems.

Обязательным требованиям для реализации информационных систем повышенного уровня защищенности, в частности защиты информации, составляющей государственную тайну, является использование мандатного (полномочного) разграничения доступа. Мандатное разграничение доступа подразумевает использование иерархических уровней конфиденциальности объектов и субъектов и неиерархических категорий конфиденциальности. Уровни конфиденциальности определяют степень секретности объекта или уровня доступа субъекта. А категории конфиденциальности представляются в виде битовой маски, отражающей область использования информации.

В нашей стране наибольшее распространение получила защищенная операционная система (ОС) Astra Linux Special Edition, которая имеет сертификат по наивысшему классу А1 и соответствует первому уровню

доверия. Очевидно, благодаря своему высокому классу она позволяет реализовывать мандатное разграничение доступа. Но построение сложных корпоративных сетей требует взаимодействия отдельных ее сегментов между собой и соответственно возникает задача реализации мандатного разграничения доступа (МРД) и при сетевом взаимодействии.

Остановимся именно на данной задаче. В рассматриваемой защищенной ОС реализация МРД при работе в корпоративной сети достигается за счет подключения создателями ОС в МЭ iptables дополнительно разработанного ими модуля astralabel.

Он в свою очередь включает в свой состав три пакета с суффиксами common, hardened, generic в их названиях, содержащие общее программного обеспечение (ПО) МРД, так и специфическое ПО для двух видов ядер ОС.

В UFW (Uncomplicated Firewall) - упрощенном интерфейсе iptables, также реализуется поддержка МРД и, в частности, меток конфиденциальности.

Для работы с этими пакетами необходимо установить их. Может использоваться Synaptic (графический менеджер пакетов) или следующая терминальная команда:

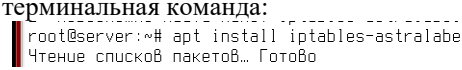

Рисунок 1 – Установка модуля, реализующего МРД для сетевых пакетов

Параметры модуля iptables-astralabel, необходимые для реализации мандатного разграничения доступа в корпоративной сети представим в виде таблицы 1

Таблица 1 – Опции МРД

<table>
<tr><th rowspan="2">Опция</th><th rowspan="2">Вариант применения</th><th colspan="2">Пример</th></tr>
<tr><th>iptables</th><th>ufw</th></tr>
<tr><td rowspan="3">-m astralabel</td><td>Модуль astralabel применяется для реализации МРД при обработке сетевого трафика</td><td colspan="2"></td></tr>
<tr><td rowspan="2">Приложение правил к трафику с меткой конфиденциальности, отличной от нуля</td><td colspan="2">Разрешить отправку пакетов с меткой конфиденциальности, отличной от 0</td></tr>
<tr><td>sudo iptables -A OUTPUT -m astralabel -j ACCEPT</td><td>sudo ufw allow out 80/tcp mac</td></tr>
</table>

Продолжение таблицы 1

Опция	Вариант применения	Пример	
		iptables	ufw
--maclev <уровни конфиденциальности>	Задание правила к трафику с определенным уровнем конфиденциальности.	Запретить отправку трафика с уровнем конфиденциальности 3	
		sudo iptables -A OUTPUT -m astralabel --maclev 3 -j DROP	sudo ufw deny out 80/tcp maclev 3
--maclev <уровни конфиденциальности>	Применение правила к пакетам с указанным через двоеточие диапазоном уровней конфиденциальности	Запретить отправку трафика с уровнями конфиденциальности в диапазоне от 1 до 2	
		sudo iptables -A OUTPUT -m astralabel --maclev 1:2 -j DROP	-
	Применение правила (при наличии символа "!" после astralabel) к пакетам, имеющим иной уровень конфиденциальности по отношению к указанному	Не пропускать входящие пакеты, имеющие уровень конфиденциальности не равный нулю	
		sudo iptables -A INPUT -m astralabel ! --maclev 0 -j DROP	-
--maccat <категории конфиденциальности>	Задание правила к трафику с определенной неиерархической категорией конфиденциальности.	Запретить отправку трафика категории конфиденциальности, соответствующей биту 1	
		sudo iptables -A OUTPUT -m astralabel --maccat 2 -j DROP	sudo ufw deny out 80/tcp maccat 2
	Задание правила для нескольких категорий конфиденциальности трафика.	Запрет приема трафика с категориями конфиденциальности, соответствующими битам 2 и 3	
		sudo iptables -A INPUT -m astralabel --maccat 2 --maccat 3 -j DROP	-
	Задание правила для трафика с определенными категориями и уровнями конфиденциальности .	Запрет отправки трафика уровня конфиденциальности 3 и категориями, соответствующими битам 2 и 3	
		sudo iptables -A OUTPUT -m astralabel --maclev 3 --maccat 2 --maccat 3 -j DROP	-

Примеры правил мандатного разграничения доступа сетевых пакетов для iptables и ufw приведены на рис. 2 и 3

```
root@server:~# iptables -A OUTPUT -m astralabel --maclev 1:2 -j DROP
root@server:~# iptables -A INPUT -m astralabel ! --maclev 0 -j DROP
root@server:~# iptables -A OUTPUT -m astralabel --maclev 3 --maccat 2 --maccat 3 -j DROP
root@server:~# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       all  --  anywhere             anywhere             maclev !0

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
DROP       all  --  anywhere             anywhere             maclev 1:2
DROP       all  --  anywhere             anywhere             maclev 3 maccat 2,3
```

Рисунок 2 – Правила фильтрации с помощью iptables

```
root@server:~# ufw deny out 80/tcp maclev 3
Rule added
Rule added (v6)
root@server:~# ufw deny out 80/tcp maccat 2
Rule added
Rule added (v6)
root@server:~# ufw allow out 80/tcp mac
Rule added
Rule added (v6)
root@server:~# ufw status
Status: active

To                         Action      From
--                         ------      ----
1194/udp                   ALLOW       Anywhere
1194/udp (v6)              ALLOW       Anywhere (v6)

80/tcp                     DENY OUT    Anywhere                   mac maclev 3
80/tcp                     DENY OUT    Anywhere                   mac maccat 2
80/tcp                     ALLOW OUT   Anywhere                   mac
80/tcp (v6)                DENY OUT    Anywhere (v6)              mac maclev 3
80/tcp (v6)                DENY OUT    Anywhere (v6)              mac maccat 2
80/tcp (v6)                ALLOW OUT   Anywhere (v6)              mac
```

Рисунок 3 – Правила фильтрации с помощью ufw

Таким образом, мы рассмотрели реализацию мандатного разграничения доступа при сетевом взаимодействии отдельных сегментов корпоративной сети на базе защищенной операционной системы Astra Linux Special Edition.

Список использованных источников:

1. Операционная система Astra Linux Special Edition РУСБ.10015-01 (обновление 1.7) – Справочный центр Astra Linux – URL: https://wiki.astralinux.ru/pages/viewpage.action?pageId=137563438 (дата обращения: 28.04.2024).

УДК 004.056

М.А. Нигматуллин
Уфимский университет
науки и технологий, Уфа, Россия

Научный руководитель:
Р.М. Яппаров
Уфимский университет
науки и технологий, Уфа, Россия

ИМПОРТОЗАМЕЩЕНИЕ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: СОВРЕМЕННОЕ СОСТОЯНИЕ И ПЕРСПЕКТИВЫ
IMPORT SUBSTITUTION IN THE FIELD OF INFORMATION SECURITY: CURRENT STATE AND PROSPECTS

Аннотация: В статье рассматривается актуальная проблема обеспечения информационной безопасности в России после ухода иностранных вендоров из страны. Выделена важность выбора отечественных решений для защиты каналов связи и передачи информации в условиях, когда иностранные компании больше не обеспечивают техническую и программную поддержку. Рассматривается широкий спектр областей, влияющих на информационную безопасность, включая ПО, сетевые технологии, телекоммуникационное оборудование, продукцию по ИБ, программное обеспечение для предприятий, облачные вычисления, виртуализацию и искусственный интеллект.

Abstract: The article deals with the actual problem of ensuring information security in Russia after the departure of foreign vendors from the country. The importance of choosing domestic solutions for the protection of communication channels and information transmission in conditions when foreign companies no longer provide technical and software support is highlighted. A wide range of areas affecting information security are considered, including software, network technologies, telecommunications equipment, information security products, enterprise software, cloud computing, virtualization and artificial intelligence.

Ключевые слова: Информационная безопасность, вендор, рынок, российские компании, отечественные решения, иностранные решения

Keywords: Information security, vendor, market, Russian companies, domestic solutions, foreign solutions

Одной из важнейших задач в условиях защиты информации является выбор правильного аппаратного или программно-аппаратного решения для обеспечения режима ИБ [5].

После событий 2022 года из России ушли иностранные вендоры, занимавших 80% рынка ИБ России [1], в том числе и решения по защищенному каналу связи. Из-за чего сказывается проблема в защите информации, поскольку иностранные вендоры ушли, то значит и техническая, программная поддержка и обновление исчезли, как и возможность покупки.

Актуальность данной темы заключается в правильном выборе отечественного решения по защите канала связи и передачи информации, как внутри организации, так и при защите связи между филиалами в разных уголках России.

Для начала проанализируем в целом какие критические нужные иностранные вендоры ушли из России и какие решения они предлагали:

1. Вендоры рынка ПО: Microsoft, Oracle, Adobe и прочие.
2. Вендоры сетевых технологий: Cisco, Palo Alto Networks, Juniper Networks и прочие.
3. Вендоры телекоммуникационного оборудования: Huawei, Ericsson, Nokia, ZTE, Ciens, Samsung и прочие.
4. Вендоры предоставляющие продукцию по информационной безопасности: Fortinet, McAfee, Salesforce и прочие.
5. Вендоры программного обеспечения для предприятий: SAP, Oracle, Microsoft и прочие.
6. Вендоры облачных вычислений: IBM, Google, Amazon и прочие.
7. Вендоры виртуализации: Oracle, VMware, Microsoft и прочие.
8. Вендоры искусственного интеллекта: Open Ai, IBM, Google Ai, Microsoft Ai, Amazon Ai и прочие.

Как можно заметить хоть список обозначен не весь и не все сферы охвачены, но все же это уже весомый список, который необходимо преодолеть. Возьмём для примера только сферу ИБ. Для решения данной проблемы правительство в России были запущены несколько решений:

1. В 2021 году запустило национальную программу «Информационная безопасность» в период до 2025 года, с бюджетом 31,4 млрд. руб. Целью проекта было обучение государственных работников информационной безопасности.

2. В 2022 году вышел Указ Президента Российской Федерации от 30.03.2022 № 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации» [2], согласно которому необходимо полностью перейти на отечественное программное и программно-аппаратное решение, что позволило стимулировать развитие и отечественных вендоров.

Итогом данных мер стало бурное развитие отечественных вендоров.

Возьмём в пример компанию АО «ИнфоТеКС» по годовым отчётам [3]:

1. 2019 год – крупных сделок не было совершено, стоимость активов оценивается в 2 736 328 рублей, прибыль оценивается в 227 млн рублей.
2. 2020 год – крупных сделок не было совершено, стоимость активов оценивается в 3 223 794 рублей, прибыль оценивается в 614 млн рублей.
3. 2021 год – есть крупная сделка на 2,1 млрд руб., стоимость активов оценивается в 4 606 602 рублей (активы сильно выросли по сравнению с предыдущими годами), прибыль оценивается в 2023 млн рублей.

Такой большой рост можно заметить во многих российских компанией, данное высказывание можно подтвердить директора по развитию бизнеса Positive Technologies Максима Филиппова «Хакеры атакуют буквально все: ВПК и ТЭК, госучреждения и банки, СМИ и ИТ-сферу. В этих новых реалиях резко возрос запрос на наши сервисы и продукты. Количество заказов всего за три недели сравнимо с третью заказов за весь прошлый год» [4].

Данные меры привели к следующему:

1. Появился большой рынок отечественных решений по импортозамещению.
2. Качество продукции и уровень предлагаемой защиты вырос.

Так, до событий 2022 года можно было поставить следующие меры защиты: Программно-аппаратные решения Cisco (как компоненты сетевых технологий, так и средства информационной безопасности), Palo Alto Networks, RSA Security и прочие, которые занимали больше половины российского рынка ИБ.

Но сейчас благодаря импортозамещению можем поставить, например, более продвинутую защиту вроде программно-аппаратных комплексов ViPNet (как по защищенному соединению – HW, Coordinator, Administrator-Client), антивирусные решения Касперского, МДЗ от НСД Dallas Lock и многие другие решения. Данные решения сертифицированы от ФСТЭК, ФСБ, Минкомсвязь что даёт большую гарантию защищённости, они законны со стороны регуляторов и их вполне легально можно ставить себе на вооружение, не опасаясь отказа от ответственности и ухода из страны.

В заключение следует сказать, что всего за пару лет в России смогли полностью перейти от иностранных решений ИБ к своим собственным, что означает большой успех в плане отечественной защиты.

Список использованных источников:

1. РБК Компании: официальный сайт – URL: https://companies.rbc.ru/news/UNfgOlPkem/nazvanyi-problemyi-v-oblasti-

informatsionnoj-bezopasnosti-v-2023-godu/?ysclid=luy4fgvy2d964425526 (дата обращения 27.04.2024).

2. Указ Президента Российской Федерации от 30.03.2022 № 166 "О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации".

3. Информационно-аналитическое агентство «Телеком-Дэйли»: официальный сайт – URL: https://telecomdaily.ru/news/2022/04/12/eksperty-iz-rossii-ushli-30-zarubezhnyh-kompaniy-segmenta-ib (дата обращения 27.04.2024).

4. Infotecs.ru: официальный сайт. – URL: https://infotecs.ru /about/shareholders/ (дата обращения 27.04.2024).

5. Янбердин, У.М. Аутентификация пользователей Интернета вещей (IOT) / У.М. Янбердин, Р.М. Яппаров // Прикладные процессы в области информационной безопасности. Тенденции развития методов защиты информации: Материалы научно-практических конференций, Самара, 19-20 октября 2023 года. – Самара: Поволжский государственный университет телекоммуникаций и информатики, 2023. – С. 23-25.

УДК 336.1

Д.А. Козорез, И.А. Смирнов
Уфимский университет
науки и технологий, Уфа, Россия

Научный руководитель:
Б.К. Кушубакова
Уфимский университет
науки и технологий, Уфа, Россия

СУВЕРЕНИТЕТ ПЛАТЕЖНОЙ СИСТЕМЫ НА ОСНОВЕ ЦИФРОВОГО РУБЛЯ И ЕГО ЗНАЧЕНИЕ В ОБЕСПЕЧЕНИЕ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ РОССИИ
THE SOVEREIGNTY OF THE PAYMENT SYSTEM BASED ON THE DIGITAL RUBLE AND ITS IMPORTANCE IN ENSURING RUSSIA'S NATIONAL SECURITY

Аннотация: В статье показано, что суверенитет платежной системы Российской Федерации в последние годы превращается в определяющий фактор ее экономического суверенитета. Также рассмотрены новые возможности, возникающие у Банка России и банков - участников оборота цифрового рубля по контролю над оборотом бюджетных и внебюджетных государственных ресурсов.

Abstract: The article shows that the sovereignty of the payment system of the Russian Federation has been turning into a determining factor of its economic sovereignty in recent years. The new opportunities arising from the Bank of Russia and banks participating in the turnover of the digital ruble to control the turnover of budgetary and extra-budgetary state resources are also considered.

Ключевые слова: Цифровой рубль, национальная безопасность, суверенитет платежной системы, платежная система страны.

Keywords: Digital ruble, national security, sovereignty of the payment system, the country's payment system.

В условиях современной геополитической нестабильности и трансформации международных экономических отношений крайне важно обеспечить экономический суверенитет России. Одним из определяющих элементов экономического суверенитета является суверенитет национальной платежной системы.

С наступлением эпохи цифровизации, а также под влиянием санкционной политики, обычные методы и инструменты регулирования платежной системы стали менее эффективными и более затратными. В связи с этим, с 1 августа 2023 года в России был официально введен цифровой рубль.

Цифровой рубль – это новая форма российской национальной валюты, которая может частично заменить в обороте наличные и безналичные денежные средства. Центральный Банк России является эмитентом и соответственно, главным контролирующим органом, что обеспечивается способом хранения цифровой валюты на специальной платформе.

Предпосылка к выпуску цифровых денег сформирована соотношением объемов обращения наличных и безналичных денежных средств, сложившихся к данному периоду в пользу безналичного денежного оборота. Так, прирост объема наличного оборота денежных средств в 2022 году по сравнению с 2013 годом составил 105,3% (13200 млрд. рублей /6430 млрд. рублей), а прирост объема безналичного оборота денежных средств составил 155,8% (53053 млрд. рублей /20735 млрд. рублей) [2, с. 136]

Как следует из расчета, результаты которого отражены в таблице 1, значителен и прирост доли безналичного денежного оборота. Так, за приведенный в расчетах период доля безналичного денежного оборота с 76,3% увеличилась до 80,1%, что сопровождается соответствующим уменьшением доли наличного денежного оборота.

Таблица 1. Динамика структуры денежного оборота за 2013-2022 гг.*

Годы	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022

Доля безналичного оборота	76,3	77,6	77,3	79,4	79,9	80,1	80,2	81,3	78,6	80,1
Доля наличного оборота	23,7	22,4	22,7	20,6	20,1	19,9	19,8	18,7	21,4	19,9

*Расчет основан на данных из публикаций [2, с. 136]

Главной целью выпуска цифрового рубля является обеспечение суверенитета национальной валюты, что показано на рис. 2 [2].

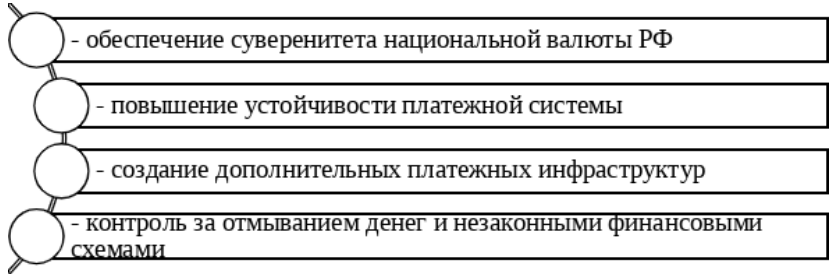

Рисунок 1 – Цели цифрового рубля

В реализации участвует огромное количество банков. Например, Альфа-Банк, Ингосстрах Банк, Банк ВТБ, Банк ГПБ, МТС-банк, Промсвязьбанк, Совкомбанк, Росбанк и многие другие. Стоит отметить, что крупные банки такие как: Сбербанк, Тинькофф, Россельхозбанк и др. [2] планируют присоединится к использованию цифрового рубля, в дальнейшем.

Главная особенность цифрового рубля состоит в том, что каждому рублю будет присвоен свой уникальный код для детального отслеживания и прозрачности операций с денежными средствами.

С помощью внедрения цифрового рубля удастся стабилизировать финансовую систему, так как оборот цифровой валюты повышает прозрачность движения денежных средств, что позволяет оперативно влиять на возникающие угрозы с целью их снижения. В особенности данный момент важен для контроля за миграцией капитала, в частности вывода капитала за пределы России.

Стабилизация финансовой системы при обороте цифровой валюты будет обеспечена и путем усиления прозрачности движения бюджетных средств и оперативного контроля за их оборотом, прежде всего в сфере государственных закупок. Учитывая, что объем государственных закупок составляет львиную долю в расходах бюджета, цифровая валюта существенно усложнит использование средств не по назначению.

Также цифровой рубль снижает риски перетока денег в частные цифровые валюты, эмиссия и обращение которых слабо контролируются или не контролируются вовсе Центральным Банком Российской Федерации, что к создает дополнительные помехи для регулирования денежного обращения.

Расширение возможностей Банка России при использовании цифровой валюты для отслеживания денежных операций как физических лиц, так и юридических лиц расширит доступ к контролю за формированием налогооблагаемой базы, что поможет бороться с отмыванием денег и уводом экономических операций от налогообложения. [1] Получается, что цифровой рубль содержит в себе значительный потенциал выполнения контрольной функции в автоматическом режиме.

Таким образом, цифровой рубль позволит укрепить суверенитет платежной системы РФ и усилить контрольную функцию рубля, что безусловно будет способствовать росту национальной безопасности страны в целом.

Список использованных источников:

1. Долгиева, М.М. Правовой режим международных санкции и цифровой рубль / М.М. Долгиева // Имущественные отношения в Российской Федерации. – 2023. – С. 59-61.

2. Официальный сайт Центрального Банка России: https://cbr.ru/statistics/cash_circulation/20230101/ (дата обращения 27.04.2024).

3. Саадулаева, Т.А. Цифровой рубль как механизм обеспечения финансовой безопасности государства / Т.А. Саадулаева // Экономика и бизнес: теория и практика. – 2022. – С. 135-137.

УДК 004.5

Г.Ф. Хайруллина
Уфимский университет
науки и технологий, Уфа, Россия

Научный руководитель:
Н.Г. Миронова
Уфимский университет
науки и технологий, Уфа, Россия

НЕКОТОРЫЕ АКТУАЛЬНЫЕ НАПРАВЛЕНИЯ ПРОТИВОДЕЙСТВИЯ ВОЙНАМ В ИНФОРМАЦИОННОЙ СФЕРЕ
CURRENT DIRECTIONS OF STRUGGLE IN THE INFORMATION SPHERE OF RUSSIA

Аннотация: Выполнен анализ ряда актуальных направлений противодействия информационной войне в интернет-среде.

Ключевые слова: Кибербезопасность, информационное противоборство

Abstract: An analysis of a number of current areas of countering information warfare in the Internet environment was carried out.

Keywords: Cybersecurity, information warfare.

В условиях глобальной информационной и технологической связанности обострились проблемы безопасности в киберпространстве; IT-технологии и средства коммуникации используются теперь как средство проведения для информационных операций, как часть гибридных войн). Термин «информационная безопасность» трактуется в Доктрине информационной безопасности РФ, других правовых актах и стратегических документах [1] как часть безопасности государства, – не только в информационно-техническом, но в политико-идеологическом и социогуманитарном контексте. В деятельности по социогуманитарному аспекту информационной безопасности в РФ участвуют не только уполномоченные органы власти (такие, как Минцифры, ФСБ, Роскомнадзор, Госдума и др.), но и общественные структуры (например, Лига безопасного интернета) и российские компании (Крибрум и др.).

Еще одно направление усилий по повышению информационной безопасности связано с избавлением России от иностранной технологической зависимости, в т.ч. зависимости от иностранного программного обеспечения, в первую очередь, на объектах критической информационной инфраструктуры [2]. К слову, действует запрет на использование иностранных платформ социальной коммуникации (в целях

снижения рисков утечки информации и усиления контроля и противодействия антироссийской деятельности, были запрещены приложения компании «Meta platforms»* (признана экстремисткой на территории РФ), в т.ч. Facebook, Instagram, Whatsapp). Именно через соцсети и интернет-медиа оттачиваются технологии концептуального перепрограммирования населения, методов социальной инженерии, собирается обширная база данных (цифровые социальные профили и компромат) на людей, которая будет использована спецслужбами иностранных государств позднее). Однако популяризация в РФ доверенных российских аналогов платформ социальной интернет-коммуникации пока слабо реализуется.

Между тем воздействие на массовое сознание в ходе информационной войны оказывается, в первую очередь, через сетевые масс медиа, в т.ч. соцсети. Формы информационной войны в интернет-пространстве и СМИ, направления разрушительного воздействия на общественное создание различны [3]: это антироссийская пропаганда; дискредитация всего российского; дискредитация органов власти, групп населения, общественных организаций и т.п.; вербовка спецслужбами иностранных спецслужб радикально и антисоциально настроенных индивидов и групп для проведения диверсий и т.п.; отвлечение и переключение внимания масс; дезинформирование населения страны; засорение информационного пространства «ложными целями», фейками и пустыми новостями, которые держат в непродуктивном напряжении общественное сознание; создание предпосылок социальной напряженности, разрушение социального доверия, связи и преемственности между социальными группами (между поколениями, гендерами, государством и населением и т.д.) для подрыва продуктивной социально-экономической деятельности в стране в условиях войны; систематическая фальсификации исторической памяти о роли и месте России в мире; создание политической враждебности, направленной на разрыв научных, экономических и культурных связей России с другими странами; размывание российской идентичности, подмена культурного кода чуждыми образчиками; популяризация и навязывание саморазрушительных и асоциальных моделей поведения, в т.ч. в среде подрастающего поколения; подрыв основ мировоззрения и «идеологическая хаотизация» для облегчения внедрения в массовое сознание радикальных и чуждых идеологий. Таким образом, поле деятельности специалистов по защите информационной безопасности (в широком смысле этого понятия) требует большой работы, которая должна идти на всех уровнях, в т.ч. технологическом, идеологическом, мировоззренческом. Тем более, что в среде российских IT-специалистов, реализующих тот самый технологический уровень информационной

безопасности, пока много «людей мира», которые в силу тесного взаимодействия с иностранной IT-продукцией и IT-средой, не берут в расчет российских национальных интересов и не видят рисков безопасности, складывающихся в цифровой среде.

Список использованных источников:

1. Указ Президента РФ от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы».
2. Указ Президента Российской Федерации от 30.03.2022 № 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации».
3. Миронова Н.Г. Арсенал технологий и методов информационного противодействия / Н.Г. Миронова // Актуальные аспекты развития науки и общества в эпоху цифровой трансформации: Сборник материалов V международной научно-практической конференции (27.02.2023). – Москва: ООО Издательство АЛЕФ, 2023. – С. 120-128.

УДК 004.5

И.Р. Якупова
Уфимский университет
науки и технологий, Уфа, Россия

Научный руководитель:
Н.Г. Миронова
Уфимский университет
науки и технологий, Уфа, Россия

О СИСТЕМНОСТИ БОРЬБЫ С ИНФОРМАЦИОННЫМИ ВОЙНАМИ
ABOUT THE SYSTEMICALITY OF COUNTERING INFORMATION WARS

Аннотация: Рассмотрены концептуальные методы противодействия в информационных войнах.

Abstract: Conceptual methods of counteraction in information wars are considered.

Ключевые слова: Информационная безопасность.

Key words: Information security.

Национальная безопасность играет ключевую роль в защите страны от разнообразных угроз, в том числе и информационных. В условиях почти тотальной цифровизации информационные угрозы приобретают высокую сложность и масштабность; арсенал средств информационной борьбы включает в себя помимо шпионажа и пропаганды, планирование спецопераций с использованием и массивов данных «цифровых двойников» социальных групп и объектов; операции в информационном пространстве (отвлечение внимания, мобилизацию агентов влияния через социальные сети, выведение из строя цифровых систем, изощренные кибератаки на критическую инфраструктуру противника и т.д.). Противостояние таким угрозам требует комплексного подхода, в т.ч. разработки и внедрения передовых технологических решений, укрепления правовой базы, повышения осведомленности и защиты населения. Информационные войны, используя цифровые каналы для разрушительной и подрывной работы по переформатированию ментальности, созданию негативного образа социальных групп и целых стран, для проведения кибератак и специопераций, не уступают сейчас по разрушительным последствиям традиционным войнам (и являются подготовительной фазой «горячей» войны) [2]. При этом в разрушение экономики и социальной инфраструктуры противником благодаря IT-техногиям и интернету вовлечено в качестве орудия и само население атакуемых государств. Государства, реализующие свои стратегии в сфере управления информацией, институтами и инфраструктурой кибербезопасности, успешнее справляются с вызовами информационных войн, защищая суверенитет и стабильность, – если делают это активно, системно и исходят из национальных интересов (а не следуют за чужой инициативой или чужой идеологической «повесткой»). Не только государства контролируют сферу информации и коммуникаций (посредством своих органов и учреждений), но и корпоративные структуры, общественные группы в борьбе за свои интересы – объект и субъект информационных процессов (и могут привлекаться для обеспечения защиты информационного пространства).

Эффективное противодействие информационным операциям требует комплексного подхода, продуманной стратегии информационной безопасности на государственном уровне, - и предполагает применение методов раннего распознания враждебного и разрушительно информационного воздействия, разработку новых методов борьбы с информационными атаками на инфраструктуру страны и на коллективное сознание (в т.ч. своевременную и системную борьбу с фейками, враждебной пропагандой, кибер-атаками), глубокую идеологическую работу в целях укрепления общественной стабильности, единства и социальной «мобилизации» общества. Требуется не спорадическое

реагирование на деструктивные внешние воздействия госструктур, отвечающих за информационную безопасность, – а выработка собственной проактивной стратегии в информационной сфере, что предполагает систематическую работу про анализу, прогнозированию и предупреждению информационных угроз, слаженную работу государственных и общественных структур, наличие системы контроля (и реагирования) за разрушительными «активностями» в цифровой среде (интернете) и СМИ, в околонаучной и околокультурной средах (указанные среды являются проводником и орудием информационного воздействия на массовое сознание, в т.ч. на сознание лиц, принимающих решения). Защита информационной безопасности страны включает в себя широкий спектр правовых, организационных, технических подходов и методов [1]. Правовые и организационные аспекты включают в себя разработку стратегий, законов и политик для регулирования области информационной безопасности, повышение уровня осведомленности граждан и специалистов об актуальных угрозах и способах их предотвращения. Технические меры противодействия информационным атакам состоят в применении эффективных средств защиты информации, мониторинге и реагировании на киберугрозы в реальном времени, противодействии утечкам важной и конфиденциальной информации, защиту каналов передачи информации, суверенный интернет; отключение по решению суда узлов и сайтов, которые занимаются экстремистской пропагандой или несут киберугрозы широкому кругу пользователей сети. Области повышения государственной информационной безопасности: развитие новых видов войск (под стать новым видам войн), специализирующихся на информационных операциях и инфоборьбе; совершенствование законодательной базы, инструментов регулирования информационного пространства; включение в учебные планы курсов, знакомящих с методами информационного воздействия и о цифровой безопасности в сети интернет; скоординированная системная работа госструктур и общественных объединений по контролю за информационным пространством; своевременное реагирование на инфоатаки.

Список использованных источников:

1. Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // Справочная система КонсультантПлюс.

2. Миронова, Н.Г. Арсенал технологий и методов информационного противодействия / Н.Г. Миронова // Актуальные аспекты развития науки и общества в эпоху цифровой трансформации: сборник материалов V международной научно-практической конференции (шифр – МКАА), Москва, 27 февраля 2023 года. – Москва: Общество с ограниченной ответственностью "Издательство АЛЕФ", 2023. – С. 120-128.

При подготовке электронного издания использовались следующие программные средства:

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

Научное издание

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ ОБЕСПЕЧЕНИЯ КОМПЛЕКСНОЙ БЕЗОПАСНОСТИ В ЦИФРОВОМ ОБЩЕСТВЕ

Сборник материалов
VII Всероссийской молодежной научно-практической конференции с международным участием
(г. Уфа, 24 – 25 мая 2024 г.)

Электронное издание сетевого доступа

За достоверность информации, изложенной в статьях, ответственность несут авторы.
Статьи публикуются в авторской редакции

Подписано к использованию 15.10.2024 г.
Гарнитура «Times New Roman». Объем 9,12 Мб.
Заказ 131.

ФГБОУ ВО «Уфимский университет науки и технологий»
450008, Башкортостан, г. Уфа, ул. Карла Маркса, 12.

Тел.: +7-908-35-05-007
e-mail: ric-bdu@yandex.ru