УФИМСКИЙ УНИВЕРСИТЕТ

приоритет2030^
лидерами становятся

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ ОБЕСПЕЧЕНИЯ КОМПЛЕКСНОЙ БЕЗОПАСНОСТИ В ЦИФРОВОМ ОБЩЕСТВЕ

Материалы IX Всероссийской молодежной научно-практической конференции с международным участием (г. Уфа, 22–23 мая 2026 г.)



Министерство науки и высшего образования РФ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Уфимский университет науки и технологий»

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ ОБЕСПЕЧЕНИЯ КОМПЛЕКСНОЙ БЕЗОПАСНОСТИ В ЦИФРОВОМ ОБЩЕСТВЕ

Материалы
IX Всероссийской молодежной научно-практической конференции с международным участием
(г. Уфа, 22–23 мая 2026 г.)

Научное электронное издание сетевого доступа

Уфа
Уфимский университет
2026

УДК 004.056
ББК 16.8
И74

Публикуется по решению кафедры управления информационной безопасностью УУНиТ. Протокол № 10 от 27.05.2026 г.

Редакционная коллегия:
канд. физ.-мат. наук **Д. С. Юнусова** (*отв. редактор*);
д-р физ.-мат. наук, доцент **А. С. Исмагилова**;
д-р техн. наук, профессор **М. Б. Гузаиров**;
д-р техн. наук, профессор **С. С. Валеев**;
канд. физ.-мат. наук, доцент **И. А. Шагапов**;
канд. юрид. наук, доцент **Р. М. Яппаров**;
канд. филос. наук **Н. Г. Миронова**;
ст. преподаватель **И. В. Салов**;
ст. преподаватель **А. Ф. Фатхелисламов**

И74 **Информационные технологии обеспечения комплексной безопасности в цифровом обществе**: материалы IX Всероссийской молодежной научно-практической конференции с международным участием (г. Уфа, 22–23 мая 2026 года) / отв. ред. Д. С. Юнусова [Электронный ресурс] / Уфимск. ун-т науки и технологий. – Уфа: Уфимский университет, 2026. – 476 с. – URL: https://uust.ru/media/documents/digital-publications/2026/222.pdf – Загл. с титула экрана.
ISBN 978-5-7477-6456-9

Представлены статьи, подготовленные в рамках основных направлений работы конференции: математические модели и методы обеспечения безопасности информации; искусственный интеллект в кибербезопасности; организационно-правовые аспекты защиты информации; концепция и методы инженерно-технического обеспечения безопасности; современные вызовы в области компьютерной безопасности.

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

УДК 004.056
ББК 16.8

ISBN 978-5-7477-6456-9 © Уфимский университет, 2026

СОДЕРЖАНИЕ

ПЛЕНАРНЫЕ ДОКЛАДЫ И ВЫСТУПЛЕНИЯ ЭКСПЕРТОВ

Бугаенко О.Д. Квантовая криптография в университетском курсе информационной безопасности: подходы и методы 12

Валеев С.С., Гузаиров М.Б. Автоматическое обнаружение аномалий в многомерных временных рядах 16

Валеев С.С., Гузаиров М.Б., Яппаров Р.М. Искусственный интеллект и кибербезопасность 20

Волошин Д.Г. Метод квазиавтономной навигации БПЛА легкого класса и формирования защищенной траектории полета в условиях активного спуфинга 25

Гусева Т.М. Тенденции развития искусственного интеллекта в кибербезопасности 30

Иконников С.Н., Шкляр Е.В. Метод идентификации пользователей по изображению лица с подсистемой пассивного обнаружения атак на биометрическое предъявление на базе Raspberry Pi 5 34

Исмагилова А.С. Модульная архитектура криптосистемы на основе ортогональных идемпотентов 39

Корнилова А.А., Гиззатова Э.Р. Аппроксимация нелинейных процессов киберугроз методами символьной регрессии 43

Лушников Н.Д., Исмагилова А.С. Перспективы применения инновационных программно-аппаратных комплексов в цифровом обществе 47

Мхитарян А.С. Актуальные средства обеспечения сохранности персональных данных работников в киберсреде 52

Салов И.В., Шагапов И.А. Идентификация человека по косвенным признакам 56

Сенцова А.Ю. Основные тенденции в области информационной безопасности 2026 года 60

Фатхелисламов А.Ф. Идентификация и мониторинг устройств через беспроводные интерфейсы 64

Шагапов И.А., Салов И.В. Непрерывность и точки разрыва в защите информации 68

Яковец Е.Н. Служебные сведения ограниченного распространения или служебная тайна? 71

Яппаров Р.М. Совершенствование системы технической защиты информации в организации 76

СЕКЦИЯ 1. МАТЕМАТИЧЕСКИЕ МОДЕЛИ И МЕТОДЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Гаврилова А.А. Визуализация угроз безопасности информации с использованием Quantickle (на примере УБИ.223)..... 81

Горяйнов С.А., Дибров Н. Метод координации роя БПЛА с передачей доверия по транзитивным цепочкам в условиях ограниченной связности 85

Долотов И.А., Кондратов М.С. Применение модели «хищник – жертва» при решении задач по отражению кибератак 89

Долотов И.А., Кондратов М.С. Об использовании модели «хищник-жертва» в решении задач по отражению кибератак..... 92

Еремина Л.А. Сравнительный анализ методов машинного обучения для обнаружения аномалий в протоколе Modbus/TCP промышленного интернета вещей 96

Жигальцова Е.А., Чижевский И.А. Адаптация типовой модели массового обслуживания для анализа отказоустойчивых систем обработки заявок в критической информационной инфраструктуре 100

Занин Д.С. Метод обеспечения семантической безопасности распределенных программных систем на основе интеллектуального семантического иммунитета..... 104

Занин Д.С. Модель интеллектуальной семантической безопасности распределенных программных систем и оценка ее эффективности по системным свойствам 107

Занин Н.С. Формальная модель распределенного кибериммунитета ECU-приложений в AUTOSAR Adaptive 111

Занин Н.С. Метод распределенной иммунной защиты ECU-приложений в AUTOSAR Adaptive на основе клеточных автоматов..... 115

Крыжановский А.Д. Разработка инструмента для интеллектуального анализа сетевого трафика 119

Лаптев Т.О., Рыцева К.В. Моделирование и идентификация параметров процесса авторегрессии первого порядка при наличии шума измерений для задач обнаружения аномалий сетевого трафика..... 123

Неборачек К.А., Диканский Д.А. Метод прогнозирования отказов межагентной коммуникации для устойчивой координации в децентрализованных киберфизических системах 127

Ожгибесова А.С. Метод оценки живучести информационных систем на основе нечетких когнитивных карт..... 132

Осипов И.В., Григорьев Д.А. Имитационное моделирование отказоустойчивой системы обработки заявок с резервированием в AnyLogic 136

Ощепков Н.В. Модель и количественная оценка механизма верификации отправителя в протоколе Modbus RTU 141

СЕКЦИЯ 2. ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В КИБЕРБЕЗОПАСНОСТИ

Аминев Б.Р., Хайсаров Р.И. Гибридная модель на основе BERT и графовой нейронной сети (GAT) для обнаружения угроз в текстовых отчетах..... 145

Бадамшин И.В., Яикбаев А.А. Сравнительный анализ эффективности методов машинного обучения для обнаружения сетевых атак..... 149

Баязитов Т.Т. О возможности перехвата ПЭМИН видеоинтерфейсов и реставрации изображении 153

Биглова М.Р. Разработка алгоритмов выявления признаков социальной инженерии на основе методов интеллектуального анализа текста 157

Бурангулов Д.Б., Куликова В.Е. Интерпретируемая оценка когнитивной манипуляции в социальной инженерии..... 161

Галимова А.Р. Глубокие нейронные сети. Применение в системах корпоративной защиты программного обеспечения..... 165

Диканский Д.А., Пронин В.И. Метод адаптивного взвешивания голосов в распределенных системах обнаружения вторжений в интернете дронов 169

Журавлева Ю.О., Шамсутдинова А.А. Применение методов машинного обучения для определения спам-писем 174

Иванов Д.К. Обнаружение аномалий в сетевом трафике с использованием изолирующего леса (Isolation Forest) без размеченных данных 177

Клыгин В.О. Применение систем искусственного интеллекта при обучении персонала основам информационной безопасности 181

Ларичев Р.С. LLM-ассистент для Threat Hunting 185

Мансурова А.Р. Применение рекуррентных нейронных сетей в системе корпоративной защиты 189

Митянин К.А., Пицин К.С. Использование искусственного интеллекта в кибербезопасности 193

Насртдинов А.С. Использование искусственного интеллекта для прогнозирования угроз безопасности: опыт внедрения прогнозных моделей в корпоративной среде 197

Попов С.И., Дончик С.А. Искусственный интеллект в киберпреступлениях: угрозы, возможности и меры защиты 201

Сунь Хаожань Адаптивный алгоритм кластеризации для БПЛА на основе обучения с подкреплением 205

Сысоева А.В. Применение сверточных нейронных сетей в системе корпоративной защиты 209

Чуркин П.Ю. Искусственный интеллект в кибербезопасности в 2026 году: как ИИ одновременно ускоряет атаки и укрепляет оборону 212

Шамин Т.С. Методы обнаружения и подавления атак нулевого дня (Zero-Day) в корпоративных сетях с использованием поведенческого анализа 216

Шигапов А.В. Идентификация фишинговых ресурсов в интернете на основе технологий машинного обучения 221

Якупов Я.Г. Персонализация обучения с использованием технологий искусственного интеллекта: концептуальные основы и образовательный потенциал 224

СЕКЦИЯ 3. ОРГАНИЗАЦИОННО-ПРАВОВЫЕ АСПЕКТЫ ЗАЩИТЫ ИНФОРМАЦИИ

Аввакумов А.В. Проблематика применения 152-ФЗ в судебной власти Российской Федерации в аспекте информационной безопасности 229

Александрова В.М. Совершенствование системы защиты информации в правоохранительных органах: анализ угроз и направления развития 232

Аскарова Г.Ф. Анализ процесса управления уязвимостями на примере деятельности органов внутренних дел 237

Баянов К.А. Парадокс формальной защищенности: правовые риски реализации требований ФСТЭК россии в государственных учреждениях 241

Биктубаева К.С. Организационно-правовые аспекты обеспечения информационной безопасности в ЦИК Республики Башкортостан с учетом новых требований ФСТЭК России 246

Гаврилова А.А. К вопросу о совершенствовании механизмов защиты персональных данных 250

Еремина Л.А. Совершенствование нормативно-правового регулирования обеспечения информационной безопасности в сети Интернет 255

Журавлева Ю.О., Шамсутдинова А.А. Роль информационной безопасности в обеспечении национальной безопасности Российской Федерации 259

Зайнуллин Б.З. Автоматизированная система оценки критичности уязвимостей в соответствии с методикой ФСТЭК России от 30 июня 2025 года 262

Ижболдина Т.К. Организационно-правовые аспекты защиты информации ГИС отдела ЗАГС Республики Башкортостан по делам юстиции 267

Иркина Ю.Р. Системы оповещения населения как объект информационной защиты 271

Кунавина О.А. Обеспечение безопасности биометрических персональных данных 276

Лаптева Е.А. Адаптация процессного подхода к ИБ медицинских информационных систем 280

Максютов Т.М. Анализ актуальных нормативно-правовых актов в области защиты информации на объектах критической информационной инфраструктуры 283

Моисеева К.А. Анализ нормативных изменений в сфере безопасности критической информационной инфраструктуры 288

Набиева А.И. Совершенствование системы защиты информации в органе местного самоуправления 292

Резбаева В.М. Правовые аспекты внедрения DLP-систем: баланс между информационной безопасностью и тайной связи 297

Рябова К.А. Возможности применения Kaspersky Unified Monitoring and Analysis Platform (KUMA) в правоохранительных органах 301

Файзуллина А.С. Расследование компьютерных инцидентов: подходы, решения, практика 304

Чернов Р.А. Использование новых средств защиты информации в работе с персоналом, допущенным к конфиденциальной информации: опыт внедрения ПК «Стахановец» 308

СЕКЦИЯ 4. КОНЦЕПЦИЯ И МЕТОДЫ ИНЖЕНЕРНО-ТЕХНИЧЕСКОГО ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Вафин А.Р. Инструменты языка программирования Python для анализа и моделирования сетевых процессов 313

Гизатова Е.А. Подход к обеспечению информационной безопасности виртуализированных АРМ на базе РЕД ОС 317

Джабаров А.М. Современные методы защиты контролируемых зон 322

Ермолаева А.В. Концептуальный подход к системе защиты информации цифровых сервисов 326

Ефимова С.В. Анализ утечек DNS и WebRTC в VPN-сервере на основе трасссировки сетевых пакетов в Wireshark 331

Кудакаев И.Ф. EDR vs XDR в гетерогенной среде: какой подход эффективнее? 335

Куликова В.Е., Колузанов Д.В. Использование криптографических средств защиты информации на основе дискретных носителей 339

Латыпов М.Р. Сквозное шифрование 343

Лукашов Н.П. Реализация защиты веб-приложений от SQL-инъекций с использованием ModSecurity и Fail2ban в среде операционной системы Astra Linux 347

Мартинкевич Д.М., Янисла́вский К.О. Блокировка приложений на межсетевом экране CHUWALL 351

Муллаяров И.Р. Проектирование и программная реализация комплексных систем защиты персональных данных в образовательных организациях на основе концепции Privacy by Design 355

Мусина К.Ш. Отечественные киберполигоны как средство обеспечения безопасности автоматизированных систем управления технологическими процессами (на примере интеграции Ampire и ЦДЭС) 360

Мухаметшина Р.А. Проверка защищенности межсетевого взаимодействия на базе платформы ViPNet Coordinator 364

Сауляк А.Ф. Методы защиты контролируемой зоны с использованием пеленгации 368

Хакимов А.И. Уязвимости протокола Bluetooth Low Energy (BLE) в системах умного дома и методы их нейтрализации 373

Чернышев К.В. Угрозы нарушения изоляции контейнеров в современных информационных системах 377

СЕКЦИЯ 5. СОВРЕМЕННЫЕ ВЫЗОВЫ В ОБЛАСТИ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

Аетбаева Р.Г. Противодействие атакам на протокол Spanning Tree с использованием ROOT Guard и BPDU Guard в корпоративных сетях 382

Аетбаева Р.Г. VPN-соединение как надежный канал удаленного доступа к корпоративной сети 386

Аминев Б.Р. Open-source решения и API-интерфейсы как вектор проникновения во внутреннюю информационную среду компании 390

Бурангулов Д.Б. Подходы к обеспечению безопасности облачного контента в гибридных инфраструктурах 394

Войткус И.А. BSUIR OSINT SYSTEM – инструмент для киберразведки 397

Гизатова Е.А., Насибуллина А.В. Киберграмотность: почему обучение сотрудников – главный щит от современных угроз 401

Иванов И.П., Хасанов Р.Р. Скрытая передача информации по ультразвуковому акустическому каналу 406

Ишмухаметов И.Р. Утечки биометрии через косвенные данные в интернет вещей: анализ косвенных угроз 410

Казина К.З., Аккужина Ф.Ф. Статистический анализ киберинцидентов 2015–2024 415

Курбатов А.Д. Конечная аутентификация в mesh-сетях Meshtastic: программно-аппаратная модификация оконечных узлов 418

Курпаченко Д.М. Цифровой след сотрудника как нерегламентированный канал передачи информации: методы превентивного управления 422

Мухаметьянова А.Р., Аюпова И.И. Модель защиты персональных данных сотрудников в условиях размытия периметра: развитие концепции Zero Trust 427

Петренко А.С. Разработка квантово-устойчивого алгоритма консенсуса с адаптивной иерархической архитектурой 430

Петренко А.С. Оптимизация устойчивости национальных блокчейн-платформ и экосистем с помощью квантово-вдохновленных алгоритмов 435

Повеликин В.Я., Машков И.А. Технология защиты телеметрической информации элементов мультиагентной системы 439

Ракипов Д.А. Zero Trust в действии: практический подход к внедрению архитектуры нулевого доверия 444

Резбаев В.М., Ахметов У.Р. Моделирование и прогнозирование динамики хищений персональных данных на основе кинетических уравнений химических реакций 448

Сорокин К.Д. Угроза аппаратного сброса пароля BIOS 452

Файзуллина А.С. Атаки на сети компаний: анализ, эксплуатация и защита от SSRF-уязвимостей на примере микросервисной архитектуры 455

Фатеев Р.Р. Программный комплекс «RouterSentry» для аутентификации домашних Wi-Fi маршрутизаторов на основе аппаратных характеристик 460

Фесько Н.В. Проблемы рефлектометрии и предложение по поиску вейвлетов для автоматизации анализа 464

Хайсаров Р.И., Шабрин А.Ю. Мессенджеры и социальные сети как среда реализации социальной инженерии: смишинг, претекстинг и использование голосовых дипфейков 468

Яикбаев А.А., Бадамшин И.В. Проблемы безопасности интернета вещей: технологии, перспективы, риски 472

ПЛЕНАРНЫЕ ДОКЛАДЫ И ВЫСТУПЛЕНИЯ ЭКСПЕРТОВ

УДК 378.147:004.056

Бугаенко О.Д.
Северный (Арктический) федеральный университет
имени М.В. Ломоносова, Архангельск

КВАНТОВАЯ КРИПТОГРАФИЯ В УНИВЕРСИТЕТСКОМ КУРСЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: ПОДХОДЫ И МЕТОДЫ

Аннотация. Алгоритм Шора на квантовом компьютере способен за полиномиальное время взламывать RSA и ECC – это один из самых серьезных современных вызовов компьютерной безопасности. В статье анализируется, как университетские курсы информационной безопасности могут ответить на этот вызов через преподавание квантовой криптографии. Рассматриваются протоколы BB84 и B92, образовательные ресурсы (CrypTool, Qiskit). Предлагается модульная структура курса. Определяются ключевые проблемы внедрения.

Ключевые слова: квантовая криптография, квантовое распределение ключей, протокол BB84, протокол B92, образовательные ресурсы, CrypTool, Qiskit, информационная безопасность.

Введение. В контексте современных вызовов компьютерной безопасности, связанных с появлением квантовых компьютеров, способных нивелировать стойкость классических криптосистем, особую актуальность приобретает подготовка специалистов, владеющих методами квантовой криптографии. Алгоритм Шора позволяет решать задачи факторизации и дискретного логарифмирования за полиномиальное время [2]. По оценкам [7], появление систем, нарушающих стойкость современных криптомеханизмов, возможно в течение 10–15 лет. Цель статьи – разработка методики преподавания квантовой криптографии, включающей модульную структуру курса и лабораторный практикум.

Теоретические основы квантовой криптографии. Квантовая криптография базируется на принципах квантовой механики: неопределенности Гейзенберга, невозможности клонирования и неразличимости неортогональных состояний [2, 7]. Протокол BB84 (Беннетт и Брассар, 1984) использует поляризационные состояния фотонов. Ключевой показатель – квантовая битовая ошибка (QBER), пороговое значение которой составляет около 11% [7]. Протокол B92 (Беннетт, 1992) использует два неортогональных состояния, что упрощает аппаратную реализацию и удобно для образования [8].

Обзор образовательных ресурсов. Для преподавания квантовой криптографии в вузе доступен широкий спектр образовательных инструментов. Проект CrypTool считается одним из наиболее распространенных программных решений для обучения криптологии [8]. Представляет собой десктопное приложение, включающее более 400 криптографических алгоритмов, в том числе симуляцию протокола BB84 с визуализацией QBER и моделированием атаки «перехват-перепосылка». Платформа IBM Quantum Experience (Qiskit) предоставляет доступ к реальным квантовым процессорам через облачные сервисы и позволяет реализовывать протоколы BB84, B92 и E91 на языке Python. MATLAB-симуляции протокола B92 демонстрируют расчет доли «разрешенных битов» в зависимости от количества переданных битов, сопоставление теоретических и экспериментальных значений, а также визуализацию эффектов подслушивания [8]. В России изданы адаптированные пособия: И.М. Арбекова «Элементарная квантовая криптография» (2025) [6] и А.П. Пленкина «Квантово-криптографические сети» (2024) [3].

Методика преподавания квантовой криптографии. На основе анализа образовательных ресурсов и опыта ведущих университетов предлагается методика преподавания квантовой криптографии в техническом вузе. Цель курса заключается в формировании у студентов компетенций, связанных с пониманием теоретических основ и освоением практических методов квантовой криптографии, необходимых для решения задач защиты информации в условиях квантовых угроз. Структура курса включает пять разделов:

1. Введение в квантовую криптографию (2 часа) – охватывает базовые положения квантовой механики, необходимые для понимания криптографических приложений.

2. Протоколы квантового распределения ключей (12 часов) – посвящен протоколам BB84 и B92, их математическому описанию, анализу QBER и пороговым значениям безопасности.

3. Образовательные симуляторы (8 часов) – включает освоение CrypTool, CrypTool-Online и MATLAB-симуляций.

4. Программирование QKD-протоколов (10 часов) – предполагает реализацию протоколов BB84 и B92 с использованием Qiskit и Python.

5. Применение в информационной безопасности (4 часа) – рассматривает защиту критической инфраструктуры, гибридные протоколы и практические проекты.

Лабораторный практикум состоит из трех работ, каждая из которых направлена на освоение определенного инструментария и протокола (табл. 1).

Таблица 1

Лабораторные работы по курсу квантовой криптографии

№	Название	Инструмент	Цель
1	Симуляция BB84 в CrypTool	CrypTool Desktop	Изучить влияние шума и атаки «перехват-перепосылка» на QBER
2	Программирование BB84 на Qiskit	IBM Qiskit (облачный доступ)	Реализовать полный цикл QKD, сравнить симуляцию и реальный квантовый процессор
3	Моделирование B92 в MATLAB	MATLAB (или Octave)	Оценить долю «разрешенных битов» и эффекты подслушивания

Практическое применение как контекст проектной деятельности является важным компонентом курса. С целью повышения мотивации и связи обучения с реальным сектором в курсе рассматриваются действующие проекты в области квантовой криптографии: проект QKDSat Европейского космического агентства (ESA) по созданию спутниковой сети QKD, протокол Quantum Lock (Эдинбургский университет), объединяющий физически неклонируемые функции с QKD, и проект QuINSiDa (Германия), сочетающий QKD с технологией Li-Fi [4, 7]. На основе этих примеров студентам предлагается разработать собственное проектное задание, например, концепцию QKD-защиты для локальной сети предприятия. Примерный перечень групповых проектов: разработка симулятора протокола BB84 с визуализацией QBER на Python/Qiskit; сравнительный анализ эффективности протоколов BB84 и B92 в условиях шума и атак; исследование атак на QKD-системы; проектирование защищенной сети на основе QKD для малого предприятия.

Проблемы и вызовы при внедрении курса. Анализ апробации выявил пять барьеров: междисциплинарность (решение – «от наглядности к теории»), дороговизна оборудования (облачные IBM Q и симуляторы), дефицит адаптированной литературы (пособия [3, 6]), высокая динамика изменений (ежегодная актуализация), психологический барьер (акцент на угрозах RSA/ECC и реальных кейсах).

Заключение. Ключевая проблема в области компьютерной безопасности развитие квантовых вычислений, делающее классические криптоалгоритмы (RSA, ECC) уязвимыми. Без подготовки специалистов по постквантовым методам защита критической инфраструктуры становится невозможной.

Ключевая проблема – развитие квантовых вычислений, делающее RSA и ECC уязвимыми. Механизмы решения: образовательный курс, методический (симуляторы до математики), технологический (облачные платформы), практико-ориентированный (проекты на реальных кейсах).

Предложенные механизмы позволяют системно ответить на вызов квантовых вычислений без значительных затрат. Дальнейшие исследования – разработка открытых эмуляторов QKD и адаптация курса для ИТ-специалистов.

Список использованных источников:

1. Djordjevic I. B. Quantum Key Distribution (QKD) Fundamentals // Physical-Layer Security, Quantum Key Distribution, and Post-Quantum Cryptography. – Cham: Springer, 2025. – P. 305–362. – DOI: 10.1007/978-3-031-88372-9_7.

2. Sellami A. Practical Quantum Key Distribution // Cyber Security Standards, Practices and Industrial Applications. – Hershey: IGI Global, 2011. – P. 130-160. – DOI: 10.4018/978-1-60960-851-4.ch007.

3. Пленкин А. П. Квантово-криптографические сети: учебное пособие / А. П. Пленкин, В. А. Прудников, В. В. Юшицына. – Ростов-на-Дону; Таганрог: Издательство Южного федерального университета, 2024. – 124 с. – ISBN 978-5-9275-4595-7.

4. European Space Agency [Электронный ресурс]. ESA and Honeywell set for quantum data protection from space. – 2025. – Режим доступа: https://www.esa.int/Applications/Connectivity_and_Secure_Communications/ESA_and_Honeywell_set_for_quantum_data_protection_from_space (дата обращения: 13.04.2026).

5. Арбеков И. М. Элементарная квантовая криптография: для криптографов, не знакомых с квантовой механикой. – Москва: URSS, 2025. – 168 с. – ISBN 978-5-9519-XXXX-X.

6. Fraunhofer IPMS [Электронный ресурс]. Secure Optical Data Communication Using Quantum Cryptography and Li-Fi. – 2025. – Режим доступа: https://www.ipms.fraunhofer.de/en/press-media/press/2023/Secure-Optical-Data-Communication-Using-Quantum-Cryptography-and-Li-Fi.html (дата обращения: 11.04.2026).

7. Gandelman S. P. Hands-On Quantum Cryptography: Undergraduate Experimentation with the B92 Protocol [Электронный ресурс] / S. P. Gandelman, A. Maslennikov, G. G. Rozenman. – GitHub, 2024. – Режим доступа: https://github.com (дата обращения: 13.04.2026).

8. CrypTool [Электронный ресурс]. CrypTool – электронное обучение криптологии. – 2025. – Режим доступа: https://www.cryptool.org/ (дата обращения: 13.04.2026).

Bugaenko O.D.
Northern (Arctic) Federal University named
after M.V. Lomonosov, Arkhangelsk

QUANTUM CRYPTOGRAPHY IN THE UNIVERSITY COURSE OF INFORMATION SECURITY: APPROACHES AND METHODS

Abstract. Shor's algorithm on a quantum computer is capable of breaking RSA and ECC in polynomial time — this is one of the most serious modern challenges in computer security. The article analyzes how university information security courses can respond to this challenge through teaching quantum cryptography. The BB84 and B92 protocols, as well as educational resources (CrypTool, Qiskit), are considered. A modular course structure is proposed. The key implementation problems are identified.

Keywords: quantum cryptography, quantum key distribution, BB84 protocol, B92 protocol, educational resources, CrypTool, Qiskit, information security.

УДК 004.4: 519.7

Валеев С.С., Гузаиров М.Б.
Уфимский университет науки и технологий, Уфа

АВТОМАТИЧЕСКОЕ ОБНАРУЖЕНИЕ АНОМАЛИЙ В МНОГОМЕРНЫХ ВРЕМЕННЫХ РЯДАХ

Аннотация. Автоматическое обнаружение аномалий в многомерных временных рядах данных имеет важное прикладное значение, в том числе при решении задач информационной безопасности, так как снижает нагрузку на персонал аналитических центров. Рассматривается система автоматического обнаружения аномалий в многомерных временных рядах данных. Система построена на применении технологий глубокого обучения. Предлагается гибридная модель глубокого обучения, включающая в себя механизмы внимания, методы графового встраивания, управляемые рекуррентные сети и вариационные автокодировщики. При этом формируется эффективная структура автоматической системы обнаружения аномалий. В качестве направлений дальнейших исследований предполагаются проверка эффективности рассматриваемой модели на большем разнообразии наборов данных, а также повышение ее точности при обнаружении аномалий в многомерных временных рядах при одновременной оптимизации гиперпараметров модели.

Ключевые слова: многомерные временные ряды, обнаружение аномалий, глубокое обучение.

В различных приложениях возникает задача анализа аномального поведения динамических многомерных процессов, описывающих поведение технической системы или информационной системы. При этом предполагается, что рассматриваемые многомерные процессы представлены в виде временных рядов данных. К основным характеристикам многомерных временных рядов данных относятся нестационарность, большая размерность и низкая частота проявления аномального поведения, что делает процедуру обнаружения аномалий в системах реального времени достаточно сложной задачей.

Обнаружение аномалий во временных рядах в настоящее время все шире используется во многих прикладных областях, таких как городское управление, обнаружение вторжений, медицинские риски и стихийные бедствия. Часто задачи, решаемые в центрах обработки данных, сводятся к визуальному анализу человеком-оператором текущих информационных потоков. Автоматизация этих процедур позволяет своевременно обнаружить, например, отказы в больших системах, тем самым обеспечивает повышение эффективности систем быстрого реагирования [1, 2].

Для обработки больших объемов данных используются системы глубокого обучения и многоагентные технологии [3-6]. Обнаружение аномалий на основе глубокого обучения включает в себя два основных метода: метод, основанный на прогнозировании, и метод, основанный на реконструкции.

Метод, основанный на прогнозировании, использует модель глубокого обучения для сравнения прогнозируемого значения с фактическим значением и на основе величины отклонения определяет, является ли это аномалией.

Метод, основанный на реконструкции, формирует сеть кодировщик-декодировщик для реконструкции выборочных данных. Если выборка является аномалией, то реконструкция временного ряда будет содержать ошибки. При этом ошибка реконструкции используется в качестве маркера для оценки того, является ли последовательность аномалией.

В докладе рассматривается модель обнаружения аномалий в многомерных временных рядах на основе системы глубокого обучения с использованием автокодировщика, графового эмбеддинга и управляемого рекуррентного блока. Эта модель относится к классу гибридных моделей глубокого обучения, сочетающей механизмы внимания, методы графового эмбединга, управляемые рекуррентные сети и вариационные

автокодировщики, которые совместно образуют эффективную структуру автоматической системы обнаружения аномалий.

Благодаря совместной работе различных блоков комбинированная модель позволяет анализировать особенности временной последовательности, что обеспечивает повышение эффективности выявления аномалий в многомерных временных рядах.

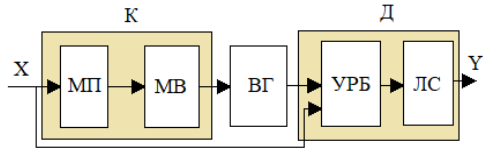


Рис. 1. Система анализа аномалий многомерных временных рядов

На рисунке 1 представлена система анализа аномалий многомерных временных рядов, где использованы следующие обозначения: *X* – многомерный временной ряд, *Y* – выход системы, МП – многослойный персептрон, МВ – блок внимания, ВГ – блок графового эмбединга, УРБ – управляемый рекуррентный блок, ЛС – линейный слой, К- кодировщик, Д – декодировщик.

На первом шаге кодировщик К использует многослойный персептрон (МП) и механизм внимания (МВ) для локального извлечения признаков с целью получения параметров распределения внутренних характеристик входных данных X. На втором шаге используется механизм адаптации параметров для получения признаков, используемых в блоке ВГ. Затем декодеровщик Д использует модуль УРБ для реконструкции временного ряда. На последнем шаге используется блок определения аномалий ЛС.

Дальнейшие исследования в данном направлении могут быть нацелены не только на проверку эффективности рассматриваемой модели на большем разнообразии наборов различных данных, но и на повышение ее точности при обнаружении аномалий в многомерных временных рядах при одновременной оптимизации ее гиперпараметров.

Список использованных источников:

1. Паттерсон, Д. Глубокое обучение с точки зрения практика / Д. Паттерсон, А. Гибсон. – Москва: ДМК Пресс, 2018. – 418 с. – ISBN 978-5-97060-481-6. – Текст: электронный // Лань: электронно-библиотечная система. – URL: https://e.lanbook.com/book/116122 (дата обращения: 13.04.2025). – Режим доступа: для авториз. пользователей.

2. Шалев-Шварц, Ш. Идеи машинного обучения: учебное пособие / Ш. Шалев-Шварц, Бен-Давид Ш.; перевод с английского А. А. Слинкина. – Москва: ДМК Пресс, 2019. – 436 с. – ISBN 978-5-97060-673-5. – Текст: электронный // Лань: электронно-библиотечная система. – URL: https://e.lanbook.com/book/131686 (дата обращения: 13.04.2025). – Режим доступа: для авториз. пользователей.

3. Валеев С.С., Кондратьева Н.В., Гузаиров М.Б., Исмагилова А.С. Иерархическая динамическая система управления информационной безопасностью информационной системы предприятия // Инженерный вестник Дона. – 2023. – № 11 (107). – С. 154-164.

4. Валеев С.С., Гузаиров М.Б. Генеративные многоагентные системы и задачи защиты информации на базе концепции нулевого доверия // Информационные технологии обеспечения комплексной безопасности в цифровом обществе. Материалы VIII Всероссийской молодежной научно-практической конференции с международным участием. – Уфа, 2025. – С. 13-17.

5. Valeev S., Kondratyeva N. Large scale system management based on Markov decision process and big data concept // В сборнике: Application of Information and Communication Technologies, AICT 2016 - Conference Proceedings. – Baku, 2016. – С. 7991829.

6. Валеев С.С., Кондратьева Н.В., Гузаиров М.Б., Мельников А.В. Этапы реинжиниринга информационной системы предприятия в рамках технологии нулевого доверия // Вестник Российского нового университета. Серия: Сложные системы: модели, анализ и управление. – 2023. – № 3. – С. 136-143.

Valeev S.S., Guzairov M.B.
Ufa University of Science and Technology, Ufa

AUTOMATIC DETECTION OF ANOMALIES IN MULTIVARIATE TIME SERIES

Abstract. Automatic anomaly detection in multivariate time series data has significant practical applications, including in information security, as it reduces the workload of analytical center personnel. A system for automatic anomaly detection in multivariate time series data is considered. The system is built using deep learning technologies. A hybrid deep learning model is proposed that incorporates attention mechanisms, graph embedding methods, supervised recurrent networks, and variational autoencoders. This results in the development of an effective structure for an automatic anomaly detection system. Further research is proposed to test the effectiveness of this model on a wider variety of datasets and to improve its accuracy in detecting anomalies in

multivariate time series while simultaneously optimizing the model's hyperparameters.

Keywords: multivariate time series, anomaly detection, deep learning.

УДК 004.4: 519.7

Валеев С.С., Гузаиров М.Б., Яппаров Р.М.
Уфимский университет науки и технологий, Уфа

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И КИБЕРБЕЗОПАСНОСТЬ

Аннотация. Как известно, кибербезопасность (КБ) представляет собой совокупность методов, технологий и практик, направленных на защиту компьютеров, серверов, мобильных устройств, электронных систем, сетей и данных от атак злоумышленников, а также на предотвращение и минимизацию последствий кибератак. Основной целью КБ является обеспечение конфиденциальности, целостности и доступности информации в цифровом пространстве. В настоящее время искусственный интеллект (ИИ) становится обязательным элементом КБ.

Ключевые слова: искусственный интеллект, кибербезопасность, глубокое обучение, гибридные архитектуры, операционная устойчивость.

1. Введение

В настоящее время происходит переход от реактивной защиты к проактивной, где ИИ не только обнаруживает, но и прогнозирует возможные атаки [1-3]. Развиваются мультиагентные системы, где множество ИИ-агентов взаимодействуют между собой, формируя экосистемы защиты [4]. Главным принципом применения ИИ является «человек в контуре»: ИИ берет на себя рутину, а человек – стратегические решения и ответственность [4-6].

Рассмотрим далее основные направления ИИ, связанные с КБ: глубокое обучение как основа современного ИИ, гибридные архитектуры как способ повышения эффективности, а также операционная устойчивость как конечная бизнес-модель внедрения ИИ [4].

2. Глубокое обучение в КБ

Глубокое обучение позволяет автоматически извлекать иерархические признаки из сырых данных, преодолевая ограничения сигнатурных методов и классических методов машинного обучения.

В Таблице 1 представлены ключевые архитектуры для глубокого обучения и их применение для решения различных актуальных задач кибербезопасности.

Таблица 1

Ключевые архитектуры и их применение

Архитектура	Назначение	Примеры задач в кибербезопасности
Сверточные сети (CNN)	Извлечение паттернов	Анализ сетевого трафика (образы потоков), обнаружение вредоносного ПО в потоке данных, анализ системных логов как последовательностей токенов.
Рекуррентные сети (RNN, LSTM, GRU)	Моделирование временных рядов	Обнаружение аномалий во временных рядах (скорость соединений, активность пользователя), анализ последовательностей системных вызовов, предсказание следующей команды.
Автокодировщики (Autoencoders)	Обучение на данных, определение выбросов	Обнаружение аномалий в потоке данных, выявление компрометации учетных записей (UEBA), определение редких атак
Графовые нейросети (GNN)	Анализ связей и реляционных структур данных	Обнаружение мошеннических транзакций, анализ графа процессов (Provenance Graph), выявление латерального перемещения по сетевому графу
Трансформеры (BERT, GPT)	Обработка длинных зависимостей, контекстное понимание	Анализ логов с длинной памятью, расследование инцидентов (Security Copilot), генерация правил IDS, анализ веб-запросов (SQLi, XSS)

Проблемы, связанные с глубоким обучением при решении задач кибербезопасности:

- набор данных для обучения: требуются большие размеченные наборы данных. Сложность возникает в формировании датасета об атаках;
- объяснимость: метод «черного ящика» неприемлем для аналитиков безопасности;
- большие накладные расходы: анализ в реальном времени требует применения GPU/TPU.

3. Гибридные архитектуры

Гибридные системы позволяют использовать сильные стороны разных парадигм ИИ. Типы гибридных архитектур ИИ, их компоненты, преимущества и примеры реализации представлены в Таблице 2.

Таблица 2

Типы гибридных архитектур

Тип гибридизации	Компоненты	Преимущества	Пример
Глубокое обучение + экспертные системы	Нейросеть (признаки) + набор логических правил	Объяснимость, детерминизм для критичных случаев	SNORT + LSTM для постобработки ложных срабатываний
Глубокое обучение + статистика	GNN / Autoencoder + статистический контроль (EWMA, CUSUM)	Робастность к шуму, раннее обнаружение изменений	Обнаружение DDoS атак на основе разложения трафика на тренд+сезонность+аномалию
Гибридные глубокие архитектуры	CNN + LSTM (ConvLSTM), CNN + Transformer	Учет пространственно-временных корреляций	Анализ пакетных потоков (CNN) с памятью о предыдущих соединениях (LSTM)
Ансамбли	Random Forest + Autoencoder + GNN	Снижение дисперсии, устойчивость к выбросам	SIEM с несколькими детекторами и голосованием
Графо-нейро-символьные системы	GNN (распознавание паттернов) + LSTM (временные роли) + база знаний MITRE ATT&CK	Отображение алертов на тактики и техники, контекстное расследование	Система, которая, например, дает комментарий: «Это похоже на T1021.006 (WinRM) с вероятностью 0.87, вот связанные процессы»

Примеры гибридного пайплайна в реальных приложениях:

1. Трафик → CNN/LSTM (аномальное событие).
2. Аномалия → Графовый классификатор (класс угрозы).
3. Класс → Экспертная система / MITRE, ФСТЭК (рекомендации действия).
4. Контур обратной связи → Эксперт (Human-in-the-loop) → Дообучение системы.

4. Операционная устойчивость

Операционная устойчивость (Operational Resilience) представляет собой способность системы выполнять целевые функции при наличии кибератак, сбоев или деградации. ИИ в этом случае не просто детектор, а компонент, обеспечивающий устойчивость функционирования системы (Таблица 3).

Таблица 3

Применение ИИ для повышения операционной устойчивости

Функция	Как помогает ИИ	Ключевые методы
Автоматическое восстановление (Self-healing)	Обнаружение отказа компонента, запуск альтернативного пути (rerouting), откат конфигураций	RL (reinforcement learning), деревья решений, предсказание отказов
Динамическая балансировка нагрузки под атакой	Перенаправление легитимного трафика в чистые зоны, подавление вредоносного ПО	DRL (Deep RL) для распределения ресурсов, прогнозирование очередей
Адаптивный периметр безопасности (Zero Trust + ИИ)	Постоянная переоценка доверия, динамическая микросегментация	GNN для графов доступа, поведенческие профили (RNN, Autoencoder)
Фолбэк ИИ-моделей	Переключение с DL-детектора (точный, медленный) на статистический (грубый, быстрый) при атаке на вычислительные ресурсы	Каскадные модели, вариативное пороговое обнаружение
Имитационные испытания (XAI + Red Teaming)	Генерация реалистичных атак, проверка AI на устойчивость к adversarial-примерам	GAN для синтеза атак, генетические алгоритмы для поиска слепых зон

Основные используемые метрики операционной устойчивости для ИИ-систем защиты:

- RTO (Recovery Time Objective) с участием ИИ-автоматизации.
- RPO (Recovery Point Objective) – минимизация потерь данных через предсказание атак.
- MTTD / MTTR с ИИ – сокращение за счет автоматической корреляции.
- Адаптивность к новым атакам, т.е. обеспечение требуемой точности на zero-day наборе.

5. Выводы

Основные тренды использования методов ИИ в КБ в рамках рассматриваемой темы:

- XAI (Explainable AI) для аналитиков, применение технологий LIME, SHAP, attention maps.
- Федеративное обучение (Federated Learning) для обеспечения обучения систем ИИ без раскрытия данных.
- LLM для Security Copilot – генерация отчетов, playbook-ов, естественно-языковой интерфейс к SIEM.
- Adversarial ML defense – тренировка на состязательных примерах, сертифицированная робастность.

Ключевые вызовы:

- Эволюция атак – атакующие тоже используют методы ИИ (deepfake-фишинг, авто-эксплойты).

− Высокая цена ошибки II рода (ложное спокойствие) – опаснее ложных тревог.

− Масштабируемость в реальном времени – AI на 100 Гбит/с трафика по-прежнему тяжел.

− Операционная сложность гибридных систем – дебаггинг и обновление набора связанных моделей непрост.

Основные выводы:

− использование методов глубокого обучения дает high recall на известных паттернах и неочевидных аномалиях.

− гибридные архитектуры обеспечивают интерпретируемость, устойчивость к шуму и совместимость с процессами SOC.

− операционная устойчивость – это системный уровень, где ИИ становится частью замкнутого контура управления безопасностью (detect → decide → act → adapt).

На практике широко используются гибридные пайплайны (CNN/Transformer + LSTM + GNN + knowledge graph), дополненные механизмами resilience (self-healing, adaptive ZT, fallback models) и объединенные с LLM-интерфейсом для аналитика.

Список использованных источников:

1. Паттерсон, Д. Глубокое обучение с точки зрения практика / Д. Паттерсон, А. Гибсон. – Москва: ДМК Пресс, 2018. – 418 с. – ISBN 978-5-97060-481-6. – Текст: электронный // Лань: электронно-библиотечная система. – URL: https://e.lanbook.com/book/116122 (дата обращения: 13.04.2025). – Режим доступа: для авториз. пользователей.

2. Шалев-Шварц, Ш. Идеи машинного обучения: учебное пособие / Ш. Шалев-Шварц, Бен-Давид Ш.; перевод с английского А. А. Слинкина. – Москва: ДМК Пресс, 2019. – 436 с. – ISBN 978-5-97060-673-5. – Текст: электронный // Лань: электронно-библиотечная система. – URL: https://e.lanbook.com/book/131686 (дата обращения: 13.04.2025). – Режим доступа: для авториз. пользователей.

3. Валеев С.С., Кондратьева Н.В., Гузаиров М.Б., Исмагилова А.С. Иерархическая динамическая система управления информационной безопасностью информационной системы предприятия // Инженерный вестник Дона. – 2023. – № 11 (107). – С. 154-164.

4. Валеев С.С., Гузаиров М.Б. Генеративные многоагентные системы и задачи защиты информации на базе концепции нулевого доверия // Информационные технологии обеспечения комплексной безопасности в цифровом обществе. Материалы VIII Всероссийской молодежной научно-практической конференции с международным участием. – Уфа, 2025. – С. 13-17.

5. Valeev S., Kondratyeva N. Large scale system management based on Markov decision process and big data concept // В сборнике: Application of Information and Communication Technologies, AICT 2016 - Conference Proceedings. – Baku, 2016. – С. 7991829.

6. Валеев С.С., Кондратьева Н.В., Гузаиров М.Б., Мельников А.В. Этапы реинжиниринга информационной системы предприятия в рамках технологии нулевого доверия // Вестник Российского нового университета. Серия: Сложные системы: модели, анализ и управление. – 2023. – № 3. – С. 136-143.

Valeev S.S., Guzairov M.B., Yapparov R.M.
Ufa University of Science and Technology, Ufa

ARTIFICIAL INTELLIGENCE AND CYBERSECURITY

Abstract. Cybersecurity (CS) is a set of methods, technologies, and practices aimed at protecting computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks, as well as preventing and minimizing the consequences of cyberattacks. The primary goal of CS is to ensure the confidentiality, integrity, and availability of information in the digital space. Artificial intelligence (AI) is currently becoming a mandatory element of CS.

Keywords: artificial intelligence, cybersecurity, deep learning, hybrid architectures, operational resilience.

УДК 004.056

Волошин Д.Г.
Северо-Кавказский федеральный университет, Ставрополь

МЕТОД КВАЗИАВТОНОМНОЙ НАВИГАЦИИ БПЛА ЛЕГКОГО КЛАССА И ФОРМИРОВАНИЯ ЗАЩИЩЕННОЙ ТРАЕКТОРИИ ПОЛЕТА В УСЛОВИЯХ АКТИВНОГО СПУФИНГА

Аннотация. В условиях зависимости беспилотных летательных аппаратов (БПЛА) от сигналов глобальных навигационных спутниковых систем (ГНСС) проблема их уязвимости к имитационным помехам (спуфингу) приобретает актуальность. Предложен метод повышения навигационной устойчивости, основанный на квазиавтономной навигации. Архитектура объединяет инерциальные измерения, видеоанализ и фазированную антенную решетку для локализации источников помех. Задача формирования защищенной траектории сведена к оптимальному управлению. Результаты натурных

экспериментов демонстрируют существенное снижение риска реализации спуфинг-атак и подтверждают эффективность предложенного метода.

Ключевые слова: БПЛА, спуфинг, информационная безопасность, квазиавтономная навигация, фазированная антенная решетка, инерциальная система.

Современные беспилотные летательные аппараты (БПЛА) легкого класса критически зависят от глобальных навигационных спутниковых систем (ГНСС) [1], что обеспечивает точность, но создает уязвимость для атак. Как показано в [2, 3], низкая помехозащищенность сигналов позволяет осуществлять дрейфовый спуфинг – постепенный увод аппарата с траектории. Это требует создания навигационной системы, устойчивой к компрометации спутниковых данных. Предлагается квазиавтономное решение в замкнутом контуре управления, объединяющее INS, визуальную одометрию и фазированную антенную решетку для пространственной фильтрации.

Для формального описания движения БПЛА введем вектор состояния, включающий положение, скорость и ориентацию аппарата:

$$\mathbf{x}(t) = \begin{bmatrix} \mathbf{r}(t) \\ \mathbf{v}(t) \\ \mathbf{q}(t) \end{bmatrix},$$

где $\mathbf{r}(t)$ – вектор положения БПЛА; (t) – вектор линейной скорости; $\mathbf{q}(t)$ – параметры ориентации (кватернион); t – время.

Динамика системы описывается нелинейным стохастическим уравнением:

$$\dot{\mathbf{x}}(t) = f(\mathbf{x}(t), \mathbf{u}(t)) + \mathbf{w}(t),$$

где $f(\cdot)$ – нелинейная функция динамики; $\mathbf{u}(t)$ – вектор управляющих воздействий; $\mathbf{w}(t$ – вектор случайных возмущений.

При реализации спуфинг-атаки в измерения ГНСС вносится аддитивная составляющая $\Delta\, t$, что приводит к рассогласованию между оценками состояния по данным ГНСС и INS.

Вектор рассогласования $\mathbf{e}(t) = \hat{\mathbf{x}}_{INS}(t) - \hat{\mathbf{x}}_{\text{ГНСС}}(t)$ используется для формирования статистического критерия обнаружения:

$$\mathbf{e}^T(t)\mathbf{S}^{-1}\mathbf{e}(t) > \gamma,$$

где $\mathbf{S}^{-1}$ – ковариационная матрица ошибок, γ – порог обнаружения. Превышение порога интерпретируется как признак атаки и инициирует переход системы в защищенный режим.

В отличие от легитимных спутниковых сигналов, приходящих с различных направлений, спуфинг, как правило, реализуется с помощью

одного или ограниченного числа наземных передатчиков [4, 5]. Это позволяет использовать методы пространственной фильтрации для оценки направления на источник помех.

В предлагаемой системе применяется четырехэлементная планарная фазированная антенная решетка (ФАР). Разность фаз сигналов $\Delta\psi_{ij}$ между антенными элементами связана с направлением прихода соотношением:

$$\Delta\psi_{ij} = \frac{2\pi}{\lambda}(\mathbf{r}_i - \mathbf{r}_j)^T\mathbf{u},$$

где λ – длина волны, $\mathbf{r}_i$ – координаты антенн, $\mathbf{u}$ – единичный вектор направления на источник. Решение системы уравнений методом наименьших квадратов дает оценку азимута $\hat{\phi}$ и угла места $\hat{\theta}$.

Для сглаживания шумовых флуктуаций применяется фильтр Калмана с вектором состояния $[\phi, \dot{\phi}, \theta, \dot{\theta}]^T$. Экспериментально достигнутая точность пеленгации составляет 3°–5°, что достаточно для построения траектории уклонения.

После подтверждения атаки система переходит в режим квазиавтономной навигации, при котором использование данных ГНСС прекращается. Задача управления формулируется как минимизация функционала качества:

$$J = \int_{t_0}^{T}\left(\| \mathbf{p}_t - \mathbf{p}_t^{ref} \|_Q^2 + \| \mathbf{v}_t - \mathbf{v}_t^{ref} \|_R^2 + \| \mathbf{u}_t \|_S^2\right) dt,$$

где $\mathbf{p}_t^{ref}$, $\mathbf{v}_t^{ref}$ – эталонные траектория и скорость.

Позиционирование осуществляется на основе интегрирования инерциальных измерений с начальными условиями, заданными последними достоверными данными ГНСС. Для компенсации дрейфа INS используются барометр и магнитометр в рамках комплементарной фильтрации. Управление отклонениями реализуется ПИД-регулятором.

Для проверки работоспособности предложенного метода был проведен комплекс натурных экспериментов на полигоне с контролируемой электромагнитной обстановкой. В состав испытательного стенда входили БПЛА массой 2,5 кг на базе контроллера Pixhawk 4 и интеллектуальный модуль защиты на базе Orange Pi 5. Для имитации атак использовался программно-определяемый радиосистема USRP B210. В ходе испытаний рассматривались три типовых сценария: дрейфовый увод (А), траекторный увод (Б) и комбинированная атака (В). Результаты оценки точности пеленгации источника спуфинга приведены в таблице 1. В таблице 2 представлены результаты оценки точности следования защищенной траектории для каждого из трех сценариев.

Таблица 1

Точность пеленгации источника спуфинга

Метрика	Среднее значение	СКО	Макс. ошибка
Ошибка азимута	3,8°	1,5°	6,2°
Ошибка угла места	4,5°	2,1°	8,1°

Как видно из представленных в таблице 1 данных, средняя ошибка определения азимута составляет 3,8°, а угла места – 4,5°, что находится в пределах теоретически ожидаемого диапазона 3–5°. Полученная точность признается достаточной для практического построения траектории уклонения, поскольку позволяет уверенно идентифицировать сектор, в котором расположен источник помех.

Таблица 2

Эффективность следования защищенной траектории

Сценарий	СКО (метод), м	СКО (без защиты), м	Успешность
А (дрейф)	12,4	>150	10/10
Б (увод)	18,7	300 (потеря)	9/10
В (комбинир.)	22,1	Авария	8/10

Анализ данных таблицы 2 показывает, что даже в наиболее сложном случае комбинированной атаки (сценарий В) среднеквадратическое отклонение не превышает 22,1 м, что обеспечивает безопасное завершение полета. Для сравнения, БПЛА без предлагаемой системы защиты в сценариях А и Б полностью терял управление и выходил за пределы полигона. Успешность завершения миссии с использованием разработанного метода составила 80-100% в зависимости от типа атаки.

В работе предложен метод квазиавтономной навигации, обеспечивающий устойчивость БПЛА легкого класса при активном спуфинге за счет интеграции алгоритмов обнаружения аномалий [6], локализации источников помех [5] и адаптивного формирования траектории [4]. Экспериментально подтверждена точность пеленгации 3–5°, удержание аппарата в коридоре 15 м при полной компрометации ГНСС и снижение риска успешной атаки более чем в 20 раз. Метод ориентирован на бортовые системы с ограниченными ресурсами (Orange Pi 5, 68 г, 12-15 Вт), что делает его пригодным для серийных БПЛА. Перспективы включают нейросетевое прогнозирование атак, MPC-управление и кооперативную защиту роя.

Список использованных источников:

1. Воловик Е.В. Типы имитационного воздействия (спуфинга) // Труды ГосНИИАС. Серия Авиационные системы. 2024. № 3 (66). С. 19-31.

2. Sathaye H. et al. An Experimental Study of GPS Spoofing and Takeover Attacks on UAVs // 31st USENIX Security Symposium. 2022. P. 3503–3520.

3. Петренко В.И., Тебуева Ф.Б., Волошин Д.Г. Метод построения траектории полета БПЛА в условиях кибератак GPS/ГЛОНАСС спуфинга // Прикаспийский журнал: Управление и высокие технологии. 2024. № 2 (66). С. 71-80.

4. Демин О.А., Костин М.С. Кросс-пилотная синхронизация фазированной антенной SDR-решетки, сформированной БПЛА-группировкой // Ракетно-космическое приборостроение и информационные системы. 2024. Т. 11. № 3. С. 64-75.

5. Петренко В.И., Наджаджра М.Х., Тебуева Ф.Б., Волошин Д.Г., Дибров Н. Трансформерная модель бинарной классификации временных рядов на данных инерциальных датчиков для детекции спуфинг-атак в БПЛА // International journal of open information technologies. 2026. Т. 14. № 2. С. 11-18.

6. Jarraya I. et al. Gnss-denied unmanned aerial vehicle navigation: analyzing computational complexity, sensor fusion, and localization methodologies // Satellite Navigation. 2025. Vol. 6. №9.

Voloshin D.G.
North-Caucasus Federal University, Stavropol

METHOD FOR QUASI-AUTONOMOUS NAVIGATION OF LIGHTWEIGHT UAVs AND FORMATION OF A SECURE FLIGHT PATH UNDER ACTIVE SPOOFING CONDITIONS

Abstract. As unmanned aerial vehicles (UAVs) increasingly rely on global navigation satellite systems (GNSS), their vulnerability to spoofing attacks becomes a pressing concern. A method for improving navigation resilience based on quasi-autonomous navigation is proposed. The architecture integrates inertial measurements, video analysis, and a phased antenna array to localize interference sources. The problem of generating a protected flight path is reduced to optimal control. Experimental results demonstrate a significant reduction in the risk of successful spoofing attacks and confirm the effectiveness of the proposed method.

Keywords: UAV, spoofing, information security, quasi-autonomous navigation, phased antenna array, inertial system.

УДК 004.08

Гусева Т.М.
Северо-Кавказский федеральный университет, Ставрополь

ТЕНДЕНЦИИ РАЗВИТИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В КИБЕРБЕЗОПАСНОСТИ

Аннотация. Данная статья посвящена тенденциям развития систем искусственного интеллекта, касательно применения его в аспектах кибербезопасности. В статье приведена статистика за последние годы об обнаруженных атаках кибербезопасности. Для предотвращения таких атак в статье рассмотрены методы искусственного интеллекта: машинное обучение, глубокое обучение, NLT-технологии. В завершении статьи указано, что системы искусственного интеллекта имеют некие ограничения применительно для кибербезопасности.

Ключевые слова: кибербезопасность, угрозы безопасности, искусственный интеллект, машинное обучение, глубокое обучение.

За последние пару лет было обнаружено огромное количество утечек персональных данных, а если быть точнее то, более 100 миллиардов записей. При этом из них 4,5 миллиардов было скомпрометировано в России. Такую статистику приводит экспертно-аналитический центр ГК InfoWatch в своем исследовании «Утечки информации ограниченного доступа. Мир, 2023-2025 годы». Одновременно с этим существенно выросла доля утечек коммерческой тайны. Такие утечки были зафиксированы более чем в трети инцидентов [1].

Если верить статистике аналитического отчета центра мониторинга и противодействия кибератакам «Код безопасности» за первое полугодие 2025 года было обнаружено около 28 миллиардов инцидентов безопасности. Среди таких инцидентов были выявлены подозрительная сетевая активность, атаки на веб-приложения, потенциальные нарушения конфиденциальности.

Если судить по текущей статистике, то существует тенденция ежегодного увеличения числа кибератак. Но традиционные методы устаревают и становятся неспособными для реагирования на новые угрозы информационной безопасности. С каждым годом все больше и больше появляется новых угроз, что требует и соответственно разработки новых методов обнаружения угроз на базе систем искусственного

интеллекта. В связи с этим можно определить актуальность научной статьи.

Актуальность научной статьи обусловлена необходимостью внедрения инновационных подходов к защите информационных систем. Искусственный интеллект и машинное обучение предоставляют принципиально новые возможности, такие как автоматизацию обнаружения угроз, адаптацию к изменяющимся условиям, прогнозирование атак на основе паттерн-анализа. По оценкам экспертов, внедрение инструментов ИИ и автоматизации сокращает время реагирования на инциденты кибербезопасности, а точность выявления аномалий порой достигает очень высоких результатов в пределах 95 %.

На рисунке 1 приведены современные методы искусственного интеллекта, применяемые в кибербезопасности.

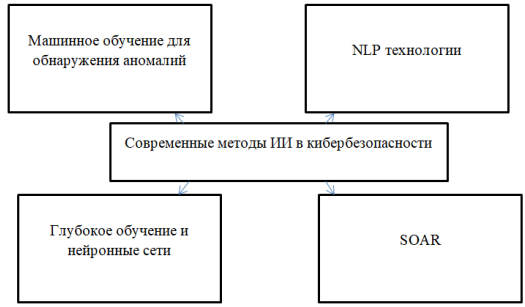


Рис. 1. Методы ИИ в кибербезопасности

Алгоритмы машинного обучения активно применяются в системах обнаружения вторжений и предотвращения вторжений. Они имеют несколько ключевых подходов, рисунок 2.

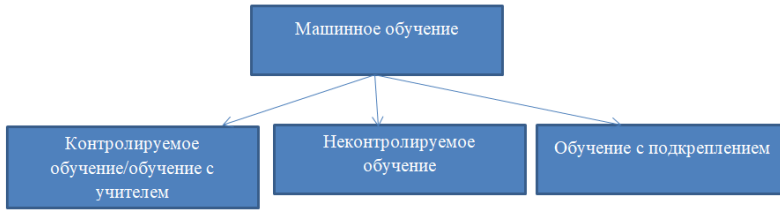


Рис. 2. Ключевые подходы машинного обучения

В зависимости от используемого подхода машинного обучения можно достичь точности обнаружения угроз от 80 до 95%.

Глубокое обучение применяется для анализа сложных паттернов в сетевом трафике и логах.

Еще одним востребованным методов предотвращения кибратак считаются NLP-технологии. Они умеют формировать отчеты об угрозах, автоматически разбирать логи безопасности, обнаруживают фишинговых письма и вредоносные сообщения в мессенджерах. По данным исследований NLP-системы сокращают время анализа отчетов на 70 % и выявляют до 90 % фишинговых атак с использованием социальной инженерии.

Используемые методы: токенизация, векторизация текста (Word2Vec, BERT), тематическое моделирование (LDA).

Система оркестрации, автоматизации и реагирования на инциденты безопасности (SOAR) – это набор служб и инструментов, которые автоматизируют процессы предотвращения кибератак и противодействия им.

Системы оркестрации и автоматизации безопасности (SOAR) интегрируют ИИ для автоматической классификации инцидентов, генерации плейбуков реагирования, изоляции скомпрометированных устройств. По данным Gartner, внедрение SOAR сокращает время реагирования на инциденты на 60 % и снижает нагрузку на аналитиков на 80 %.

Тенденции развития системы искусственного интеллекта отмечают переход от статических моделей к динамическим моделям, которые обучаются в режиме реального времени на новых обнаруженных угрозах [2].

Такое обучение систем ИИ позволяет

- оперативно адаптироваться к новым видам атак;
- снижать количество ложных срабатываний;
- учитывать специфику конкретной инфраструктуры.

Статистика: системы с адаптивным обучением сокращают количество ложных срабатываний на 35–50 % по сравнению со статическими моделями.

Также тенденции развития систем ИИ отмечают развитие методов интерпретируемого машинного обучения. По данным исследования компании iTPROTECT, 78 % организаций планируют внедрить такие решения в текущем году.

На практике стали использоваться гибридные системы защиты, они позволяют обнаруживать на 25% больше угроз, чем отдельные системы.

ИИ-системы переходят от реактивного обнаружения к прогнозированию атак – они производят анализ глобальных трендов киберугроз, моделируют различные сценарии атак на информационные

системы, производят оценку уязвимостей инфраструктуры на основе исторических данных.

Использование ИИ в рамках кибербезопасности на сегодняшний день считается неотъемлемой частью. Но существуют проблемы и ограничения для использования систем искусственного интеллекта для обнаружения кибератак. Рассмотрим их. Во-первых, системы искусственного интеллекта имеют уязвимости, рисунок 3.

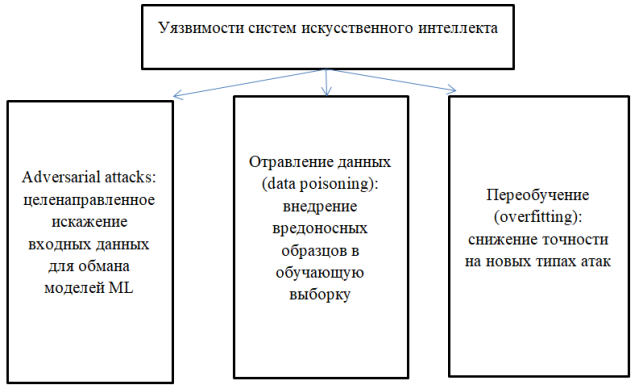


Рис. 3. Уязвимости систем искусственного интеллекта

Во-вторых, существуют ограничения использования искусственного интеллекта. К ним можно отнести ресурсоемкость, этические и правовые аспекты.

При использовании систем ИИ необходимо хранить огромные объемы данных, а также тратить огромный бюджет на покупку инфраструктуры для ИИ, а также согласно ФЗ-152 соблюдать конфиденциальность персональных данных при обучении моделей систем искусственного интеллекта [3].

Список использованных источников:

1. InfoWatch: за 3 года в России утекло 4,5 млрд записей персональных данных. Электронный ресурс. URL: https://safe.cnews.ru/news/line/2026-03-19_infowatch_za_3_goda_v_rossii_uteklo.

2. Т. Э. Николаенко, Т. М. Гусева Перспективы и тенденции развития искусственного интеллекта // Общество и личность: теория и практика гуманизации в современных реалиях: Материалы X всероссийской научно-практической конференции, Ставрополь, 13 мая 2022 года. – Ставрополь: Северо-Кавказский социальный институт, 2022. – С. 240-243.

3. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».

Guseva T.M.
North Caucasus Federal University, Stavropol

ARTIFICIAL INTELLIGENCE DEVELOPMENT TRENDS IN CYBERSECURITY

Abstract. This article addresses the development of artificial intelligence (AI) and its application in cybersecurity. It presents statistics on detected cybersecurity attacks over recent years. To prevent such attacks, the article discusses methods for using AI: machine learning, deep learning, and neural network technologies. The article concludes by noting that AI systems have some limitations, particularly for cybersecurity.

Keywords: cybersecurity, security threats, artificial intelligence, machine learning, deep learning.

УДК 004.056.53

Иконников С.Н., Шкляр Е.В.
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина), Санкт-Петербург

МЕТОД ИДЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ ПО ИЗОБРАЖЕНИЮ ЛИЦА С ПОДСИСТЕМОЙ ПАССИВНОГО ОБНАРУЖЕНИЯ АТАК НА БИОМЕТРИЧЕСКОЕ ПРЕДЪЯВЛЕНИЕ НА БАЗЕ RASPBERRY PI 5

Аннотация. Разработан метод биометрической идентификации пользователей по изображению лица с подсистемой пассивного обнаружения атак на биометрическое предъявление, предназначенный для работы в реальном времени на Raspberry Pi 5. Метод основан на ансамбле предобученных сетей MiniFASNet с усреднением выходов. Экспериментально достигнуты EER = 3,61 % (порог 0,691) для идентификации и ACER = 13,03 % для подсистемы ОАБП.

Ключевые слова: биометрия, обнаружение атак на биометрическое предъявление, изображение лица, биометрическая идентификация.

На основании [1, 2] при реализации многофакторной аутентификации в качестве дополнительного фактора можно использовать биометрию в соответствии с ГОСТ Р 58833–2020. Биометрия в РФ активно применяется [3], зачастую без постоянного операторского

контроля. Злоумышленник может вмешаться в процесс идентификации на этапе биометрического предъявления. Такое воздействие, определенное в ГОСТ Р 58624.1–2019 как атака на биометрическое предъявление (АБП), противопоставляется надлежащему предъявлению (НБП). Для защиты от АБП используется подсистема обнаружения атаки на биометрическое предъявление (ОАБП). В данной работе в качестве метода ОАБП использовалось обнаружение витальности. Их можно разделить на четыре категории: форматы запрос – ответ, запрос – непроизвольный ответ, знание субъекта и часть субъекта, пассивное обнаружение. Пассивное ОАБП может быть использовано в процессе регистрации и не усложняет взаимодействие пользователя с системой.

Для оценки эффективности системы идентификации используются метрики показателей ошибок первого и второго рода, описанные установленные ГОСТ Р 71414.1–2024: FAR, FRR и общепринятая метрика EER [4].

FAR – доля ошибочно предоставленных доступов, показатель ошибки первого рода.

$$FAR=\frac{FP}{FP+TN}, \#\ (1)$$

где FP – количество ложноположительных идентификаций, TN – количество корректно отвергнутых идентификаций.

FRR – доля ошибочных отказов в доступе, показатель ошибки второго рода.

$$FRR=\frac{FN}{FN+TP}, \#\ (2)$$

где FN – количество ошибочно отвергнутых идентификаций, TP – количество корректно принятых идентификаций.

Метрики FAR и FRR зависят от порогового значения τ, определяющего допустимое различие между предъявляемыми и эталонными биометрическими признаками: снижение τ повышает «доверчивость» системы, увеличивая FAR, но снижая FRR. Для порого-независимого сравнения систем используется коэффициент равных ошибок (EER) – точка пересечения кривых FAR и FRR; чем ниже EER, тем выше эффективность разграничения легитимных пользователей и злоумышленников.

Для оценки эффективности подсистемы ОАБП, используются следующие метрики из ГОСТ Р 58624.3–2019: ВОКПА (APCER), вероятность ошибки классификации предъявления при атаке:

$$APCER = \frac{\text{количество АБП, воспринятых в НБП}}{\text{общее количество АБП}}; \#\ (3)$$

ВОКПБП (BPCER), вероятность ошибки классификации подлинных биометрических предъявлений:

$$BPCER = \frac{\text{количество НБП, воспринятых за АБП}}{\text{общее количество НБП}}; \#\ (4)$$

ACER (average classification error rate), средняя вероятность ошибки классификации – комбинированный показатель средней ошибки системы

$$ACER = \frac{APCER + BPCER}{2}. \#\ (5)$$

Обзор литературы (2020–2025 гг.) проводился по запросам «face liveness spoofing presentation attack» с последующим отбором работ, использующих стандартизированные метрики [5]. В соревнованиях LivDet-Face 2021 [6] и 2024 [7] лучшие результаты показали трехкомпонентный ансамбль (ACER=16,47 %), 12-слойная CNN с модулями внимания (ACER=18,71 %), гибридная архитектура EfficientNet+ViT (ACER=5,53 %) и автоэнкодер на базе VGG19 (ACER=9,91 %). Высокую точность также продемонстрировали двухпотоковая сеть LwFLNeT [8] (ACER=0,3 %) и ансамбль легковесных CNN [9] (ACER=2,67 %). Сравнение результатов приведено в таблице 1.

Таблица 1

Сравнительный анализ методов обнаружения витальности

Метод	**APCER, %**	**BPCER, %**	**ACER, %**
LivDet-2021-2 [6]	13,33	24,08	18,71
LivDet-2021-1 [6]	17,61	15,33	16,47
LivDet-2024-2 [7]	0,88	18,93	9,91
LivDet-2024-1 [7]	0,46	10,60	5,53
Ensemble Model [9]	0	5,355	2,67
LwFLNeT [8]	0,2	0,4	0,3

Анализ подтверждает, что максимальную эффективность ОАБП обеспечивают ансамбли моделей, специализирующихся на различных признаках подлинности.

Цель работы – разработка системы идентификации по изображению лица с подсистемой пассивного ОАБП для работы в реальном времени на одноплатных компьютерах в архитектуре БСОВ (вход – изображение с одной камеры). Реализация: Raspberry Pi 5, Python. Ядро ОАБП – ансамбль предобученных MiniFASNet: V2 (масштаб 2,7) анализирует глобальные текстуры, V1SE (масштаб 4,0) – локальные детали лица. Итоговое бинарное решение и показатель уверенности формируются усреднением выходов обеих сетей. В ходе экспериментов для оценки эффективности системы идентификации и подсистемы ОАБП методом случайной выборки была взята часть открытого набора данных CelebA-Spoof [10], состоящая из 3106 субъектов и содержащая в себе как НБП,

так и АБП. Было собрано порядка 3,3 млн. пар для внутриклассовых сравнений и порядка 75 млн. пар для межклассовых сравнений. Было получено оптимальное значение порога 0,691, а значение EER системы составило 3,61%. Для наглядного представления зависимости FAR/FRR от порогового значения построен график (рисунок 1), на котором отмечены точка EER и соответствующее пороговое значение.

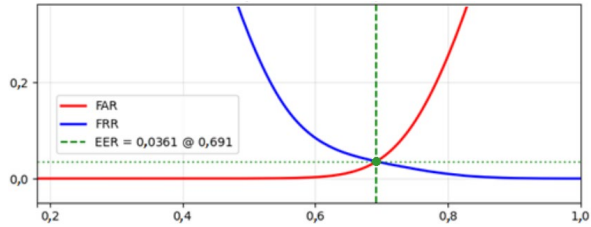


Рис. 1. Полученное значение EER

Для оценки эффективности подсистемы ОАБП, все изображения из тестовой выборки (171 422 изображения, 64 417 – НБП, 107 005 – АБП) последовательно подавались на вход подсистемы ОАБП, которая выносила бинарное решение: «реальное лицо» или «подделка». Были получены численные показатели APCER = 23,88% и BPCER = 2,17%, значение ACER = 13,03%

Итоговая разработанная система имеет ключевые показатели эффективности EER = 3,61% и ACER = 13,03%, сопоставимый с рассмотренными решениями. Система требует дальнейшей модификации, с точки зрения увеличения точности идентификации и снижения ACER подсистемы ОАБП, путем дообучения и точной настройки моделей. В ходе экспериментов подсистема ОАБП обнаружила 76,12% атак, что ведет к значительному снижению вероятности ложного допуска, а низкое значение BPCER в 2,17% оказывает крайне незначительное влияние на вероятность ложного недопуска, что повышает общую защищенность системы.

Список использованных источников:

1. TAdviser. Самые популярные пароли [Электронный ресурс]. URL: https://www.tadviser.ru/index.php/Статья:Самые_популярные_пароли (дата обращения: 01.06.2025).

2. InfoWatch. Россия: утечки информации ограниченного доступа 2023-2024 [Электронный ресурс]. URL: https://www.infowatch.ru/sites/default/files/analytics/files/rossiya-utechki-informatsii-ogranichennogo-dostupa-2023-2024.pdf (дата обращения: 01.06.2025).

3. Единая биометрическая система | Гражданам [Электронный ресурс]. URL: https://ebs.ru/citizens/ (дата обращения: 23.04.2025).

4. Nayak R., Pati U., Das S. A comprehensive review on deep learning-based methods for video anomaly detection // Image and Vision Computing. 2021. Т. 106. С. 104078. DOI: 10.1016/j.imavis.2020.104078.

5. Иконников С.Н., Шкляр Е.В. Методы определения витальности в биометрических системах // XIII научно-практическая конференция с международным участием «Наука настоящего и будущего» для студентов, аспирантов и молодых ученых: сборник материалов конференции (15-17 мая 2025 года, г. Санкт-Петербург). Том 1. – СПб: СПбГЭТУ «ЛЭТИ», 2025. – С. 256.

6. Purnapatra S., Smalt N., Bahmani K., Das P., Yambay D., Mohammadi A., George A., Bourlai T., Marcel S., Schuckers S. Face Liveness Detection Competition (LivDet-Face) – 2021 [Электронный ресурс]. URL: https://livdet.org/face2021-livdet-org/face_2021.pdf (дата обращения: 01.06.2025).

7. Lambert Igene, Afzal Hossain, Mohammad Zahir Uddin Chowdhury, Humaira Rezaie, Ayden Rollins, Jesse Dykes, Rahul Vijaykumar, Alain Komaty, Sébastien Marcel, Stephanie Schuckers. Face Liveness Detection Competition (LivDet-Face) – 2024 // IEEE International Joint Conference on Biometrics (IJCB). 2024. DOI: 10.1109/IJCB62174.2024.10744462.

8. Swapnil R. Shinde, Anupkumar M. Bongale, Deepak Dharrao, Sudeep D. Thepade. An enhanced light weight face liveness detection method using deep convolutional neural network // MethodsX. 2025. DOI: 10.1016/j.mex.2025.103229.

9. Patel A., Haloi M., Salim A., Shekhar S. An Ensemble Model for Face Liveness Detection // arXiv. 2022. DOI: 10.48550/arXiv.2201.08901.

10. CelebA-Spoof [Электронный ресурс]. URL: https://github.com/ZhangYuanhan-AI/CelebA-Spoof (дата обращения 09.04.2026).

Ikonnikov S.N., Shklyar E.V.
Saint Petersburg Electrotechnical
University «LETI», Saint-Petersburg

FACE IMAGE-BASED USER IDENTIFICATION METHOD WITH A PASSIVE PRESENTATION ATTACK DETECTION SUBSYSTEM ON RASPBERRY PI 5

Abstract. A method for biometric user identification based on face images has been developed, including a passive presentation attack detection subsystem, designed for real-time operation on Raspberry Pi 5. The method is

based on an ensemble of pre-trained MiniFASNet networks with output averaging. Experimentally, an EER of 3.61% (threshold 0.691) was achieved for identification, and an ACER of 13.03% for the PAD subsystem.

Keywords: biometrics, presentation attack detection, face image, biometric identification.

УДК 004.056.55

Исмагилова А.С.
Уфимский университет науки и технологий, Уфа

МОДУЛЬНАЯ АРХИТЕКТУРА КРИПТОСИСТЕМЫ НА ОСНОВЕ ОРТОГОНАЛЬНЫХ ИДЕМПОТЕНТОВ

Аннотация. Исследуется вычислительная сложность восстановления секретного ключа в криптосистеме, основанной на сопряжении в группе обратимых элементов ассоциативного кольца с ортогональными идемпотентами. Показано, что алгебраическая декомпозиция кольца на независимые идеалы обеспечивает модульную архитектуру с изолированными доменами доверия. Подтверждена стойкость схемы к классическим и квантовым атакам. При оптимальных параметрах достигается 128-битная защита и реализация гомоморфных операций.

Ключевые слова: ассоциативные кольца, ортогональные идемпотенты, криптографическая стойкость, гомоморфное шифрование.

В современных условиях стремительного развития квантовых вычислительных технологий классические асимметричные криптосистемы находятся под угрозой. Алгоритм Шора доказал принципиальную возможность полиномиального решения указанных задач на квантовых компьютерах [1]. Тем самым возникает задача поиска альтернативных математических методов для постквантовой криптографии [2]. Одним из способов решения данной задачи является алгебраическая криптография, использующая структуры некоммутативных колец и групп [3, 4].

В данной работе исследуется вычислительная сложность восстановления секретного ключа в криптосистеме, построенной на структуре ассоциативных колец с полной ортогональной системой идемпотентов [5, 6]. Основная цель исследования − обоснование криптографической стойкости схемы, основанной на задаче сопряженности в линейных группах.

Для обоснования криптографической стойкости и реализации модульной архитектуры перейдем к формальному алгебраическому описанию.

Пусть R – ассоциативное кольцо, $1/2 \in R$, задана плотная ортогональная система идемпотентов $\{e_i \in R | 1 \leq i \leq n\}$. Пусть $U(R)$ – группа обратимых элементов кольца R, $E(R)$ – элементарная подгруппа группы $U(R)$, порожденная элементами вида $1 + e_i x e_j$ при $x \in R$, $i \neq j$. Для произвольного идеала $I \lhd R$ определим $E(I)$ – нормальную подгруппу в $E(R)$, $C(I)$ – прообраз центра группы $U(R/I)$ при каноническом гомоморфизме $\varphi_I: U(R) \to U(R/I)$.

Ключевым алгебраическим результатом, лежащим в основе архитектуры схемы, является следующее утверждение:

Если $U(R) = G \oplus H$, $G \cap H = \{1\}$, где G, H – нормальные подгруппы, то существуют идеалы $I, J \lhd R$, такие что: $R = I \oplus J$, $E(I) \subseteq G \subseteq C(I) - G$ содержит все элементарные преобразования над I и действует централизованно при факторизации по I. Аналогично $E(J) \subseteq H \subseteq C(J)$.

Процесс шифрования в предлагаемой схеме основан на операции сопряжения элементов в группе обратимых элементов. Пусть сообщение $m \in I$, т.е. $m = eae$. Шифротекст вычисляется по формуле $c = g(1 + m)g^{-1}$, где $g \in G$ – секретный ключ. Элемент c является обратимым в R и маскирует исходное сообщение за счет действия сопряжения. Расшифровка выполняется обратным сопряжением, после чего восстановление m осуществляется проекцией на идеал I путем умножения на идемпотент e слева и справа.

Важным преимуществом данной алгебраической конструкции является возможность реализации частично гомоморфных операций. Умножение шифротекста на центральные элементы из J позволяет реализовывать гомоморфное умножение на публичные скаляры, так как ортогональность идемпотентов гарантирует отсутствие искажений данных в идеале I. А центральность элементов обеспечивает согласованность операций. Таким образом, декомпозиция кольца создает основу для построения модульных криптосистем.

Безопасность схемы определяется вычислительной сложностью восстановления исходного сообщения m или секретного ключа g по известному шифротексту c. Задача сводится к решению уравнения $c = g(1 + m)g^{-1}$ относительно неизвестных g и m что является частным случаем задачи сопряженности в линейных группах над конечными полями.

Рассмотрим конкретную реализацию. Пусть $R = M_n(F_q) \times M_n(F_q)$, идемпотент $e = (I_n, O)$, ключ $g = (P, I_n)$, $P \in GL_n(F_q)$, сообщение $m = (M, O)$, $M^2 = O$. Шифротекст принимает вид $C = P(I_n + M)P^{-1}$.

Знающий C, но не знающий P и M, сталкивается со следующими вычислительными барьерами. Во-первых, поскольку M нильпотентна, матрица $I_n + M$ является унипотентной (все ее собственные значения равны единице). В теории линейной алгебры известно, что все унипотентные матрицы одинакового размера имеют идентичную жорданову форму, что делает невозможным выделение конкретной M стандартными спектральными методами. Во-вторых, даже при гипотетическом знании M, восстановление P не является однозначным: множество матриц, сопрягающих $I_n + M$ в C образует централизатор, размер которого экспоненциально растет с увеличением n. Это исключает возможность эффективного перебора.

Анализ известных классов атак подтверждает устойчивость схемы. Атака полным перебором требует обхода всей группы GL_n порядок которой асимптотически оценивается как q^{n^2}. При параметрах $n \geq 64$, $q \geq 2^{16}$ сложность перебора выходит за пределы вычислительной реализуемости. Атака по известному открытому тексту сводится к поиску сопрягающей матрицы для унипотентных матриц большой размерности, для которой не известно эффективных алгоритмов в общем случае. Линеаризационные и алгебраические атаки приводят к системам полиномиальных уравнений высокой степени с числом переменных порядка n^2.

Важным аспектом является устойчивость к квантовым атакам. В отличие от задач факторизации и дискретного логарифма, задача сопряженности в линейных группах над конечными полями не сводится к задаче о скрытой абелевой подгруппе. Следовательно, алгоритм Шора и его производные неприменимы для ее решения. На сегодняшний день не существует квантовых алгоритмов, способных эффективно решать задачу сопряженности в указанных структурах. При выборе параметров n и q в соответствии с рекомендациями постквантовой криптографии схема обеспечивает стойкость на уровне 128 бит.

Практическая ценность предложенного подхода заключается в возможности построения постквантовых криптосистем с модульной архитектурой, где алгебраическая декомпозиция кольца естественным образом разделяет доверенные домены. Это позволяет разрабатывать протоколы с изолированными зонами ответственности, что особенно актуально для распределенных систем, многоуровневых защищенных сетей и сред с различными уровнями классификации информации.

Дальнейшие исследования могут быть направлены на оптимизацию вычислительной сложности операций сопряжения, а также изучение применимости метода к другим классам ассоциативных алгебр. Также представляет интерес исследование устойчивости схемы к

комбинированным атакам в условиях частичного раскрытия параметров идеала.

Таким образом, в работе обоснована вычислительная сложность восстановления секретного ключа в криптосистеме, основанной на ортогональных идемпотентах и задаче сопряженности в группе обратимых элементов ассоциативного кольца. Предложенная математическая модель обеспечивает естественное разделение ключевого пространства и данных на независимые идеалы, что создает основу для модульных криптографических архитектур с изолированными доменами доверия. Проведенный анализ подтверждает стойкость схемы к атакам полным перебором, по известному открытому тексту, алгебраическим и линеаризационным методам, а также демонстрирует ее принципиальную устойчивость к квантовым вычислениям. При корректном выборе параметров схема гарантирует 128-битную стойкость и обладает потенциалом для реализации частично гомоморфных операций. Полученные результаты могут быть использованы при проектировании защищенных протоколов передачи данных следующего поколения, устойчивых к угрозе квантового превосходства.

Список использованных источников:

1. Shor P.W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer // Foundations of Computer Science: Conference Publications. − 1997. − P. 1484−1509.
2. Пьянков П.Е., Ведерникова О.С., Кротова Е.Л. Сравнение стандартов шифрования // Инновационные технологии: теория, инструменты, практика. − 2017. − Т. 1. − С. 273-279.
3. Романьков В.А. Алгебраическая криптография / В.А. Романьков. – Омск: Омский государственный университет им. Ф.М. Достоевского, 2013. – 136 с. – ISBN 978-5-7779-1600-6.
4. Бабенко Л.К., Маро Е.А. Анализ стойкости блочных алгоритмов шифрования к алгебраическим атакам // Известия ЮФУ. Технические науки. − 2011. − № 12(125). − С. 110-119.
5. Исмагилова А.С. Декомпозиция колец и их применение в алгебраической криптографии / А.С. Исмагилова // Информация и безопасность. – 2025. – Т. 28, № 4. – С. 503-506. – DOI 10.36622/1682-7813.2025.28.4.005.
6. Исмагилова А.С. О вычислительной сложности восстановления секретного ключа в криптосистеме на основе ортогональных идемпотентов / А.С. Исмагилова // Инженерный вестник Дона. – 2026. – № 4(136).

Ismagilova A.S.
Ufa University of Science and Technology, Ufa

MODULAR ARCHITECTURE OF A CRYPTOSYSTEM BASED ON ORTHOGONAL IDEMPOTENTS

Abstract. We study the computational complexity of secret key recovery in a post-quantum cryptosystem based on conjugation in a group of invertible elements of an associative ring with orthogonal idempotents. We demonstrate that algebraic decomposition of the ring into independent ideals provides a modular architecture with isolated trust domains. The system's resistance to classical and quantum attacks is confirmed. With optimal parameters, 128-bit security and homomorphic operations are achieved.

Keywords: associative rings, orthogonal idempotents, cryptographic strength, homomorphic encryption.

УДК 004.94:544.42

Корнилова А.А., Гиззатова Э.Р.
Уфимский университет науки и технологий, Уфа

АППРОКСИМАЦИЯ НЕЛИНЕЙНЫХ ПРОЦЕССОВ КИБЕРУГРОЗ МЕТОДАМИ СИМВОЛЬНОЙ РЕГРЕССИИ

Аннотация. В работе предложен оригинальный междисциплинарный подход к исследованию динамики киберугроз на основе методов химической кинетики. С использованием генетического алгоритма проведена аппроксимация данных об утечках информации за период 2013–2025 гг. Полученные результаты подтвердили высокую адекватность математической модели (R^2 до 0.98), а динамика весовых коэффициентов позволила математически обосновать смену режимов функционирования системы в точках ключевых глобальных трансформаций

Ключевые слова: генетический алгоритм, утечка данных, химическая кинетика, аппроксимация.

Современная эпоха характеризуется глобальной эскалацией киберугроз, приобретающих тотальный масштаб. В 2023 году в мире зафиксировано 11 549 утечек информации, что на 61,5% превышает показатели 2022 года [1]. Рост объема скомпрометированных персональных данных (ПДн) обусловлен интенсификацией хакерской активности на фоне геополитической нестабильности. В 2024 году Российская Федерация заняла второе место в мире по количеству

инцидентов, уступив лишь США. Несмотря на зафиксированное в 2025 году снижение числа утечек на 18% [2], характер угроз становится все более сложным и нелинейным. Это диктует необходимость перехода от простого статистического учета к глубокому математическому моделированию динамики киберугроз методами символьной регрессии.

В [3-4] был разработан программный комплекс для аппроксимации экспериментальных зависимостей сложных химических процессов. В основу метода заложен генетический алгоритм (ГА), позволяющий идентифицировать кинетические закономерности через подбор функций, описывающих фундаментальные типы реакций: нуклеацию, автокатализ, диффузию и др.

Настоящая работа преследует цель адаптировать данный инструментарий для анализа глобальной статистики киберугроз. Основной задачей является моделирование временных рядов количества скомпрометированных ПДн с целью выявления скрытых динамических особенностей. Использование «химических» моделей в данном контексте позволяет не просто аппроксимировать данные, но и диагностировать характер процесса – от линейного накопления до цепного (автокаталитического) распространения угроз. Результаты аппроксимации показал следующие результаты:

Таблица 1

Результаты аппроксимации временных рядов утечек информации по характерным периодам развития

Период	R^2	F2	C1	C2	F1	A2	B1
[2013-2019]	0.98	0.037	0.31	0.65			
[2020-2023]	0.88	0.98		~0	~0		
[2024-2025]	0.91		0.94			0.02	0.04

Анализ динамики весовых коэффициентов позволяет выделить три качественно различающихся этапа эволюции киберугроз:

1. Период [2013-2019 гг.]: Экстенсивное накопление (Кинетика первого и второго порядков). В данный интервал доминируют функции C1 и C2, соответствующие реакциям первого и второго порядков. Это характеризует эволюционный тип роста системы. Увеличение числа инцидентов протекало пропорционально глобальной скорости цифровизации социально-экономических процессов. Отсутствие признаков автокатализа указывает на то, что угрозы носили разрозненный характер, а их динамика определялась преимущественно линейным ростом объема генерируемых данных («цифрового следа»).

2. Период [2020-2023 гг.]: Фаза автокаталитической эскалации (Логистический рост). Смена доминирующего механизма на функцию автокатализа F2 свидетельствует о переходе системы в режим самоускоряющейся реакции. Внешним катализатором выступила пандемия COVID-19 [5] и переход на дистанционные формы работы. Математическая модель фиксирует возникновение положительной обратной связи: каждая успешная компрометация данных облегчала реализацию последующих атак (эффект «цепной реакции»). Система находилась в состоянии «взрывного» роста, при котором интенсивность потока утечек определялась накопленным критическим объемом уязвимостей.

3. Период [2024-2025 гг.]: Структурная трансформация и нуклеация. Результаты аппроксимации фиксируют резкое снижение вклада автокатализа и рост значимости функций диффузии (B1) и нуклеации (A2). Это указывает на качественное изменение топологии угроз: от сплошного фронтального роста система перешла к очаговому распределению. Появление «ядер» (нуклеация) объясняется концентрацией атак на критически важных узлах – государственных инфраструктурах и стратегических ИТ-хабах в условиях геополитической турбулентности. Снижение количественных показателей в 2025 году интерпретируется не как деградация угрозы, а как фазовый переход системы к более сложной, таргетированной структуре «кристаллизации» инцидентов.

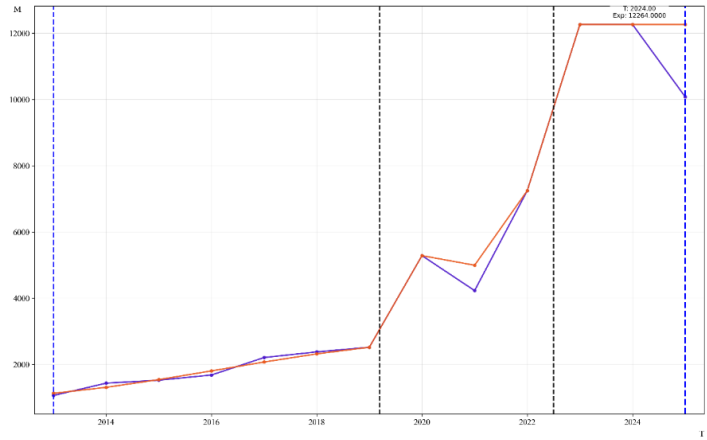


Рис. 1. Результат работы программного комплекса (синяя линия – статистические данные, красная – расчет, пунктирные линии – временные периоды)

Проведенное моделирование выявило фундаментальную трансформацию природы киберугроз: от линейного роста (2013-2019 гг.) через фазу «автокаталитического взрыва» (2020-2023 гг.) к современной очаговой нуклеации (2024-2025 гг.). Снижение количества утечек в 2025 году, зафиксированное моделью через функции диффузии и нуклеации, интерпретируется не как ослабление векторов атак, а как их концентрация на критических узлах инфраструктуры. Это требует пересмотра стратегий информационной безопасности в сторону защиты «ядер» (центров кристаллизации рисков).

Список использованных источников:

1. Утечки информации в мире, 2022–2023 годы: отчет / Экспертно-аналитический центр InfoWatch. – 2024. – URL: infowatch.ru (дата обращения: 17.04.2025). – Текст: электронный.

2. Не победа ИБ: количество утечек персональных данных в 2025 г. снизилось, но не благодаря ИБ // ComNews: информационный портал. – 2026. – 13 марта. – URL: https://www.comnews.ru/content/244202/2026-03-13/2026-w11/1008/ne-pobeda-ib-kolichestvo-utechek-personalnykh-dannykh-2025-g-snizilos-no-ne-blagodarya-ib (дата обращения: 17.04.2025). – Текст: электронный.

3. Программный комплекс сегментированного моделирования данных по термической деструкции генетическим алгоритмом: свидетельство о государственной регистрации программы для ЭВМ № 2026616287 Рос. Федерация / Э. Р. Гиззатова, С. И. Никонова, А. А. Корнилова; заявитель и правообладатель ФГБОУ ВО «Уфимский университет науки и технологий». – № 2026615000; заявл. 03.03.2026; опубл. 05.03.2026.

4. Программа для интеллектуального анализа кинетических закономерностей полимерных систем на основе методов глобальной оптимизации: свидетельство о государственной регистрации программы для ЭВМ № 2026616598 Рос. Федерация / Э. Р. Гиззатова, С. И. Никонова, А. А. Корнилова; заявитель и правообладатель ФГБОУ ВО «Уфимский университет науки и технологий». – № 2026615500; заявл. 03.03.2026; опубл. 10.03.2026.

5. Корнилова, А. А. Обзор кибератак в период пандемии Covid-19 / А. А. Корнилова, Д. С. Юнусова // 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. 25-27. – DOI 10.33184/itokbco-2021-05-21.4.

Kornilova A.A., Gizzatova E.R.
Ufa University of Science and Technology, Ufa

APPROXIMATION OF NONLINEAR CYBER THREAT PROCESSES USING SYMBOLIC REGRESSION METHODS

Abstract. The paper proposes an original interdisciplinary approach to studying the dynamics of cyber threats based on chemical kinetics methods. Using a genetic algorithm, data on information leaks for the period 2013–2025 were approximated. The results confirmed the high adequacy of the mathematical model (R^2 up to 0.98), while the dynamics of the weight coefficients provided a mathematical justification for the shift in system operation modes at points of key global transformations.

Keywords: genetic algorithm, data leakage, chemical kinetics, approximation.

УДК 004.056

Лушников Н.Д.
Уфимский колледж радиоэлектроники, телекоммуникаций и безопасности, Уфа
Исмагилова А.С.
Уфимский университет науки и технологий, Уфа

ПЕРСПЕКТИВЫ ПРИМЕНЕНИЯ ИННОВАЦИОННЫХ ПРОГРАММНО-АППАРАТНЫХ КОМПЛЕКСОВ В ЦИФРОВОМ ОБЩЕСТВЕ

Аннотация. В данной статье приведены сведения о перспективах развития применяемых программно-аппаратных комплексов в области информационной безопасности и защиты информации в цифровом обществе. В ходе проведенного исследования рассмотрены модели и алгоритмы биометрической аутентификации на основе нейронных сетей, методы и принципы шифрования на базе программно-аппаратного комплекса с применением квантовых технологий.

Ключевые слова: биометрическая аутентификация, квантовые технологии, шифрование.

В современном обществе к числу наиболее актуальных проблем следует отнести вопрос обеспечения безопасности используемых данных от несанкционированных действий. Несмотря на изобилие применяемых инструментов защиты информации стоит признать, что векторы атак злоумышленников становятся наименее тривиальными. Для реагирования

на данные тенденции всем сегментам (B2C, B2B и B2G) следует применять инновационные комплексы защиты информации, которые позволят нейтрализовать угрозы и нивелировать потенциальные риски воздействия на информационно-телекоммуникационные системы.

Для повышения уровня защищенности информационных ресурсов и минимизации уровня воздействия потенциальных рисков, угроз применяются мультимодальные системы биометрической аутентификации.

Распознавание пользователей информационной системы неразрывно связано с понятиями «точность» и «достоверность». Для повышения показателей точности и достоверности необходимо применение нескольких биометрических признаков [1].

В ходе проведенного исследования были разработаны модели биометрической аутентификации по изображению лица и по голосу на основе нейросетевых технологий (Рис.1, Рис.2).

В рамках данного исследования разработана архитектура сверточной нейронной сети на основе конкатенации вектора признаков изображений лица и голоса. Разработан программный модуль распознавания пользователей информационных систем по биометрическим характеристикам, который позволит защитить биометрические персональные данные пользователей информационной системы от несанкционированного доступа.

Сверточная нейронная сеть на основе конкатенации векторов признаков (изображение лица и голос) достигает показателей точности обучения 99,31 % и функции потерь = 0,032, что позволяет повысить надежность процедуры распознавания пользователей информационной системы.

Разработаны мультимодальная система биометрической аутентификации пользователей информационной системы на основе нейронных сетей и программный комплекс данной системы, позволяющие осуществить разграничение доступа пользователей информационной системы [2].



Рис. 1. Модель биометрической аутентификации пользователей информационной системы по изображению лица



Рис. 2. Модель биометрической аутентификации пользователей информационной системы по голосу

В основе защиты информации применяются защищенные сетевые сегменты, ключевая информация с применением криптосистем и методов

шифрования [3]. Для обеспечения высоконадежной защиты информации и высокоскоростной пакетной передачи данных применяются квантовые технологии.

Квантовые технологии основаны на принципе передатчик Алиса – приемник Боб и перехватчик Ева.

Передатчик Алиса состоит из источника фотонов и модулятора поляризации света, включающего:

– полуволновую пластину ($\lambda/2$), которая поворачивает поляризацию на удвоенный угол;

– четверть волновую пластину ($\lambda/4$), которая преобразовывает линейную поляризацию в эллиптическую и обратно с произвольным коэффициентом поляризации [4].

Приемник Боб состоит из:

– преобразователя поляризации с волновыми пластинами $\lambda/2$ и $\lambda/4$. Волновая пластина $\lambda/2$ поворачивает поляризацию на удвоенный угол. Затем волновая пластина $\lambda/4$ преобразовывает эллиптическую поляризацию в линейную;

– поляризационного светоделителя. Свет попадает в светоделитель и передается к обоим выходам с некоторой вероятностью. Сигнал на выходе каждого фотодетектора PD пропорционален мощности падающего на него света. Полученные значения интерпретируются в биты, соответствующие правилам протокола (0, 1 или неопределенность X) [4].

В программном симуляторе квант света, попадающий на фотодетектор, вычисляется с помощью генератора случайных чисел, рассчитанных на вероятности выхода фотона из куба.

Устройство аппаратной платформы симулятора квантового распределения ключей представлено на рисунке 3. Программная часть программно-аппаратного комплекса квантового распределения ключей включает в себя приложение ViPNet QKDSim, которое позволяет подобрать необходимую конфигурацию углов и составить собственный протокол или модификацию протокола.

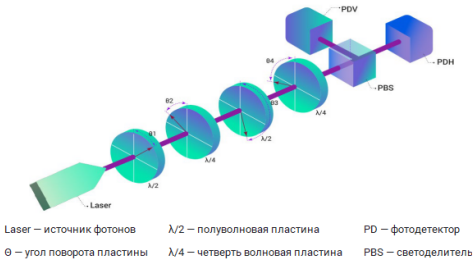


Рис. 3. Симулятор для системы квантового распределения ключей

Дальнейшее исследование в области квантового распределения ключей будет включать следующие основополагающие теоретические и практические разделы:

- комплексные числа;
- гейт Адамара [5];
- принцип суперпозиции;
- юстировка данных [6].

Изучение данных разделов необходимо для проведения исследования, которое направлено на минимизацию показателя QBER (Quantum Bit Error Rate, коэффициент квантовых ошибок). Данный базовый показатель в квантовой криптографии отражает процент ошибочно принятых фотонов (кубитов) по отношению к общему количеству переданных в квантовом канале связи [7].

Таким образом, современные проблемы в области защиты информации требуют современных решений, которые интерпретированы в виде разработки инновационных инструментов на основе наукоемких исследований.

Список использованных источников:

1. Шелупанов А.А. Идентификация и аутентификация в цифровом мире: монография / А.Г. Сабанов, А.А. Шелупанов. – М.: Горячая линия – Телеком, 2022 – 356 с.: ил. – ISBN 978–5–9912–0976–2. – (Серия «Технологии доверенного взаимодействия»).

2. Лушников Н.Д. Модели и алгоритмы мультимодальной биометрической аутентификации на основе сверточной нейронной сети: дис. ... канд. техн. наук: 2.3.6 / Лушников Никита Дмитриевич. – Уфа, 2026. – 188 с.

3. Бабаш А.В. Криптографические методы защиты информации: учебник для вузов / А.В. Бабаш, Е.К. Баранова. – Москва: КноРус, 2016. – 189 с.

4. Комплект документации ViPNet QKDSim: [Программный комплекс симуляции квантового распределения ключей] / АО «ИнфоТеКС». – Москва, 2023. – Режим доступа: свободный. – URL: https://infotecs.ru/products/vipnet-qkdsim/ (дата обращения: 10.04.2026).

5. Нильсен М.А., Чанг И.Л. Квантовые вычисления и квантовая информация. – М.: Мир, 2006. – 824 с.

6. Гайдаш А.А., Наседкин Б.А., Самсонов Э.О., Савельева С.В. Квантовые технологии: учебно-методическое пособие. – Санкт-Петербург: Университет ИТМО, 2022. – 73 с.

7. Elboukhari et al. Quantum Key Distribution Protocols: A Survey // International Journal of Universal Computer Sciences. – 2010.

Lushnikov N.D.
Ufa College of Radioelectronics,
Telecommunications and Security, Ufa
Ismagilova A.S.
Ufa University of Science and Technology, Ufa

PROSPECTS FOR THE APPLICATION OF INNOVATIVE HARDWARE-SOFTWARE SYSTEMS IN A DIGITAL SOCIETY

Abstract. This article outlines the development prospects for hardware-software systems used in information security and data protection within the digital society. The study examines neural network-based biometric authentication models and algorithms, as well as encryption methods and principles implemented via hardware-software systems utilizing quantum technologies.

Keywords: biometric authentication, quantum technologies, encryption.

УДК 347

Мхитарян А.С.
Западно-Уральский институт экономики и права, Пермь

АКТУАЛЬНЫЕ СРЕДСТВА ОБЕСПЕЧЕНИЯ СОХРАННОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ РАБОТНИКОВ В КИБЕРСРЕДЕ

Аннотация. Персональные данные работника как никогда прежде сталкиваются с рядом угроз в отношении их сохранности. Защита персональных данных работника напрямую влияет на возможность работника быть защищенным не только в киберсреде, но и в реальном правовом поле. Автор приходит к выводу о том, что существующие меры по сохранности персональных данных работников в российской правовой системе необходимо постоянно совершенствовать в связи со стремительным развитием технологий.

Ключевые слова: персональные данные работника, информация, кибербезопасность, киберсреда

Сегодня информация как никогда является уязвимым объектом посягательства со стороны недобросовестных лиц: данные о каждом из нас могут потенциально перейти из разряда конфиденциальных в общедоступные, становясь доступными широкому кругу лиц без нашего согласия.

Риски разглашения персональных данных сотрудников во многом связаны со следующими существующими угрозами: непрерывное и

стремительное совершенствование технологий; заинтересованность работодателя к использованию современных средств обработки персональных данных, к примеру, средств считывания сетчатки глаза или отпечатка пальцев работника на рабочем месте, которые парадоксальным образом, не гарантируют безопасности данных, а напротив, повышают риск утечки данных; безответственность и халатность сотрудников, в особенности, работающих в отделе кадров, к сохранности данных; элементарное незнание работниками законодательства по защите данных; отсутствие в иерархии компании вакансии по назначению специального сотрудника, компетентного за сохранность данных всего персонала; нежелание работников следовать четким инструкциям по соблюдению сохранности данных; рост случаев «фишинговых» атак; чрезмерное доверие персонала злоумышленникам, ввиду использования последними психологических методов в общении для предоставления сотрудниками актуальной информации о коллегах или о компании.

Среди актуальных средств и методов по борьбе с разглашением данных сотрудников можно считать наиболее подходящими следующие:

1. **внедрение обучения персонала базовым знаниям и навыкам по сохранности данных**, а также использованию законодательства в указанной области. Такие уроки правовой грамотности, проводимые работодателем в конкретном учреждении, действительно оказывают **положительное влияние на сферу сохранности данных. Об** этом, в частности, свидетельствуют зарубежные авторы, называя статистические данные: обучение персонала кибербезопасности позволило снизить число инцидентов нарушения безопасности на 50% в течение первых двух лет. Между тем, помимо обучения персонала кибербезопасности, следует также внедрять системы аудита и мониторинга активности сотрудников, чтобы минимизировать человеческие ошибки, которые могут привести к утечкам данных [2];

2. **цифровая гигиена и минимизация данных**. О цифровой гигиене, столь необходимой в правовом и **киберпространстве** в последнее время говорят все больше. Она подразумевает не только осознанное ограничение субъектом персональных данных объема информации о себе, выставляемой в общем информационном доступе, но и разумные меры по предупреждению возможных взломов устройств, содержащих соответствующую охраняемую законом информацию о работнике. Сегодня цифровая гигиена изучается в рамках повышения правовой культуры даже в общеобразовательных учреждениях. Минимизация данных – конкретная законодательная мера, направленная на процесс обработки только нужной актуальной информации о сотруднике, исключающей сбор и обработку иной, излишней информации с целью предотвращения угрозы разглашения данных [4];

3. **использование средства шифрования данных**, **подразумевающее** преобразование информации открытого текста в нечитаемую форму, известную как зашифрованный текст, с использованием криптографических алгоритмов [1]. Такой метод во многом связан с новейшими разработками и технологиями, которые простому обывателю недоступны. В связи с этим повышается вероятность сохранности данных, поскольку далеко не каждый человек способен применить подобную технологию для распознавания актуального текста;

4. **совершенствование законодательства**. Действующее законодательство правовой системы России весьма **эффективно** регулирует защиту персональных данных работников. В частности, помимо специального Федерального закона «О персональных данных», целая гл. 14 Трудового кодекса РФ посвящена вопросу сохранности данных работников. Между тем, в настоящий момент в законодательстве не содержится актуальной регламентации конкретных видов персональных данных работника, что повышает риски незнания работниками и работодателями информации, охраняемой законодательством;

5. **расширение доктринального и законодательного толкования** объема защищаемой законом информации о работнике. Некоторые авторы призывают включать в категорию «персональные данные работника» не только общеизвестные данные (имя, фотография и почта сотрудника, религиозные убеждения и состояние здоровья), но также его местоположение, разговоры с клиентами и даже сплетни между коллегами [3]. Такой подход, в частности, позволяет расширить границы представления о категории персональных данных, добавляя в них не только ту информацию, которой работник обладал еще при трудоустройстве на работу, но и те его действия, которые непосредственно затрагивают исполнение им трудовой функции, т.е. позволяет защищать те сведения, которые возникают на рабочем месте и вне его. таким образом, персональные данные работника – это не только личная информация о самом работнике, но и те сведения, которые могут каким-либо образом быть связаны с его персоналией и одновременно влиять на репутацию работодателя, клиентов, иных лиц, связанных с трудовыми правоотношениями [5].

Только комплексный и многогранный подход к сохранности персональных данных сможет гарантировать безопасность в отношении защиты персональных данных работника на рабочем месте. Зачастую все задействованные случаи утечки персональных данных связаны с единственной главной проблемой – уверенность лиц в том, что нематериальные блага (различные виды информации, относящиеся

непосредственно к категории персональные данные) существуют, функционируют и изменяются вне правового сознания реальных физических лиц. Между тем, настоящее исследование доказывает, что защита данных сегодня – это не только важнейшая мера на пути к безопасной киберсреде, но и к нормальному функционированию в обществе самого индивида, которому эти данные принадлежат от рождения.

Список использованных источников:

1. Кадомец К.С. Защита персональных данных с помощью шифрования // E-Scio. 2023. №5 (80). URL: https://cyberleninka.ru/article/n/zaschita-personalnyh-dannyh-s-pomoschyu-shifrovaniya (date of access: 19.04.2026).

2. Maulidar Maulidar, Edi Wanda, Maudi Hijriatin. Cybersecurity awareness in HR: protecting employee data in the digital era. International journal of engineering science and information technology. 2025.

3. Matthew T. Bodie. The law of employee data: privacy, property, governance URL: https://www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=11448&context=iljs.714. (date of access: 19.04.2026).

4. Prabu Manoharan. Review on cybersecurity in HR systems: protecting employee data in the age of AI. International journal of advanced research in science communication and technology. 2024.

5. Jefferson Graham & Laura Schulte, Wisconsin workers embedded with microchips, USA TODAY (Oct. 15, 2017, 8:49 AM), URL: https://www.usatoday.com/story/tech/talkingtech/2017/08/01/wisconsin-employees-got-embedded-chips/529198001/ [https://perma.cc/RV6M-J5ZD]. (date of access: 19.04.2026).

Mkhitaryan A.S.
West Ural Institute of Economics and Law, Perm

CURRENT MEANS OF SECURING EMPLOYEE PERSONAL DATA IN THE CYBER ENVIRONMENT

Abstract. Employee personal data faces a number of security threats as never before. Protecting employee personal data directly impacts their ability to be protected not only in the cyber environment but also in the legal framework. The author concludes that existing measures to protect employee personal data in the Russian legal system must be continually improved due to rapid technological advances.

Keywords: employee personal data, information, cybersecurity, cyber environment.

УДК 004

Салов И.В., Шагапов И.А.
Уфимский университет науки и технологий, Уфа

ИДЕНТИФИКАЦИЯ ЧЕЛОВЕКА ПО КОСВЕННЫМ ПРИЗНАКАМ

Аннотация. Развитие современных технологий привело к возникновению нового класса угроз – утрату приватности через косвенные каналы. Wi-Fi устройства, умные часы, фитнес-браслеты и другие устройства получают данные, которые после обработки с помощью нейросетей и глубокого обучения. могут позволить с большой вероятностью идентифицировать человека.

Ключевые слова: Wi-Fi CSI-матрица, CSI-спектрограмма, идентификация, приватность.

Термин «идентификация» в области информационной безопасности чаще всего понимается как первый этап доступа к информационной системе, когда пользователь сообщает свое «имя». В результате чего пользователь, вернее процесс, который запустил пользователь, получает идентификатор, который затем в этой системе и используется. Затем уже идет процесс аутентификации и так далее. Однако, в области криминалистике, это установление тождества объекта (человека, документа, вещества) на основе сравнения его характеристик с уже известными образцами. Почему эта формулировка становится важным и как она может повлиять на информационную безопасность в современном мире?

Определить человека, не желающего представляться, то есть сохранить приватность в информационной системе (чаще всего в сети интернет), научились довольно давно. Речь идет о так называемом «цифровом отпечатке» или «цифровом двойнике». Суть технологии заключатся в сборе общедоступной информации, которую передает программное обеспечение по запросу, например, сайта. В нее включается наименование браузера, информация о версии операционной системы, версии видеодрайверов и т.д. При, казалось бы, безобидности данной информации, набор у каждого человека получается довольно уникальный. Что позволяет достаточно точно идентифицировать человека. Официально, данная идентификация использовалась для создания так называемого «индивидуального рекламного профиля».

Однако, технологии не стоят на месте и в современном мире можно идентифицировать человека не только в информационной системе, но и в реальном мире. Первое, что приходит в голову, это предъявление каких-либо идентификаторов, таких как банковские карты и т.п. И видеокамеры

с их идентификацией по базе данных. Конечно, данная информация используется сейчас, в том числе, для разведывательной фазы в ходе подготовки атаки на информационную систему. Но, кроме указанных, есть и менее очевидные, действенные методы идентификации, которые позволяют отслеживать человека без использования камер видеонаблюдения и компрометации его устройств на программном уровне.

Одним из таких методов является идентификация по радиотражению Wi-Fi сигнала (Wi-Fi Sensing). Количество Wi-Fi устройств вокруг современного человека превысило все разумные пределы. И, поскольку в городе сложно найти место, где Wi-Fi сигнал отсутствует, появилась идея использовать данный сигнал для получения информации о человеке. Конечно, основной смысл Wi-Fi устройств в передаче информационного сигнала. Тем не менее, кроме информационной составляющей, любые сигналы несут служебную и вспомогательную информацию. Радиоволны микроволнового диапазона в Wi-Fi устройствах подвержены эффекту многолучевого распространения (Multipath Propagation): сигнал отражается от стен, мебели и людей [1]. Современные протоколы Wi-Fi (начиная с 802.11n), использующие технологию MIMO (Multiple Input Multiple Output) и OFDM-модуляцию, позволяют извлекать информацию о состоянии канала, которая описывает амплитудные и фазовые искажения сигнала для каждой поднесущей частоты (Channel State Information, CSI-матрица) [2]. Человеческое тело, является отличным поглотителем и отражателем радиоволн. Любое движение человека в зоне покрытия Wi-Fi (между роутером и принимающим устройством) вызывает уникальные, математически описываемые возмущения. Причем, этот метод позволяет получать информацию даже сквозь стены.

Нейросети и машинное обучение позволили усложнить алгоритмы обработки информации, получаемой из CSI-матриц. Так появился еще один метод косвенной идентификации человека с использованием Wi-Fi сигнала, идентификация по походке и микромоторике. Исследования на стыке области информационной безопасности, искусственного интеллекта и машинного обучения доказали, что анализ изменений CSI позволяет распознавать паттерны человеческой походки (Gait Recognition). Походка является уникальным биометрическим маркером, зависящим от длины конечностей и мышечной моторики. Чувствительность современных Wi-Fi приемников позволяет фиксировать не только особенности походки, но и микроскопические движения грудной клетки при дыхании и сердцебиении, когда человек неподвижен. А алгоритмы глубокого обучения (например, сверточные нейросети – CNN), анализируя спектрограммы CSI, способны

идентифицировать человека в группе до 20 лиц с точностью свыше 96–98% (например, алгоритмы GaitSense и Gate-ID) [3].

Еще одним методом идентификации по косвенным признакам является цифровой дактилоскопический отпечаток (Device Fingerprinting) уникального набора носимых радиоэлектронных устройств. Любой современный человек носит с собой внушительный набор электронных устройств, таких как смартфон, умные часы и фитнес-браслет, RFID-карты и RFID-метки, смарт-карты, TWS-наушники и т.п.

Даже если смартфон не подключен к сети, он непрерывно отправляет широковещательные запросы (Probe Requests) для поиска знакомых точек доступа. Эти пакеты содержат не только MAC-адрес, но и Information Elements (IE): параметры чипсета, поддерживаемые скорости, а иногда и списки ранее использованных сетей (Preferred Network List, PNL). Это позволяет составить некий набор информации о человека.

Носимая электроника, работающая в Bluetooth диапазоне, генерирует BLE-маячки (Advertisements) сотни раз в минуту. Например, экосистема Apple использует BLE для работы сервисов Continuity, Handoff, AirDrop и Find My. Умные часы и фитнес-трекеры, находясь на руке, постоянно «пингуют» смартфон, выдавая присутствие владельца и даже уровень заряда батареи его гаджетов. Для защиты от трекинга разработчики (Apple, Google) внедрили MAC-рандомизацию: устройства регулярно меняют свой MAC-адрес. Однако для IT-специалиста этот механизм легко обходится. Один из путей обхода заключается в использовании счетчиков пакетов (Sequence Numbers). Программные тайминг-атаки позволяют связать старый и новый MAC-адрес в непрерывную цепочку, анализируя постоянное возрастание порядкового номера кадра (Sequence Number) до и после смены адреса. Кроме того, аппаратное обеспечение (генераторы тактовой частоты) имеет микроскопические производственные дефекты (Hardware Imperfections). Это порождает дрейф синхронизации (Clock Skew) или смещение несущей частоты (Carrier Frequency Offset). Исследования показывают, что анализ этих отклонений (например, система BTrack) позволяет отслеживать конкретный чип смартфона или часов с точностью до 97 процентов, игнорируя любые программные смены MAC-адресов. Ну и такие события, как BAT-атаки (Bluetooth Address Tracking), показали, что логические ошибки в спецификации BLE позволяют злоумышленнику связывать случайные адреса и воспроизводить данные жертвы [4].

Приведенные в качестве примера два метода утраты приватности при использовании косвенных признаков, представляют серьезную угрозу. И методы борьбы с этими угрозами не являются простыми.

Так, в качестве методов защиты для предотвращения анализа CSI, можно предложить использование радиофизических средств защиты (клетки Фарадея, радиопоглощающие материалы). Конечно, организационные меры (хранение персональной носимой электроники в специальных экранирующих боксах вне режимных помещений). В перспективе, модификация используемых протоколов (применение динамического изменения мощности передачи и внедрение криптографических методов для защиты BLE-адресов от деанонимизации.

Список использованных источников:

1. Zhang, Y., et al. Y. Zhang, Y. Zheng, G. Zhang, K. Qian, C. Qian, and Z. Yang, «GaitSense: Towards ubiquitous gait-based human identification with Wi-Fi», «GaitSense: На пути к повсеместной идентификации человека по походке с помощью Wi-Fi».ACM Trans. Sensor Netw., vol. 18, no. 1, pp. 1–24, Feb. 2022.

2. F. Hong, X. Wang, Y. Yang, Y. Zong, Y. Zhang, and Z. Guo, «WFID: Passive device-free human identification using WiFi signal», «WFID: Пассивная идентификация человека без использования устройств с помощью сигнала Wi-Fi».i n Proc. 13th Int. Conf. Mobile Ubiquitous Syst., Comput., Netw. Services (MOBIQUI-TOUS), Nov. 2016, pp. 47-56.

3. Wu, C., et al. «Multiple People Identification Through Walls Using Off-The-Shelf WiFi», «Идентификация нескольких человек сквозь стены с использованием стандартных беспроводных интерфейсов Wi-Fi». https://www.researchgate.net/publication/346885587_Multiple_People_Identification_Through_Walls_Using_Off-The-Shelf_WiFi University of California. November 2020.

4. Cunha, M., et al. «On the Difficulty of NOT being Unique: Fingerprinting Users from Wi-Fi Data in Mobile Devices», «О сложности НЕ быть уникальным: идентификация пользователей по данным Wi-Fi в мобильных устройствах». https://www.dcc.fc.up.pt/~joaovilela/publications/sac2025.pdf. April 2025.

Salov I.V., Shagapov I.A.
Ufa University of Science and Technology, Ufa

HUMAN IDENTIFICATION BY INDIRECT SIGNS

Abstract. The development of modern technologies has led to the emergence of a new class of threats: loss of privacy through indirect channels. Wi-Fi devices, smartwatches, fitness trackers, and other devices receive data

that, after processing using neural networks and deep learning, can allow for a high degree of identification.
Keywords: Wi-Fi, CSI matrix, CSI spectrogram, identification, privacy.

УДК 004.056

Сенцова А.Ю.
Уфимский университет науки и технологий, Уфа

ОСНОВНЫЕ ТЕНДЕНЦИИ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 2026 ГОДА

Аннотация. В статье рассматриваются основные тенденции в области информационной безопасности, которые по прогнозам аналитиков, будут актуальны в 2026 году. Также внимание уделяется некоторым общим характерным чертам, присущим атакам прошлого года. Даются рекомендации компаниям для построения системы защиты, которая учитывала наиболее актуальные угрозы информационной безопасности.
Ключевые слова: информационная безопасность, угрозы, искусственный интеллект, киберустойчивость, деструктивное воздействие, агентные ИИ, модель нулевого доверия, Secure by Design, социальная инженерия, дипфейк.

На сегодняшний день классическая схема построения системы защиты организации, которая делала ставку на превентивные меры, может терять свою эффективность. 2025 год показал, что даже компании с серьезными финансовыми вложениями в защищенность собственной инфраструктуры, а тем более компании, показывающие высокий уровень цифровизации своих бизнес-процессов, не всегда справляются с вызовами в области информационной безопасности.

Успешные атаки на компании в прошлом 2025 году имели несколько общих характерных черт, среди которых можно выделить:

1. Повсеместное использование злоумышленниками инструментов для атаки с поддержкой искусственного интеллекта. Это позволяет злоумышленникам сократить затраты на атаку и снизить требования к необходимым навыкам.
2. Все более широкое использование самописных эксплойтов для проведения атак, и в частности, для деструктивного воздействия на систему.
3. Активное использование скомпрометированных вендоров, производителей различного оборудования, представителей технической поддержки, чьи инфраструктуры уже были скомпрометированы, что в

дальнейшем может быть использовано злоумышленником как плацдарм для проведения атаки на более серьезные объекты, в том числе промышленные объекты и значимые объекты критической информационной инфраструктуры.

Со стороны компаний, желающих обеспечить безопасность своего бизнеса, вектор развития сменился в сторону обеспечения киберустойчивости. Киберустойчивость – способность организации непрерывно предоставлять свои услуги и выпускать продукты, несмотря на любые неблагоприятные киберинциденты, путем активной подготовки к ним, планирование защитных мер, обнаружения и реагирования на инциденты, а также восстановления организации после атак [1]. Кроме того, специалисты отмечают, что атаки, с целью нанесения материального ущерба сейчас уходят на второй план, уступая атакам, целью которых является декструктивное воздействие на объект, инфраструктуру, ресурсы компаний [2].

Активное использование во всех отраслях искусственного интеллекта (как в ИТ-инфраструктурах, так и для проведения атак злоумышленниками), активная цифровая трансформация бизнеса приводят к появлению новых, ранее неизвестных угроз нарушения информационной безопасности. Также можно отметить, что современные классические средства защиты теряют свою эффективность и плохо справляются с вызовами в области ИБ. Основные последствия успешных атак 2025 года, их характерные черты, а также развитие IT-технологий в целом, дают возможность спрогнозировать и четко сформулировать возможные тенденции в области информационной безопасности в 2026 году.

1. Дальнейшее использование искусственного интеллекта как инструмента поддержки злоумышленника при проведении атак, со смещением вектора в сторону использования агентного искусственного интеллекта (ИИ). Агентные ИИ – автономные системы, способные самостоятельно проводить таргетированные атаки, заниматься планированием и разработкой сценариев атак, а также использовать различные вспомогательные инструменты. Главной особенностью агентных ИИ является возможность принимать решения с минимальным участием человека. Все это упрощает реализацию сценариев атак, однако также может привести к неконтролируемым и непредсказуемым действиям со стороны самих агентов.

2. Уход от простой квантовой криптографии для обеспечения безопасности данных в сторону постквантовой криптографии. Постквантовая криптография является новым поколением криптографических алгоритмов, проявляющих высокую степень устойчивости к квантовым атакам, которые проводятся с помощью

квантовых машин. Хотя сейчас использование инфраструктуры квантовой криптографии является довольно дорогостоящим, специалисты рекомендуют хотя бы попытаться постепенно уходить к данным алгоритмам шифрования в силу того, что с приходом достаточно производительных квантовых компьютеров классические системы шифрования перестанут является надежным средством обеспечения конфиденциальности и целостности данных [3].

3. Развитие центров мониторинга IT-среды организаций (SOC) с целью предотвращения инцидентов информационной безопасности в круглосуточном режиме. SOC активно использовались и ранее, сейчас же потребность рынка в них возрастает в геометрической прогрессии. Причем, главными тенденциями в сфере развития SOC были и остаются: анализ данных, реагирование на инциденты, предотвращение ущерба, круглосуточный режим работы, высокая степень автоматизации, возможность учесть специфику объекта защиты.

4. Использование модели нулевого доверия (Zero Trust), в которой каждый запрос пользователя к информации подвержен дополнительной проверке, даже для уже авторизованного пользователя. Похожая практика уже активно применялась в операционных системах Windows, где пользователи, включая администратора, работали изначально с минимальными привилегиями, а для выполнения задач, для которых требовалось повышение привилегий, маркер администратора выдавался с проверкой и на определенную операцию (либо на определенный момент времени) [4].

5. Плавный переход к проектированию элементов инфраструктуры и сетей с точки зрения подхода Secure by Design, который, по мнению специалистов, в будущем должен стать фундаментом при разработке любого сервиса, проектировании сети компании, умного дома и разработке «умных вещей». Информационная безопасность в обозримом будущем не должна быть просто надстройкой над системой, сетью, приложением или сервисом, а должна быть внедрена с самого начала жизненного цикла устройства или системы, а также должна отвечать требованиям непрерывности и сквозного наложения на весь жизненный цикл систем и устройств, то есть, безопасность закладывается в конечный продукт с самого начала. Главным принципом подхода Secure by Design, к которому стремятся сейчас разработчики IT-систем: проще и безопаснее внедрить функции безопасности сразу, на этапе проектирования, чем потом надстраивать систему защиты информации, а также устранять уязвимости и последствия атак [5].

6. Благодаря использованию искусственного интеллекта различные виды социальной инженерии переживают процесс перехода на новый эволюционный уровень. Фишинг, дипфейки и другие виды социальной

инженерии сейчас, опираясь на проведенный ИИ анализ больших данных, социальный сетей, общедоступной информации, становятся одним из самых доступных инструментов злоумышленника при разработке сценария атаки. В совокупности с отсутствием действующей нормативной правовой базы РФ в области ограничений искусственного интеллекта, методы социальной инженерии становятся подходами, которые могут привести к реализации серьезных атак.

Таким образом, основные направления развития информационной безопасности меняют вектор подходов защиты IT-инфраструктуры компании от простых технических решений и необходимости соответствия требованиям регуляторов к устойчивости бизнеса в рамках развития новых технологий и появления новых угроз. Современная система защиты должна обеспечивать все эти аспекты. Необходимо учитывать сложность инфраструктуры предприятия (возможность удаленной работы, ЦОД и тонкие клиенты, вендоров и поставщиков оборудования и т.д.), внедрять новые технологии, такие как Zero Trust, Secure by Design и ИИ для построения защищенной информационной инфраструктуры. Кроме того, необходимо регулярно проводить аудит информационной безопасности предприятия, что позволит оценить уровень защищенности и устранить уязвимости.

Список использованных источников:

1. Курс на антихрупкость. Стратегический обзор киберугроз 2025. Отчет компании Инфосистемы Джет. Режим доступа: https://jetcsirt.su/analytics/ (дата обращения 20.04.2026).

2. Информационная безопасность (тренды). Статья из обзора TAdviser «Российский рынок ИБ». Режим доступа: https://www.tadviser.ru/index.php (дата обращения 20.04.2026).

3. Постквантовая криптография: основные подходы и причины использования. Режим доступа: https://habr.com/ru/sandbox/163505/ (дата обращения 20.04.2026).

4. Тренды информационной безопасности в 2026 году: что учитывать бизнесу. Режим доступа: https://korusconsulting.ru/blog/tekhnologii/trendy-informatsionnoy-bezopasnosti-v-2026-godu-chto-vazhno-uchityvat-biznesu/ (дата обращения 20.04.2026).

5. Эксперты назвали десять трендов кибербезопасности в 2026 году. Режим доступа: https://hi-tech.mail.ru/articles/138080-eksperty-nazvali-desyat-trendov-kiberbezopasnosti-v-2026-godu/ (дата обращения 20.04.2026).

Sentsova A.Y.
Ufa University of Science and Technology, Ufa

KEY TRENDS IN INFORMATION SECURITI IN 2026

Annotation. This article examines the key trends in information security that analysts predict will be relevant in 2026. It also highlights some common characteristics of last year's attacks. Recommendations are provided for companies to build a defense system that addresses the most pressing information security threats.

Keywords: information security, threats, artificial intelligence, cyber resilience, destructive impact, agent-based AI, zero-trust model, Secure by Design, social engineering, deepfake.

УДК 004

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

ИДЕНТИФИКАЦИЯ И МОНИТОРИНГ УСТРОЙСТВ ЧЕРЕЗ БЕСПРОВОДНЫЕ ИНТЕРФЕЙСЫ

Аннотация. В работе рассматриваются методы идентификации устройств через анализ сигналов Bluetooth и Wi-Fi. Анализируются современные подходы к деанонимизации устройств в условиях применения механизмов рандомизации MAC-адресов. Предложены способы применения полученных значений в процессе прослушивания радиоканалов беспроводных интерфейсов для идентификации и последующего мониторинга и анализа состояния устройства.

Ключевые слова: прослушивание сигналов, беспроводное подключение, идентификация, MAC-адресация, анализ пактов, Bluetooth, Wi-Fi.

Много работ посвящено вопросам обеспечения безопасности при подключениях по радиоканалу по технологиям Wi-fi и Bluetooth, а также сохранению анонимности устройств, но мало изучена тема идентификации и методов применения полученных служебных пакетов при обмене данными через протоколы подключений. Например, в работе [1] даны рекомендации по защите от несанкционированного доступа к информации, передаваемой по беспроводным технологиям связи Bluetooth и Wi-Fi и проведены экспериментальное исследование методик обнаружения уязвимостей беспроводной технологии Bluetooth, даны рекомендации по их устранению. В [2] проведено исследование

проблемы перехвата конфиденциальной информации и представлены рекомендации по предотвращению несанкционированного доступа к передаваемой беспроводными способами связи информации, а также проведены экспериментальные исследования по обнаружению и локализации атак на BLE-устройства. В [3] проведено обобщение и систематизация методов обеспечения информационной безопасности технологий беспроводной передачи данных Wi-Fi и Bluetooth, рассмотрены основные методы обнаружения и локализации различных атак на устройства, поддерживающие Wi-Fi и Bluetooth технологии, проанализированы способы противодействия несанкционированному проникновению к элементам интернета вещей и проведено исследование Bluetooth Low Energy (BLE) технологий. Настоящая работа направлена на анализ идентификационных полей стандартов BLE (Bluetooth Low Energy) и IEEE 802.11, а также методов их использования для субъектов мониторинга.

Современные электронные устройства с беспроводным интерфейсом для подключения или сопряжения в состоянии ожидания генерируют периодические кадры протоколов Bluetooth и Wi-Fi. Данные кадры содержат служебную информацию, необходимую для обнаружения сетей и сопряжения. С точки зрения радиочастотного мониторинга эти кадры образуют детерминированный радиоканальный портрет устройства. Задача идентификации сводится к извлечению таких уникальных служебных данных, которые позволят строить математические модели для последующего мониторинга и анализа.

Традиционные методы защиты информации полагаются на шифрование трафика и рандомизацию идентификаторов (MAC-адресов), но современные исследования демонстрируют уязвимость этих механизмов [4-6]. В режиме мониторинга адаптер не устанавливает соединения, а анализирует служебные пакеты, которые устройства передают для обнаружения сетей и других устройств. К информации, доступной для сбора, относятся: физические параметры сигнала, идентификационная информация и сетевые параметры.

К физическому параметру относится уровень сигнала (RSSI - Received Signal Strength Indicator) – это значение, измеряемое в dBm, которое коррелирует с расстоянием до источника сигнала. Характер изменения RSSI во времени позволяет оценивать траекторию движения устройства. Если имеются несколько приемников сигнала, то можно определить местоположение и перемещение устройства в зоне контроля. Также к физическим параметрам относятся временные метки – время приема каждого пакета, которое позволяет определять скорость работы устройства и его аппаратные возможности.

К идентификационной информации относится MAC-адрес (BSSID) и имя устройства. MAC-адрес представляет собой уникальный идентификатор сетевого интерфейса, у которого первые 24 бита (OUI - Organizationally Unique Identifier) указывают на производителя оборудования. Имя устройства содержит идентифицирующую информацию, например название телефона.

Однако идентификационная информации не является постоянной, так как в современных мобильных устройствах внедрена система рандомизация MAC-адресов как механизм защиты приватности. Устройства периодически (обычно каждые 10–40 минут) заменяют свой реальный MAC-адрес на случайный псевдоним. Однако существуют способы обхода этой защиты [6]. Ряд исследований связан с использованием RSSI как постоянной характеристики устройства для связывания различных случайных MAC-адресов, принадлежащих одному физическому устройству. Теория основана на физическом принципе: устройство не может без каких-либо признаков мгновенно исчезнуть из зоны видимости или появиться в ней (за исключением моментов включения/выключения радиомодуля).

Сетевые параметры – это имя сети Wi-Fi, к которой подключено или пыталось подключиться (содержится в probe request-пакетах) и поддерживаемые скорости канала связи.

В условиях, когда ни один из протоколов по отдельности не дает абсолютной уникальности, можно применить перекрестную корреляцию, когда устройство излучает одновременно кадры Wi-Fi и BLE. Если два потока пакетов наблюдаются в едином временном окне с идентичными параметрами RSSI и направлениями на приемник сигнала, то они с высокой вероятностью принадлежат одному физическому объекту. Формируется связка данных подключения Wi-Fi и протокола BLE, которая будет стабильна даже при смене всех адресов.

Данные, полученные с помощью режима прослушивания с последующим их анализом с помощью программ-анализаторов (например, Wireshark), позволяют извлечь сведения для идентификации и последующего мониторинга состояния исследуемого устройства. Рандомизация MAC-адресов нарушает прямую идентификацию устройств по адресному полю, но не устраняет возможность идентификации по совокупности параметров канального уровня. Кросс-протокольная корреляция данных Wi-Fi и BLE существенно повышает достоверность идентификации и дает возможность для создания систем мониторинга.

Список использованных источников:

1. Методы обеспечения информационной безопасности беспроводных сетей / К. А. Муравьев, В. О. Захарова, Е. А. Салуев, Т. Н. Махмудов // Динамика сложных систем - XXI век. – 2023. – Т. 17, № 1. – С. 13-29. – DOI 10.18127/j19997493-202301-02.

2. Корсаков, И. Н. Обеспечение безопасности при подключении медицинских устройств по протоколу Bluetooth Low Energy / И. Н. Корсаков, С. М. Купцов, Д. А. Разнометов // Инновации в науке. – 2015. – № 46. – С. 130-136.

3. Саенко, М. А. анализ уязвимостей беспроводных каналов передачи информации / М. А. Саенко, Д. А. Мельников, М. А. Данилов // Образовательные ресурсы и технологии. – 2023. – № 1(42). – С. 82-90. – DOI 10.21777/2500-2112-2023-1-82-90.

4. Girish, A., Reardon, J., Tapiador, J., Matic, S., & Vallina-Rodriguez, N. (2025). Your Signal, Their Data: An Empirical Privacy Analysis of Wireless-scanning SDKs in Android. Proceedings on Privacy Enhancing Technologies (PoPETs), 2025(3), 361–381.

5. Ellis, C., Zhang, Y., Jangid, M. K., Zhao, S., & Lin, Z. (2025). Deanonymizing Device Identities via Side-channel Attacks in Exclusive-use IoTs & Mitigation. Network and Distributed System Security Symposium (NDSS).

6. Gagnon, G., Gambs, S., & Cunche, M. (2024). RSSI-based attacks for identification of BLE devices. Computers & Security, 147, 104080. doi.org

Fatkhelislamov A.F.
Ufa University of Science and Technology, Ufa

IDENTIFICATION AND MONITORING OF DEVICES VIA WIRELESS INTERFACES

Abstract. This paper examines methods for identifying devices through Bluetooth and Wi-Fi signal analysis. Modern approaches to deanonymizing devices using MAC address randomization mechanisms are analyzed. Methods for using the obtained values during wireless interception are proposed for identification, subsequent monitoring, and analysis of device status.

Keywords: signal sniffing, wireless connection, identification, MAC addressing, packet analysis, Bluetooth, Wi-Fi.

УДК 004.056

Шагапов И.А., Салов И.В.
Уфимский университет науки и технологий, Уфа

НЕПРЕРЫВНОСТЬ И ТОЧКИ РАЗРЫВА В ЗАЩИТЕ ИНФОРМАЦИИ

Аннотация. В статье предложен математический подход использования точек разрыва в защите информации с одновременным обеспечением принципа непрерывности. В основе данного подхода лежат математические понятия: области непрерывности и точки разрыва функции одной переменной. Показано, что после внесения некоторых изменений и адаптаций эти понятия вполне могут быть применены в сфере защиты информации.

Ключевые слова: математический подход, непрерывность, точка разрыва, устранимая точка разрыва, неустранимая точка разрыва, защита информации, система защиты информации, математический анализ.

Свойство непрерывности или отсутствие таковой встречается практически в любой области, в частности, это касается процессов. Процессы бывают непрерывными и дискретными.

В дискретных процессах есть разрыв между элементами. Примером может служить последовательность чисел (конечная или бесконечная). На практике, конечно, удобнее работать с конечным набором так как элементы можно пронумеровать и обращаться к элементу по номеру и т.д. Даже когда элементы «не заканчиваются» можно говорить о счетном множестве, пусть даже и «равном бесконечности». Главное – один элемент отличается от другого разрывом (зазором), между ними «ничего нет», т.е. соседние элементы друг о друге ничего «не знают» или «знают мало». Этой областью в основном занимаются алгебра и дискретная математика. На практике это дискретные или цифровые процессы.

В непрерывных процессах разрыва или зазора между элементами нет. Здесь говорить о количестве элементов, как правило, бессмысленно. Оно есть континуум, это даже не бесконечно, а еще «больше». Следовательно, «соседние» элементы друг о друге «знают много» или даже все. Например, для функций есть понятие предела функции в точке, а также производная функции в точке и т.д., где основным требованием является наличие непрерывности функции, которая в свою очередь определяется через соседние точки. Этим занимается, в первую очередь, математический анализ. На практике это аналоговые процессы.

В практической деятельности человека встречаются много задач, когда для описания непрерывных процессов удобнее (а может

необходимо) перейти в дискретное множество. В математике в первую очередь это приближения одного объекта (как правило, со сложной структурой) последовательностью других специально подобранных объектов, которые устроены более просто. В частности, существуют методы, основанные на замене единого цельного непрерывного процесса конечным дискретным множеством.

Есть задачи, в которых заданное множество, в котором ищется решение задачи, состоит из непрерывных элементов (процессов). Например, в защите информации. Она (защита) должна быть непрерывной – это один из ее основных принципов.

На практике для обеспечения непрерывности защиты информации, в основном, выбирают или строят, а потом применяют одну стационарную систему. Тогда вопрос непрерывности целиком относится только к этой системе. Другое дело, бывает, что необходимо применять несколько различных систем параллельно, последовательно или их сочетание. Например, в случае, когда системе грозит взлом, отключение, перехват управления. Как правило, это возможно, когда внешние силы имеют доступ (НСД) к устройству системы. Другими словами, при НСД система или должна измениться или отключится под воздействием внешних сил, не предусмотренных функционированием системы. С точки зрения автора, уязвимость таких систем следует из того, что непрерывность гарантирует возможность постепенного перехода из одного элемента на другой, т.е. присутствует возможность изучения системы.

С другой стороны, существуют подходы, когда единый процесс искусственно делится на конечное количество частей так, чтобы вычислить переход из заданного элемента на другой, было сложно или невозможно [1]. Другими словами, непрерывный процесс разрывается на конечное число «несвязанных» друг с другом элементов. Это означает уменьшение количество доступной информации, а точнее - разрыв конкретных связей между элементами. Можно даже сказать, что информация о связях исчезает совсем или становится известной ограниченному кругу (конфиденциальной). Таким образом, в таких подходах разрыв или отсутствие непрерывности помогает ограничивать полный доступ к информации о системе, тем самым защищаться от взлома, вмешательства и т.д.

Мы рассмотрели подход, когда известный нам непрерывный процесс превратили в дискретный. Здесь ключевое слово «нам». Опасность не только в том, что эта информация от нас может уйти, но и в том, что удаленные за счет разрывов связи можно пытаться восстановить, например, вычислить. Возникает вопрос: процесс мы обязательно должны знать заранее? Другими словами, можно ли процесс (часть процесса) на ходу придумать, чтобы следующий шаг нельзя было

вычислить? Например, переключаться между состояниями случайно или псевдослучайно. Оказывается, можно и такие системы строить [2,3]. Например, использовать случайный выбор из заданного конечного множества возможных элементов [1].

Теперь вернемся к защите информации, где одним из принципов является обеспечение непрерывности. До этого, для повышения непредсказуемости работы системы защиты информации, мы искусственно ввели разрывы. Естественно это нарушает принцип непрерывности. Как быть?

Обратимся к математике. В математическом анализе разрывы делятся на два типа: устранимые и неустранимые. Устранимые (склеиваемые, стыкуемые) устроены достаточно просто – в точке разрыва отсутствует значение функции или оно «неправильное». Разрыв устраняется определением или переопределением значения функции в точке разрыва как пределов функции справа и слева от этой точки (в этом случае эти пределы совпадают). Такое устранение разрыва можно назвать как «склейка встык». Когда разрыв неустранимый (нестыкуемый, несклеиваемый), пределы справа и слева разные (случай бесконечности не рассматриваем), поэтому просто переопределением значения функции в точке разрыва обойтись не получится, надо выбирать. Но какой бы выбор не сделали, достичь непрерывность не получится.

Предлагается дополнить математику практическим подходом – использовать и то и другое значение, а не выбирать. Конечно, функция перестает быть однозначной – в каждой точке из области определения любая однозначная функция может иметь только одно значение (тоже принцип). Решение – отказаться от однозначности функции. Тогда в точках разрыва «нефункция» будет иметь два значения, т. е. временно в точках разрыва появляется двухзначная функция. Так мы устраняем разрыв. Такое практическое устранение разрыва можно назвать «склейкой внахлест». В рамках защиты информации это будет означать, что в точках, где отсутствовала непрерывность, будут работать одновременно две системы (возможно даже два экземпляра одной и той же системы) т.е. разрыв устраняется. После такой склейки (перехода) можно снова вернуться к защите одной системой.

Таким образом, мы получили новую надсистему, которая сочетает в себе и ограничение доступа к полной информации о системе за счет искусственных разрывов или естественного выбора не стыкуемых частей, и одновременно обеспечили непрерывность за счет использования параллельного соединения.

Список использованных источников:

1. Исмагилова, А.С. Количественная оценка рекомпозиционной системы защиты информации / А.С. Исмагилова, И.А. Шагапов, И.В. Салов // Инженерный вестник Дона. – 2024. – № 8(116). – С. 273-281.
2. Шагапов, И.А. Математический конструктивный подход построения систем защиты информации / И.А. Шагапов // Естественные и технические науки. – 2025. – № 12(211). – С. 366-369. – DOI 10.25633/ETN.2025.12.39.
3. Шагапов, И.А. О некоторых особенностях построения систем защиты информации / И.А. Шагапов // Естественные и технические науки. – 2023. – № 12(187). – С. 305-307. – DOI 10.25633/ETN.2023.12.31.

Shagapov I.A., Salov I.V.
Ufa University of Science and Technology, Ufa

CONTINUITY AND BREAK POINTS IN INFORMATION SECURITY

Abstract. This article proposes a mathematical approach to using discontinuity points in information security while simultaneously ensuring the principle of continuity. This approach is based on the mathematical concepts of continuity domains and discontinuity points of a single-variable function. It is shown that, with some modifications and adaptations, these concepts can be applied to information security.

Keywords: mathematical approach, continuity, discontinuity point, removable discontinuity point, irremovable discontinuity point, information security, information security system, mathematical analysis.

УДК 347.8 (075)

Яковец Е.Н.
Российская таможенная академия, Люберцы

СЛУЖЕБНЫЕ СВЕДЕНИЯ ОГРАНИЧЕННОГО РАСПРОСТРАНЕНИЯ ИЛИ СЛУЖЕБНАЯ ТАЙНА?

Аннотация. В статье рассматриваются проблемы использования и защиты сведений, составляющих служебную тайну. Анализируется ее соотношение с понятием служебных сведений ограниченного распространения. Говорится о необходимости совершенствования ведомственного нормативно-правового регулирования защиты сведений рассматриваемой категории, а также о тех правовых последствиях, которые могут наступить в случае нарушения законных интересов их первичных обладателей – физических и юридических лиц.

Ключевые слова: служебная тайна; служебные сведения ограниченного распространения; характерные особенности служебной тайны; доверители конфиденциальной информации; держатели конфиденциальной информации.

В советский период действовала достаточно эффективная система защиты информации ограниченного доступа. Тогда выделялось три основных ее вида: государственная тайна (информация с грифами секретности носителей «особой важности» и «совершенно секретно»), служебная тайна (информация с грифом секретности носителей «секретно»), а также информация «для служебного пользования». С принятием в 1993 г. Закона РФ «О государственной тайне» [1, ст. 8] гриф «секретно» стал присваиваться носителям сведениям, составляющим государственную тайну, а новый институт правовой охраны служебной тайны остался не сформированным. Несовершенство правового регулирования защиты служебной тайны наглядно демонстрировала появившаяся в 1994 г. ст. 139 Гражданского кодекса РФ (впоследствии утратившая силу [2, ст. 17, п. 12]), которая практически нивелировала понятия служебной и коммерческой тайн.

В соответствии с положениями Перечня сведений конфиденциального характера [3, п. 3], «служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (служебная тайна)», были отнесены к сведениям конфиденциального характера. Вследствие того, что в действующем законодательстве четкие ориентиры для определения сущности как конфиденциальной информации в целом, так и служебной тайны в частности отсутствуют, для определения содержания последней следует руководствоваться научными подходами, согласно которым информация может считаться служебной тайной лишь в том случае, если она обладает рядом особых признаков.

Первая особенность служебной тайны заключается в том, что ее субъектами могут являться исключительно *государственные* или *муниципальные служащие.* Причем, к служебной тайне может относиться лишь та конфиденциальная информация, которая становится им известной в силу исполнения профессиональных обязанностей, *связанных с государственной или муниципальной службой.* Последние являются ее *субъектами* и одновременно *носителями.* Однако *обладателями* сведений, составляющими служебную тайну, наделенными правом распоряжения ими, могут являться только сами *государственные органы власти* или *органы местного самоуправления* в лице их руководителей.

Данное обстоятельство является *вторым признаком,* характеризующим сущность сведений, относящихся к служебной тайне.

Третья особенность характеризует *качественный состав* информации рассматриваемой категории. Практика свидетельствует о том, что в государственных и муниципальных структурах обычно концентрируются сведения двух основных видов:

1) информация, связанная с отдельными сторонами функционирования самих субъектов государственного и муниципального управления, ограничения на распространение которой диктуются служебной необходимостью и регламентируются подзаконными и ведомственными нормативными правовыми актами;

2) информация, получаемая субъектами управления из внешних источников на законных основаниях в силу исполнения государственными и муниципальными служащими своих служебных обязанностей (ее первооснову составляет конфиденциальная информация, первоначальными обладателями которой являются иные лица).

Касаясь первой категории сведений, следует особо подчеркнуть, что они не относятся к сведениям, составляющим государственную тайну, несмотря на то что их разглашение или утрата в отдельных случаях могут причинить ущерб интересам государства. Это так называемая «внутренняя» составляющая служебной тайны или «служебная информация ограниченного распространения».

Во втором случае речь идет о трансформации в служебную тайну главным образом коммерческой или профессиональной тайн, а также тайны частной жизни и персональных данных граждан. Эта «внешняя» составляющая служебной тайны. При получении субъектами управления подобной информации они обязаны вводить для ее защиты режим конфиденциальности. Причем, конфиденциальность полученной информации должна учитывать интересы не только ее *держателей* (лиц, передавших сведения субъектам управления), но и *доверителей* (первоначальных обладателей этих сведений, если таковые имеются).

На основе изложенного можно дать следующее научное определение служебной тайны. *Служебная тайна – это не относящиеся к государственной тайне сведения, связанные с деятельностью государственных и муниципальных органов, доступ к которым ограничен законодательством, а также сведения ограниченного доступа, ставшие известными органам государственной власти и местного самоуправления на законных основаниях в силу исполнения их представителями своих служебных полномочий*.

Следует особо подчеркнуть, что до 2016 г. Положением о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти, уполномоченном органе

управления использованием атомной энергии и уполномоченном органе по космической деятельности [4] обеспечивался правовой режим исключительно «внутренней» составляющей служебной тайны. Редакция п. 1.2 данного Положения гласила, что «к служебной информации ограниченного распространения относится несекретная информация, касающаяся деятельности организаций, ограничения на распространение которой диктуются служебной необходимостью», а в его п. 1.8 за разглашение или необоснованное использование последней предусматривалось применение исключительно дисциплинарной ответственности.

Названное Положение на сегодняшний день является единственным межотраслевым нормативным актом в области правовой защиты информации подобного рода. Именно на его основе разработаны действующие ведомственные нормативные правовые акты, регламентирующие правовую защиту информации подобного рода в различных ведомствах, практически продублировавшие подходы этого Положения.

Однако в соответствии с постановлением Правительства РФ от 20 февраля 2016 г. № 123 «О внесении изменения в Положение о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти и уполномоченном органе управления использованием атомной энергии»[5] п. 1.2 был дополнен словами «, а также поступившая в организации несекретная информация, доступ к которой ограничен в соответствии с федеральными законами». Пункт 1.8 при этом обрел следующую формулировку: «За разглашение служебной информации ограниченного распространения, а также нарушение порядка обращения с документами, содержащими такую информацию, в том числе их уничтожения, допустившие указанные нарушения лица привлекаются к предусмотренной законодательством Российской Федерации ответственности». Этим самым было констатировано, что за нарушение безопасности различных видов конфиденциальной информации, лежащей в основе служебной информации ограниченного распространения, наряду с дисциплинарными мерами может применяться гражданско-правовая, административная или уголовная ответственность.

Таким образом, с принятием данных дополнений содержание понятий служебной тайны и служебной информации ограниченного распространения стали практически равнозначными. Однако требования по защите второго сегмента служебной тайны (ее «внешней» составляющей) ведомственными нормативными правовыми актами до сих пор не урегулированы. Содержание служебной информации ограниченного распространения в них по-прежнему определяется более

узким ее форматом, включающим в свой состав лишь сведения «внутреннего» характера, а юридическая ответственность за разглашение этих сведений или нарушение порядка обращения с содержащими их документами ограничивается лишь дисциплинарными мерами.

Вместе с тем, нанесенный сотрудниками государственных или муниципальных органов материальный ущерб и (или) причиненный моральный вред физическим и юридическим лицам – первоначальным обладателям сведений, требующих защиты в режиме служебной тайны, – могут быть взысканы с виновных на основании актуализированных норм рассмотренного выше Положения, которые обладают более высокой юридической силой по сравнению с нормами ведомственных нормативных правовых актов. По этому же основанию виновные могут быть одновременно привлечены к административной (по ст. 13.11, 13.12, 13.14, 13.14.1 и др**.** КоАП РФ) либо уголовной (по ст. 137, 138, 155, 183, 310, 320 и др. УК РФ) ответственности.

Список использованных источников:

1. О государственной тайне: Закон РФ от 21 июля 1993 г. № 5485-I (с изм. и доп.) // Российская газета. 1993. 21 сентября.

2. О введении в действие части четвертой Гражданского кодекса Российской Федерации: Федеральный закон РФ от 18 декабря 2006 г. № 231-ФЗ // Российская газета. 2006. 22 декабря.

3. Перечень сведений конфиденциального характера: утв. Указом Президента РФ от 6 марта 1997 г. № 188 (с изм. и доп.) // Собр. законодательства Рос. Федерации от 10 марта 1997 г. № 10, ст. 1127.

4. Положение о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти, уполномоченном органе управления использованием атомной энергии и уполномоченном органе по космической деятельности: утв. постановлением Правительства РФ от 3 ноября 1994 г. № 1233 (с изм. и доп.) // Собр. законодательства Рос. Федерации. – 2005. – № 30, ст. 3165.

5. Постановление Правительства РФ от 20 февраля 2016 г. № 123 «О внесении изменения в Положение о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти и уполномоченном органе управления использованием атомной энергии» // Консультант Плюс. – URL: www. consultant.ru (дата обращения: 11.03.2026).

Yakovets E.N.
Russian Customs Academy, Lyubertsy

OFFICIAL INFORMATION OF THE LIMITED DISTRIBUTION OR OFFICIAL SECRET?

Abstract. The article discusses the problems of using and protecting information that constitutes official secrecy. It analyzes the relationship between this information and the concept of restricted official information. The article also discusses the need to improve the departmental legal regulation of the protection of this type of information, as well as the legal consequences that may arise if the legitimate interests of its primary owners, individuals and legal entities, are violated.

Keywords: official secrecy; restricted official information; characteristics of official secrecy; confidential information trustees; confidential information holders.

УДК 004.056

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

СОВЕРШЕНСТВОВАНИЕ СИСТЕМЫ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ В ОРГАНИЗАЦИИ

Аннотация. В статье анализируются современные подходы к построению системы технической защиты информации в организации. Исследование охватывает ключевые проблемы, такие как быстрое устаревание технологий, человеческий фактор, ограниченное финансирование и рост сложности атак. На основе анализа современных угроз и уязвимостей предложены практические рекомендации по внедрению новых технических решений и управлению рисками информационной безопасности.

Ключевые слова: информационная безопасность, защита данных, киберугрозы, технические средства защиты, управление рисками, технические средства, программное обеспечение.

Информация является стратегическим ресурсом любой организации, играя ключевую роль в обеспечении ее конкурентоспособности, устойчивости и эффективности [7]. С развитием цифровых технологий объем создаваемых, передаваемых и обрабатываемых данных значительно возрос, что делает информацию одной из наиболее уязвимых целей для злоумышленников. В условиях постоянно растущего числа

кибератак и эволюции методов проникновения нарушителей в систему защиты информации обеспечение надежной защиты данных становится приоритетной задачей для организации [1].

В настоящее время риски информационной безопасности связаны с:

– увеличением числа угроз, направленных на компрометацию систем защиты информации и защищаемой информации;

– ограниченностью ресурсов, выделяемых на модернизацию систем защиты информации;

– усложнением соблюдения нормативных требований и стандартов информационной безопасности [2].

Совершенствование системы технической защиты информации требует постоянного пересмотра используемых технологий и подходов, чтобы противостоять стремительному росту кибератак [3]. Современные системы технической защиты информации постоянно сталкиваются с проблемами, которые можно успешно разрешить. К ним следует отнести:

1. Устаревание технических решений. Многие организации продолжают использовать традиционные межсетевые экраны и антивирусное программное обеспечебие не учитывая сложность иерархии компьютерных атак [4]. В этой связи мы предлагаем для повышения эффективности программно-аппаратной защиты информации заменить традиционные firewalls на NGFW, которые анализируют сетевой трафик на уровне приложений, поддерживают систему предотвращения вторжений (IPS) и фильтрацию веб-контента. Для управления рисками информационной безопасности необходимо внедрение EDR-решений, позволяющих мониторить активность конечных устройств в режиме реального времени и предотвращать угрозы, внедряя механизмы на основе машинного обучения.

2. Ограниченность обнаружения угроз. Применение традиционных SIEM-систем, которые лишь анализируют логи безопасности, уже недостаточно [5]. Необходимо использование SIEM-решений с поддержкой UEBA (User and Entity Behavior Analytics), таких как Splunk, IBM QRadar или ELK Stack. Эти решения позволяют выявлять аномальное поведение пользователей и автоматически реагировать на потенциальные угрозы.

3. Недостаточная автоматизация процессов реагирования на компьютерные атаки [5]. Для сокращения времени реагирования на инциденты необходимо внедрение SOAR (Security Orchestration, Automation and Response). В данном случае мы считаем, что оптимальным решением являются использование Cortex XSOAR и IBM Resilient, которые позволяют автоматизировать обработку инцидентов, интегрируются с SIEM-системами и обеспечивают автоматический запуск сценариев реагирования на атаки.

4. Проблемы управления доступом. Использование устаревших методов аутентификации (логин/пароль) повышает риск компрометации данных [6]. В качестве решения рекомендуется:

– внедрение многофакторной аутентификации (MFA) с использованием токенов и биометрии;

– переход на Zero Trust-модель, исключающую доверие к любым пользователям и устройствам по умолчанию;

– использование решений PAM (Privileged Access Management), таких как CyberArk или BeyondTrust для управления доступом привилегированных пользователей.

Таким образом, пути совершенствования системы технической защиты информации в организации связаны с решением следующих вопросов:

1. Модернизация технических решений:

– внедрение NGFW с интеграцией системы обнаружения атак (IPS) для глубокой инспекции трафика и выявления сложных угроз;

– использование EDR, таких как CrowdStrike Falcon или Microsoft Defender for Endpoint, для анализа действий пользователей и мониторинга конечных точек;

– развертывание решений DLP (Data Loss Prevention) от ведущих производителей (Symantec, Forcepoint) для предотвращения утечек данных;

– применение CASB (Cloud Access Security Broker), таких как McAfee MVISION или Netskope, для контроля облачных сервисов и предотвращения несанкционированного доступа.

2. Автоматизация процедур обнаружения и реагирования на угрозы:

– использование SIEM-решений с UEBA для выявления аномалий в поведении пользователей и проактивного анализа угроз;

– внедрение SOAR-платформ, таких как Palo Alto Cortex XSOAR и Splunk Phantom, для автоматизированного управления инцидентами и координации действий служб безопасности.

3. Управление доступом с целью минимизации рисков НСД:

– внедрение Zero Trust-модели с сегментацией сети и строгими политиками контроля доступа;

– применение PAM-решений (CyberArk, BeyondTrust) для мониторинга и ограничения действий привилегированных пользователей;

– разработка строгих политик безопасности, включая Least Privilege Access (минимальные привилегии) и автоматизированные механизмы отзыва прав доступа при подозрительных действиях.

4. Повышение осведомленности персонала организации в сфере обеспечения информационной безопасности:

– регулярное проведение киберучений и тестов на фишинг с помощью платформ KnowBe4 или PhishMe;

– создание системы мониторинга за действиями сотрудников, имеющих доступ к защищаемой информации, включая поведенческий анализ и анализ инцидентов.

Таким образом, совершенствование системы технической защиты информации в организации заключается в использовании современных технических решений, направленных на модернизацию инфраструктуры, автоматизацию процессов безопасности и контроль доступа. Включение в систему защиты информации таких продуктов как NGFW, EDR, SIEM с UEBA, SOAR, использование концепции Zero Trust, позволяет значительно снизить вероятность компрометации данных и повысить уровень безопасности информационных активов организации. Реализация предложенных мер, на наш взгляд, обеспечит снижение рисков утечек данных, минимизацию финансовых потерь и защиту критически важных активов организации.

Список использованных источников:

1. Аверченков, В. И. Служба защиты информации: организация и управление: учебное пособие / В. И. Аверченков, М. Ю. Рытов. – Москва: ФЛИТНА, 2021. – 186 с. – ISBN 978-5-9765-1271-9. – Текст: электронный // Университетская библиотека онлайн: электронно-библиотечная система. – URL: https://biblioclub.ru/index.php?page=book_red&id=93356 (дата обращения: 25.04.2026).

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: 25.04.2026).

3. Козьминых, С. И. Обеспечение комплексной защиты объектов информатизации: учебное пособие / С. И. Козьминых. – Москва: Юнити-Дана, 2020. – 544 с. – ISBN 978-5-238-03200-9. – Текст: электронный // Университетская библиотека онлайн: электронно-библиотечная система. – URL: https://biblioclub.ru/index.php?page=book_red&id=615695 (дата обращения: 25.04.2026).

4. 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: 22.04.2026).

5. Мамай, И. Н. Информационные технологии в профессиональной деятельности: практикум: учебное пособие / И. Н. Мамай, О. В. Мамай. – Самара: СамГАУ, 2022. – 135 с. – ISBN 978-5-88575-691-4. – Текст:

электронный // Лань: электронно-библиотечная система. – URL: https://e.lanbook.com/book/301976 (дата обращения: 20.04.2026).

6. Трайнев, В. А. Системный подход к обеспечению информационной безопасности предприятия (фирмы): монография/ В. А. Трайнев. – Москва: Дашков и К, 2022. – 332 с. – ISBN 978-5-394-05035-0. – Текст: электронный // Университетская библиотека онлайн: электронно-библиотечная система. – URL: https://biblioclub.ru/index.php?page=author_red&id=9705 (дата обращения: 25.04.2026).

7. Шагапов, И.А. К вопросу построения системы защиты информации / И.А. Шагапов // 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. 51-54.

Yapparov R.M.
Ufa University of Science and Technology, Ufa

IMPROVING THE TECHNICAL PROTECTION SYSTEM IN AN ORGANIZATION

Abstract. The article analyzes modern approaches to building an information security system in an organization. The study covers key issues such as rapid technology obsolescence, the human factor, limited funding, and the increasing complexity of attacks. Based on the analysis of current threats and vulnerabilities, the article provides practical recommendations for implementing new technical solutions and managing information security risks.

Keywords: information security, data protection, cyber threats, technical means of protection, risk management, technical means, and software.

СЕКЦИЯ 1. МАТЕМАТИЧЕСКИЕ МОДЕЛИ И МЕТОДЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

УДК 004.056

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

Научный руководитель:
Сенцова А.Ю.
Уфимский университет науки и технологий, Уфа

ВИЗУАЛИЗАЦИЯ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ С ИСПОЛЬЗОВАНИЕМ QUANTICKLE (НА ПРИМЕРЕ УБИ.223)

Аннотация. В статье рассматривается УБИ.223 (несанкционированный доступ к Docker-контейнерам с получением расширенных привилегий). Представлен анализ механизмов изоляции Docker и модели привилегий. Разработан сценарий атаки, с использованием Quantickle построена визуальная модель (16 узлов, 15 связей), проведено сравнение текстового и графового представлений. На основе графа предложены меры предотвращения атаки.

Ключевые слова: УБИ.223, Docker, контейнеризация, граф атаки, Quantickle, визуализация угроз.

Современная ИТ-инфраструктура активно использует технологии контейнеризации, лидером среди которых является Docker. Однако массовое внедрение любой технологии влечет появление новых угроз нарушения информационной безопасности. Наиболее опасным сценарием реализации угрозы является ситуация, когда нарушитель получает доступ к контейнеру с избыточными правами и использует их для преодоления контейнерной изоляции и несанкционированного доступа к хост-системе. Данная проблема зафиксирована в Банке данных угроз ФСТЭК под идентификатором УБИ.223 [1].

Контейнеры Docker – изолированные процессы в пользовательском пространстве хоста за счет namespaces и cgroups. Linux capabilities дробят привилегии root. По умолчанию Docker сбрасывает большинство опасных возможностей. Проблемы возникают при запуске контейнера с флагом --privileged, что дает ему практически все права хостового root [2], что по сути означает, что злоумышленник получает права суперпользователя в системе.

В статье предложено моделирование сценариев угроз с помощью инструмента Quantickle [3]. Для построения графа смоделирован

сценарий эксплуатации привилегированного контейнера. Исходные условия: на хосте host01 запущен контейнер с флагом --privileged, внутри работает веб-приложение с RCE-уязвимостью. Действия нарушителя включают проникновение (эксплуатация RCE), разведку (команды id, capsh, mount), эскалацию привилегий (mkdir, mount), закрепление в системе (запись SSH-ключа) и выход за пределы изолированной среды контейнера с получением несанкционированного доступа к хост-системе (подключение по SSH к хосту). На основе сценария сформированы provenance-данные, загруженные в инструмент Quantickle. Построенный граф атаки представлен на рисунке 1.

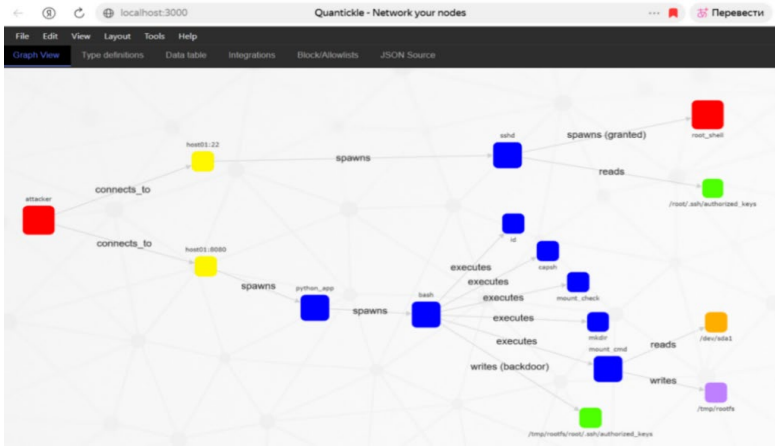


Рис. 1. Граф атаки при реализации УБИ.223, построенный в Quantickle

Описание узлов графа приведено в таблице 1.

Таблица 1

Описание узлов графа

Узел в графе	Тип	Описание
attacker	actor	Внешний IP-адрес нарушителя
host01:8080	port	Порт веб-приложения
python_app	process	Веб-приложение внутри контейнера
bash	process	Командная оболочка, запущенная нарушителем
id	process	Команда проверки идентификатора пользователя
capsh	process	Команда проверки Linux capabilities
mount_check	process	Проверка текущих точек подключения
mkdir	process	Создание точки подключения
mount_cmd	process	Подключение устройства хоста
/dev/sda1	device	Корневой раздел хоста

Узел в графе	Тип	Описание
/tmp/rootfs	folder	Точка подключения внутри контейнера
host01:22	port	SSH-порт хоста
sshd	process	SSH-сервер на хосте
/root/.ssh/authorized_keys	file	Файл авторизованных ключей на хосте
/tmp/rootfs/root/.ssh/authorized_keys	file	Тот же файл, подключенный в контейнере
root_shell	process	Командная оболочка с root-доступом на хосте

Описание связей графа приведено в таблице 2.

Таблица 2

Описание связей графа

Источник	Действие	Цель
attacker	connects_to	host01:8080
host01:8080	spawns	python_app
python_app	spawns	bash
bash	executes	id
bash	executes	capsh
bash	executes	mount_check
bash	executes	mkdir
bash	executes	mount_cmd
mount_cmd	reads	/dev/sda1
mount_cmd	writes	/tmp/rootfs
bash	writes	/tmp/rootfs/root/.ssh/authorized_keys
attacker	connects_to	host01:22
host01:22	spawns	sshd
sshd	reads	/root/.ssh/authorized_keys
sshd	spawns	root_shell

Построенный граф имеет четкую структуру. Левый кластер – внешний нарушитель, проникающий в контейнер через открытый сетевой порт. Центральный – действия внутри контейнера, приводящие к взаимодействию с ресурсами хоста. Правый – завершающий этап, где нарушитель напрямую взаимодействует с хостом через SSH. Детализация включает промежуточные команды (mount_check, mkdir), что соответствует принципу сбора provenance-данных, фиксирующих каждый системный вызов. Для наглядности узлам графа присвоены цвета в зависимости от типа: actor - красный, port - желтый, process - синий, device - оранжевый, folder - сиреневый, file - зеленый.

Сравнение текстового описания и графа показало преимущества последнего: охват картины атаки одним взглядом, явная визуализация всех связей (включая скрытые), выделение критических точек и возможность принятия решений по поводу реализации контрмер на критических точках.

Анализ графа выделил ключевые точки предотвращения атаки. Проникновение блокируется безопасной обработкой ввода и обновлением

зависимостей. Блокирование эскалации привилегий (узлы mount_cmd, mkdir на графе) достигается запретом флага --privileged и отключением всех возможностей (capabilities). Предотвращение закрепления требует мониторинга целостности критических файлов и централизованного сбора логов.

Таким образом, проведен анализ УБИ.223, разработана визуальная модель атаки в Quantickle, созданы рекомендации. Граф позволяет проследить действия нарушителя и выявить критические точки для усиления защиты.

Список использованных источников:

1. ФСТЭК России. Банк данных угроз безопасности информации. URL: https://bdu.fstec.ru/threat/ubi.223 (дата обращения: 31.03.2026).

2. Docker Inc. Docker Security Documentation. URL: https://docs.docker.com/engine/security/ (дата обращения: 31.03.2026).

3. RSA Labs. Quantickle: Network Graph Visualization for Threat Intelligence. URL: https://github.com/RSAC-Labs/Quantickle (дата обращения: 31.03.2026).

Gavrilova A.A.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Sentsova A.U.
Ufa University of Science and Technology, Ufa

VISUALIZATION OF INFORMATION SECURITY THREATS USING QUANTICKLE (CASE STUDY OF UBI.223)

Abstract. The article considers UBI.223 (unauthorized access to Docker containers with extended privileges). Analysis of Docker isolation mechanisms and the privilege model is presented. An attack scenario is developed, a model (16 nodes, 15 edges) is constructed using Quantickle, and textual and graphical representations are compared. Based on the graph, measures to prevent attack are proposed.

Keywords: UBI.223, Docker, attack graph, Quantickle, threat visualization.

УДК 004.056

Горяйнов С.А., Дибров Н.
Северо-Кавказский федеральный университет, Ставрополь

Научный руководитель:
Петренко В.И.
Северо-Кавказский федеральный университет, Ставрополь

МЕТОД КООРДИНАЦИИ РОЯ БПЛА С ПЕРЕДАЧЕЙ ДОВЕРИЯ ПО ТРАНЗИТИВНЫМ ЦЕПОЧКАМ В УСЛОВИЯХ ОГРАНИЧЕННОЙ СВЯЗНОСТИ

Аннотация. Рассматривается задача координации роя беспилотных летательных аппаратов в условиях ограниченной связности сети и наличия вредоносных узлов. Предложен метод, в котором при недостатке прямых наблюдений доверие к удаленному агенту формируется по транзитивным цепочкам связи с учетом длины пути и надежности промежуточных узлов. По результатам моделирования показано, что метод уменьшает риск атакующего воздействия и повышает качество выявления вредоносных узлов по сравнению с базовыми подходами.

Ключевые слова: рой БПЛА, координация, доверие, транзитивное доверие, ограниченная связность, вредоносные узлы, устойчивость сети.

Роевые системы беспилотных летательных аппаратов все шире применяются в задачах мониторинга, поиска, сопровождения объектов и распределенного сбора данных. Вместе с тем надежность таких систем определяется не только качеством маршрутизации и распределения ролей, но и устойчивостью коллективного выбора действий к вредоносным воздействиям и искажению передаваемой информации [1-3]. Существенной особенностью реальных роевых систем является ограниченная связность: не каждый аппарат имеет возможность прямого обмена данными со всеми участниками, а структура сети может быть линейной, кольцевой, древовидной или разреженной

В современных исследованиях по безопасности сетей БПЛА и летающих самоорганизующихся сетей одним из перспективных способов повышения устойчивости является применение доверительных оценок, позволяющих уменьшать влияние подозрительных узлов на общее решение [4]. Отмечается, что вредоносные узлы способны искажать сообщения, влиять на маршрутизацию и нарушать согласованность действий группы [5-8]. Однако при ограниченной связности прямых наблюдений за удаленными участниками часто недостаточно. Поэтому возникает задача формирования доверия не только по непосредственным

взаимодействиям, но и по косвенной информации, передаваемой через промежуточные узлы.

Целью работы является разработка метода координации роя БПЛА, в котором доверие к удаленным участникам формируется по транзитивным цепочкам связи и используется при распределенном выборе планов в условиях ограниченной связности.

Рассматривается рой из восьми аппаратов, взаимодействующих в графе связи. На каждом шаге каждый агент формирует набор допустимых локальных планов, характеризуемых ожидаемой полезностью, затратами ресурсов и согласованностью с общей целью миссии. Часть узлов считается вредоносной. Такие узлы могут завышать полезность собственного плана, передавать недостоверные сведения о своем состоянии и отклоняться от ранее заявленного поведения при выполнении миссии.

Для сравнительного анализа использовались три подхода. Первый подход не применяет доверительный механизм и учитывает вклад всех узлов одинаково. Второй подход использует только прямое доверие, накапливаемое по истории взаимодействий пары соседних агентов. В предлагаемом подходе прямое доверие дополняется транзитивной оценкой, передаваемой по цепочкам связи между удаленными участниками.

Прямое доверие между двумя агентами формируется по результатам наблюдения за соответствием фактического поведения узла переданным им данным. Если прямых наблюдений недостаточно, для оценки удаленного агента рассматриваются допустимые цепочки связи. Для каждой такой цепочки доверительная оценка вычисляется по формуле

$$D(p) = \left(\prod_{(u,v)\in p} D_{uv}^{\text{пр}}\right) \cdot \gamma^{L(p)-1}, \qquad (1)$$

где $D(p)$ – доверительная оценка цепочки p; $D_{uv}^{\text{пр}}$ – прямое доверие между соседними узлами u и v; $L(p)$ – длина цепочки в ребрах; γ – коэффициент ослабления доверия по длине пути.

Из формулы (1) следует, что надежность косвенной оценки уменьшается как при снижении доверия к промежуточным узлам, так и при увеличении длины цепочки. Иными словами, более длинные маршруты передачи информации считаются менее надежными, чем короткие.

Если между двумя агентами существует несколько допустимых цепочек, на их основе формируется обобщенная транзитивная оценка, которая затем объединяется с прямым доверием. Итоговое доверие определяется по формуле

$$D_{ij} = \alpha D_{ij}^{\text{пр}} + (1-\alpha) D_{ij}^{\text{тр}}, \qquad (2)$$

где D_{ij} – итоговое доверие агента i к агенту j; $D_{ij}^{\text{пр}}$ – прямая оценка доверия; $D_{ij}^{\text{тр}}$ – транзитивная оценка, полученная по допустимым цепочкам; α – коэффициент, задающий вклад прямых наблюдений в итоговую оценку.

Согласно формуле (2), при наличии достаточной прямой информации преобладает непосредственная оценка, а при ее недостатке возрастает роль транзитивной составляющей. Итоговое доверие используется при коллективном выборе плана как весовой коэффициент, уменьшающий влияние узлов с низким уровнем доверия.

Моделирование проводилось на области 16×8 при длине эпизода 10 шагов, числе аппаратов 8 и 12 планах на агента. Рассматривались линейная, кольцевая, древовидная и разреженная случайная топологии. В атакуемом сценарии доля вредоносных узлов составляла 0,25, вероятность отклонения от заявленного поведения – 0,7. Использовались десять начальных инициализаций. Оценивались риск атакующего воздействия, риск невыявленных вредоносных узлов, а также точность, полнота и F1-мера.

В сценарии без атаки различия между методами практически отсутствовали, что подтверждает нейтральность доверительного механизма в штатном режиме. В атакуемом сценарии наихудший результат показал подход без доверия: средний риск атакующего воздействия составил 0,248, а F1-мера была равна нулю. Метод прямого доверия улучшил показатели незначительно: риск снизился до 0,246, а F1-мера возросла до 0,204. Наилучший результат получен при использовании транзитивного доверия: риск атакующего воздействия уменьшился до 0,205, а F1-мера достигла 0,420.

Преимущество транзитивного доверия наблюдалось во всех топологиях. Наиболее заметный эффект получен для древовидной структуры, где прирост F1-меры относительно метода прямого доверия составил 0,2644, а снижение риска атакующего воздействия – 0,0451. Это связано с ограниченным числом прямых соседей у части узлов, из-за чего транзитивные цепочки эффективнее компенсируют недостаток прямых наблюдений.

Дополнительное сравнение вариантов метода показало, что различия между использованием одного и нескольких маршрутов невелики. Отказ от ослабления доверия по длине цепочки также привел лишь к небольшому изменению средних значений. Таким образом, предложенный метод повышает устойчивость распределенного выбора планов в условиях ограниченной связности и наличия вредоносных узлов. В дальнейшем целесообразно рассмотреть динамически изменяющуюся связность и задержки передачи сообщений.

Список использованных источников:

1. Phadke A., Medrano F. A. Towards resilient UAV swarms – a breakdown of resiliency requirements in UAV swarms // Drones. 2022. Vol. 6, no. 11. Art. 340. DOI: 10.3390/drones6110340.

2. Tsao K.-Y., Girdler T., Vassilakis V. G. A survey of cyber security threats and solutions for UAV communications and flying ad-hoc networks // Ad Hoc Networks. 2022. Vol. 133. Art. 102894. DOI: 10.1016/j.adhoc.2022.102894.

3. Adil M., Jan M. A., Liu Y., Abulkasim H., Farouk A., Song H. A systematic survey: security threats to UAV-aided IoT applications, taxonomy, current challenges and requirements with future research directions // IEEE Transactions on Intelligent Transportation Systems. 2023. Vol. 24, no. 2. P. 1437–1455. DOI: 10.1109/TITS.2022.3220043.

4. Hosseinzadeh M., Mohammed A. H., Alenizi F. A., Malik M. H., Yousefpoor E., Yousefpoor M. S., Ahmed O. H., Rahmani A. M., Tightiz L. A novel fuzzy trust-based secure routing scheme in flying ad hoc networks // Vehicular Communications. 2023. Vol. 44. Art. 100665. DOI: 10.1016/j.vehcom.2023.100665.

5. Wang X., Zhao Z., Yi L., Ning Z., Guo L., Yu F. R., Guo S. A survey on security of UAV swarm networks: attacks and countermeasures // ACM Computing Surveys. 2024. Vol. 57, no. 3. Art. 3703625. DOI: 10.1145/3703625.

6. Bai N., Hu X., Wang S. A survey on unmanned aerial systems cybersecurity // Journal of Systems Architecture. 2024. Vol. 156. Art. 103282. DOI: 10.1016/j.sysarc.2024.103282.

7. Chandrasekar V., Shanmugavalli V., Mahesh T. R., Shashikumar R., Borah N., Vinoth Kumar V., Guluwadi S. Secure malicious node detection in flying ad-hoc networks using enhanced AODV algorithm // Scientific Reports. 2024. Vol. 14. Art. 7818. DOI: 10.1038/s41598-024-57480-6.

8. Ceviz O., Sen S., Sadioglu P. A survey of security in UAVs and FANETs: issues, threats, analysis of attacks, and solutions // IEEE Communications Surveys & Tutorials. 2025. Vol. 27. P. 3227–3265. DOI: 10.1109/COMST.2024.3515051.

Goryainov S.A., Dibrov N.
North-Caucasus Federal University, Stavropol

Scientific supervisor:
Petrenko V. I.
North-Caucasus Federal University, Stavropol

A METHOD FOR UAV SWARM COORDINATION WITH TRUST PROPAGATION ALONG TRANSITIVE CHAINS UNDER LIMITED CONNECTIVITY

Abstract. The paper considers the problem of coordinating a UAV swarm under limited network connectivity and in the presence of malicious nodes. A method is proposed in which, when direct observations are insufficient, trust in a remote agent is formed using transitive communication chains with regard to path length and the reliability of intermediate nodes. Simulation results show that the proposed method reduces the risk of adversarial influence and improves the quality of malicious-node detection compared with baseline approaches.

Keywords: UAV swarm, coordination, trust, transitive trust, limited connectivity, malicious nodes, network resilience.

УДК 519.6

Долотов И.А., Кондратов М.С.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Хисаметдинова Г.К.
Уфимский университет науки и технологий, Уфа

ПРИМЕНЕНИЕ МОДЕЛИ «ХИЩНИК-ЖЕРТВА» ПРИ РЕШЕНИИ ЗАДАЧ ПО ОТРАЖЕНИЮ КИБЕРАТАК

Аннотация. На основе модели Лотки-Вольтерры в работе получено решение для отражения кибератак: построены графики отраженных атак и уровней защиты, позволяющие прогнозировать их поведение при изменении параметров.

Ключевые слова: математическое моделирование, модель Лотки-Вольтерры, решение системы дифференциальных уравнений.

Введение

В работе рассматривается применение модели «хищник-жертва», изначально разработанной в биологии для динамики популяций, в области кибербезопасности. Основное достоинство модели — адекватное описание циклического противоборства двух сторон, аналогичного взаимодействию «атакующий — система защиты». Цель исследования — адаптация данной модели и ее численный анализ для оценки эффективности противодействия кибератакам.

1. Описание математической модели «хищник-жертва» в аспекте задачи отражения кибератак

Исходная модель Лотки-Вольтерры может быть переписана как модель отражения кибератак, в которой функции «жертвы» и «хищника» отождествляются успешными атаками (x) и уровнем защиты от них (y), соответственно:

$$\begin{aligned} \frac{dx}{dt} &= (\alpha - \beta y)x \\ \frac{dy}{dt} &= (-\gamma + \delta x)y \end{aligned} \qquad (1)$$

где x – число успешных атак; y – уровень защиты, исчисляемый количеством, например, сетевых экранов; t– время; α – коэффициент увеличения атак; β – коэффициент, описывающий снижение численности атак за счет их подавления защитой; γ – коэффициент уменьшения уровня защиты при отсутствии атак; δ – коэффициент увеличения защиты, связанный с увеличением атак.

Если положить, что защита отсутствует, то, очевидно, что количество атак на объект будет стремительно (неограниченно) расти. В противоположном случае, когда атак не происходит какое-то время, уровень защиты резко падает. Такое поведение тривиально в условия задачи и не вызывает сомнений.

2. Вычислительный эксперимент и анализ параметрической чувствительности

Одной из актуальных задач информационной безопасности является моделирование процессов отражения кибератак. В этой задаче важно учитывать взаимодействие атакующей стороны (нарушителя) и защитной стороны (например, межсетевые экраны и шифрование данных).

На основе работы [1] вводятся параметры, ассоциируемые с параметрами модели – α, β, γ, δ и функциями – x, y. Так, параметр α – скорость распространения атак; β – эффективность защиты против атак; γ – скорость деградации защиты; δ – влияние атак на защиту; функция x – число успешных атак, y - уровень защищенности. В [1] за коэффициенты было приняты следующие значения: $\alpha=0{,}25$, $\beta=0{,}018$, $\gamma=0{,}12$, $\delta=0{,}009$.

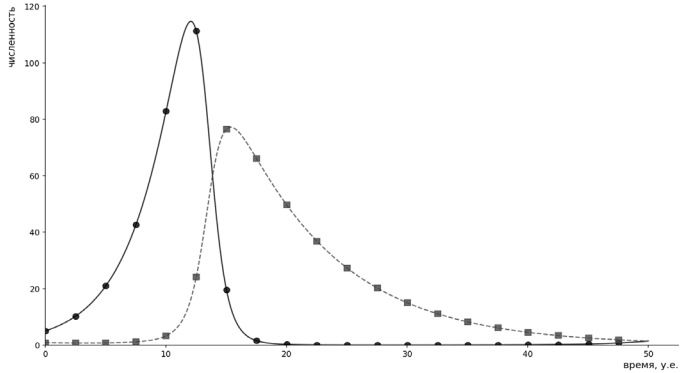


Рис. 1. Соотношение функций количества кибератак – y (сплошная линия) и отражений атак – x (пунктирная линия) во времени

На рисунке 1 представлен базовый сценарий с заданными параметрами. Характер изменения функций *x(t)* и *y(t)* соответствует реальным процессам: резкий рост уровня защищенности *x(t)* (с 6-й по 7-ю минуту) приводит к столь же резкому падению числа успешных атак *y(t)* (с 95% до 40%). Это демонстрирует итеративность систем защиты: скачок эффективности происходит после обнаружения угрозы.

Следующий рисунок 2 характеризует фазовую траекторию функций *x(t)* и *y(t)*. Четко прослеживаются замкнутый цикл поведения функций во времени. Очевидно, что при увеличении времени петля будет закручиваться внутрь. Количество временных петель будет возрастать до тех пор, пока не произойдет обнуление функций *x(t)* или *y(t)*.

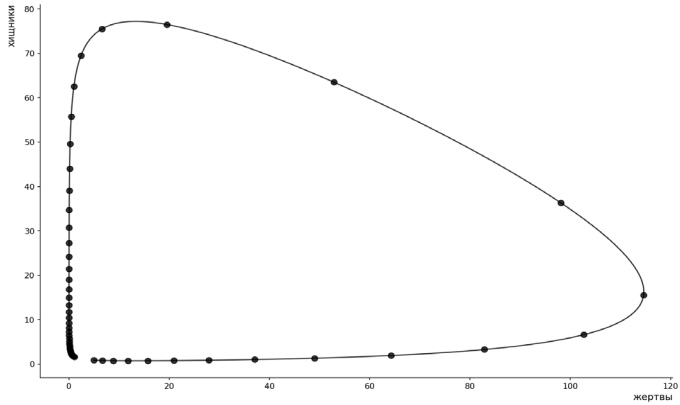


Рис. 2. Фазовая траектория функций количества кибератак и отражений во времени с данными: α=0,25, β=0,018, γ=0,12, δ=0,009

Заключение

Таким образом, для перехода системы защиты в устойчивый режим необходимо не просто наращивать ресурсы, но и внедрять превентивные механизмы (повышение δ) и сокращать время реакции (снижение α за счет проактивной разведки угроз).

Список использованных источников:

1. Trapeznikov E.V. // Modeling, Optimization and Information Technology. – 2024. – Т. 12, № 2.

Dolotov I.A., Kondratov M.S.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Khisametdinova G.K.
Ufa University of Science and Technology, Ufa

APPLICATION OF THE PREDATOR-PREY MODEL IN SOLVING CYBER ATTACK RESPONSE TASK

Abstract. Based on the Lotka-Volterra model, the paper provides a solution for repelling cyberattacks by constructing graphs of reflected attacks and protection levels that allow for predicting their behavior when parameters are changed.

Keywords: mathematical modeling, Lotka–Volterra model, numerical solution of a system of differential equations.

УДК 519.6

Долотов И.А., Кондратов М.С.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Гиззатова Э.Р.
Уфимский университет науки и технологий, Уфа

ОБ ИСПОЛЬЗОВАНИИ МОДЕЛИ «ХИЩНИК-ЖЕРТВА» В РЕШЕНИИ ЗАДАЧ ПО ОТРАЖЕНИЮ КИБЕРАТАК

Аннотация. В работе представлено решение задачи отражения кибератак на основе модели Лотки-Вольтерры. Показаны графики функций количества отраженных кибератак и функции количества

уровней защиты. Результаты моделирования позволяют прогнозировать поведение функций при изменении отдельных параметров модели.

Ключевые слова: математическое моделирование, модель Лотки-Вольтерры, решение системы дифференциальных уравнений.

Введение

Модель «хищник-жертва», традиционно применяемая в биологии для описания колебаний численности популяций, находит все более широкое применение в междисциплинарных областях. Ее ключевое преимущество – способность описывать циклические процессы противоборства двух сторон, где одна сторона оказывает давление на другую, что в точности соответствует схеме «атакующий – система защиты» в киберпространстве. Данная работа посвящена адаптации и численному анализу этой модели для прогнозирования эффективности отражения кибератак.

1. Математическая модель описания задачи динамики популяций «хищник-жертва»

В общем виде взаимодействие «жертва» (успешные атаки) и «хищник» (уровень защиты) описывается системой обыкновенных дифференциальных уравнений первого порядка:

$$\begin{aligned} \frac{dx}{dt} &= (\alpha - \beta y)x \\ \frac{dy}{dt} &= (-\gamma + \delta x)y \end{aligned} \qquad (1)$$

где x – численность популяции жертв; y – численность популяции хищников; t– время; α – коэффициент рождаемости жертв; β – коэффициент, описывающий снижение численности жертв за счет встреч с хищниками; γ – коэффициент смертности хищников в отсутствие пищи; δ – коэффициент прироста хищников, связанный с потреблением жертв.

В отсутствие защиты ($y=0$) число атак растет экспоненциально, а в отсутствие атак ($x=0$) защитные механизмы постепенно деградируют.

2.Анализ параметров чувствительности

Был проведен вычислительный эксперимент, заключающийся в сравнении получаемых расчетных данных с моделью при исходных значениях коэффициентов: α=0,25, β=0,018, γ=0,12, δ=0,009. Каждое значение было сначала увеличено, а затем уменьшено на 20%. Таким образом получилось провести сравнительный анализ расчетных кривых. Он выявил следующее:

Относительно параметра α, его увеличение на 20% ведет к тому, что:

1) число успешных атак возрастает примерно в 1,5 раза по сравнению с базовым сценарием;

2) система защиты реагирует на возросшую угрозу со значительной задержкой, что выражается в увеличении петли по горизонтали и вертикали.

Относительно параметра β, его уменьшение на 20% ведет к тому, что:

1) Пиковые значения *x(t)* возрастают почти на 40% по сравнению с базой;

2) Колебания становятся более затяжными, система защиты «захлебывается», не успевая нейтрализовать атаки.

Относительно параметра γ, его увеличение на 20% показывает, что:

1) Результаты моделирования показывают критическое снижение минимального уровня *y(t)* почти до нулевых значений, что соответствует временной потере контроля над системой.

2) Восстановление защиты требует существенно большего времени.

Относительно параметра δ, его увеличение на 20% приводит к:

1) Снижению амплитуды колебаний *x(t)*.

2) Быстрой стабилизации системы и выходу на более низкий, «подавленный» уровень атак.

Таблица 1

Анализ чувствительности параметров

Переменная	+20%	-20%	Вывод
α	+15 по y	-15 по y	Изменение параметра α влияет на изменение петли по вертикали, так и по горизонтали соответственно. При этом, можно отметить, что увеличение параметра заостряет как вертикаль петли, так и ее горизонталь. То есть, при увеличении α будет увеличивается частота волн и амплитуда.
β	-15 по y	+20 по y	Параметр β противоположен по смыслу параметру α. Петли также изменяются по осям абсцисс и ординат. При увеличении параметра затупляет вертикаль и горизонталь. То есть частота и амплитуда будут уменьшаться при увеличении параметра.
γ	+10 по x	-10 по x	В свою очередь γ изменяется только по горизонтали. При изменении параметра видно, что данный параметр заостряет только горизонталь петли. Значит изменятся будет только амплитуда.
δ	-15 по x	+25 по y	Параметр δ так же противоположен по смыслу γ. При увеличении параметра ось абсцисс затупляется. То есть при увеличении параметра амплитуда будет уменьшаться.

Заключение

На основании полученных результатов можно сделать следующие выводы:

1. Ключевым фактором нестабильности является скорость распространения атак (α). Даже незначительное увеличение этого параметра ведет к экспоненциальному росту амплитуды колебаний и риску пропуска критического числа инцидентов.

2. Деградация защиты (γ) представляет собой скрытую угрозу: при ее ускорении система может войти в режим глубоких «провалов» защищенности, что критично для непрерывных производств.

3. Повышение эффективности реагирования (δ) (внедрение SOC, SOAR) является наиболее эффективной мерой стабилизации, позволяющей не только снизить ущерб, но и перевести систему в режим с малой амплитудой колебаний.

4. Увеличение средней численности успешных атак за период колебаний однозначно прогнозирует рост общего ущерба от реализации угроз информационной безопасности.

Список использованных источников:

1. Trapeznikov E.V. // Modeling, Optimization and Information Technology. – 2024. – Т. 12, № 2.

Dolotov I.A., Kondratov M.S.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Gizzatova E.R.
Ufa University of Science and Technology, Ufa

APPLICATION OF THE PREDATOR-PREY MODEL IN SOLVING THE PROBLEM OF REJECTING CYBER ATTACKS

Abstract. The paper presents a numerical solution to the problem of cyberattack response based on the Lotka–Volterra model. Graphs of the function of the number of repelled cyberattacks and the function of the number of protection levels are provided. The simulation results make it possible to predict the behavior of the functions when individual parameters of the model are changed.

Keywords: mathematical modeling, Lotka–Volterra model, numerical solution of a system of differential equations.

УДК 004.056

Еремина Л.А.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Сенцова А.Ю.
Уфимский университет науки и технологий, Уфа

СРАВНИТЕЛЬНЫЙ АНАЛИЗ МЕТОДОВ МАШИННОГО ОБУЧЕНИЯ ДЛЯ ОБНАРУЖЕНИЯ АНОМАЛИЙ В ПРОТОКОЛЕ MODBUS/TCP ПРОМЫШЛЕННОГО ИНТЕРНЕТА ВЕЩЕЙ

Аннотация. В статье рассматриваются методы машинного обучения для обнаружения аномалий в протоколе Modbus/TCP промышленного интернета вещей (IIoT). Проведен сравнительный анализ алгоритмов XGBoost, LightGBM, SVM, KNN и Decision Tree. Особое внимание уделено оценке качества обнаружения и применимости методов в условиях ограниченных ресурсов промышленных контроллеров. Показано, что ансамблевые методы градиентного бустинга обеспечивают наилучшие показатели полноты и F1-меры.

Ключевые слова: промышленный интернет вещей, Modbus/TCP, обнаружение аномалий, машинное обучение, XGBoost, LightGBM, безопасность IIoT.

Введение

Промышленный интернет вещей (IIoT) обеспечивает интеграцию интеллектуальных устройств в единую цифровую экосистему, реализуя концепцию «Индустрии 4.0» [1]. Однако этот технологический прорыв сопровождается серьезными вызовами в области кибербезопасности и приводит к появлению новых, ранее неизвестных уязвимостей. Особую озабоченность специалистов вызывает использование устаревших протоколов, среди которых Modbus/TCP остается одним из наиболее распространенных [2]. Простота и повсеместное использование протокола на промышленных объектах оборачивается критическими уязвимостями – отсутствием аутентификации, шифрования и проверки целостности данных [3].

Актуальность исследования обусловлена ростом кибератак на объекты критической инфраструктуры, в частности, на объекты промышленных субъектов критической информационной инфраструктуры. Традиционные сигнатурные методы защиты неэффективны против формально корректных, но семантически вредоносных сообщений, что требует применения интеллектуальных

методов анализа [4]. В данной работе проведен сравнительный анализ методов машинного обучения для обнаружения аномалий в трафике Modbus/TCP.

Актуальность проблемы безопасности промышленных сетей

Протокол Modbus/TCP построен по принципу «клиент-сервер», сообщения передаются через порт 502 [5]. Структура сообщения включает заголовок MBAP (7 байт) и блок данных PDU с кодом функции [6].

Отсутствие аутентификации и шифрования позволяет злоумышленнику перехватывать команды, подменять параметры, инициировать DoS-атаки и сканировать сеть. Согласно репозиторию PLC-SoK [7], через Modbus/TCP реализуются такие атаки, как *False Command Injection Attack*, *Modbus Flooding Attack*, *Password reset attack* и *ROP Attack*. Все перечисленные уязвимости и атаки могут привести к нарушению технологического процесса на объекте. Это обусловливает применение методов поведенческого анализа на основе машинного обучения для превентивного обнаружения атак и детектирования аномалий. Кроме того, в соответствии с Федеральным законом № 187-ФЗ [8], приоритетной задачей системы безопасности на объекте КИИ является предупреждение атак, что также подтверждает актуальность темы исследования.

Методы машинного обучения для обнаружения аномалий

В исследовании рассматриваются следующие методы машинного обучения:

XGBoost – градиентный бустинг на ансамбле деревьев решений, эффективен на структурированных данных, устойчив к переобучению [9].

LightGBM – реализация градиентного бустинга с высокой скоростью обучения и низким потреблением памяти за счет техник GOSS и EFB [10].

SVM – классический метод, эффективен при работе с данными высокой размерности [11].

KNN – непараметрический алгоритм, классифицирующий объект на основе голосования ближайших соседей.

Decision Tree – иерархическая структура правил, обладающая высокой интерпретируемостью [12].

Экспериментальная оценка

Для проведения эксперимента используется набор реальных пакетов Modbus/TCP (609 934 записи) [13]. Датасет дополнен метками на основе сценариев атак из PLC-SoK [8]. Объем аномального трафика – 15% выборки. Реализация выполнена на Python с использованием scikit-learn, xgboost, lightgbm. Оценка проводилась по метрикам Accuracy, Precision, Recall, F1-score, ROC-AUC с кросс-валидацией (рис.1).

Метод	Accuracy	Precision	Recall	F1-score	ROC-AUC	Время обучения (с)
XGBoost	0.992	0.981	0.965	0.973	0.997	124
LightGBM	0.991	0.979	0.963	0.971	0.996	87
SVM (RBF)	0.975	0.941	0.912	0.926	0.983	342
KNN (k=5)	0.968	0.925	0.908	0.916	0.975	12
Decision Tree	0.961	0.903	0.897	0.900	0.958	8

*Рис. 1.*Сравнительная оценка методов машинного обучения

Анализ результатов

Методы градиентного бустинга (XGBoost, LightGBM) показывают лучшие результаты (F1-score > 0.97). LightGBM выигрывает по времени обучения (87 с против 124 с у XGBoost), что важно для систем с периодическим переобучением. SVM уступает по времени (342 с) при сопоставимом качестве. KNN и Decision Tree демонстрируют низшие метрики, что может приводить к недопустимому уровню ложных срабатываний.

Полнота (Recall) для XGBoost и LightGBM составляет 96.5% и 96.3% соответственно. Для критической инфраструктуры пропуск атаки (false negative) недопустим, что делает высокую полноту ключевой характеристикой.

Заключение

Проведенное исследование подтверждает, что ансамблевые методы градиентного бустинга (XGBoost, LightGBM) демонстрируют наилучшие показатели (F1-score > 0.97), что делает их предпочтительным выбором для защиты критической инфраструктуры. LightGBM обеспечивает сопоставимое качество при меньшем времени обучения. Дальнейшие исследования могут быть направлены на гибридные подходы (CNN + градиентный бустинг) и адаптацию алгоритмов к распределенным архитектурам с федеративным обучением.

Список использованных источников:

1. Ghobakhloo, M. (2019). Industry 4.0, digitization, and opportunities for sustainability. *Journal of Cleaner Production*, 252, 119869.

2. Sergi, F. Securing Modbus in legacy industrial control systems: A decentralized approach using proxies, Post-Quantum Cryptography and Self-

Sovereign Identity / F. Sergi // Journal of Information Security and Applications. – 2025. – Vol. 89.

3. Modbus Organization. (2006). Modbus Application Protocol Specification V1.1b3.

4. Kotzanikolaou, P., et al. (2025). Defending industrial internet of things against Modbus/TCP threats. International Journal of Information Security, 24, 157.

5. Modbus Organization. (2012). Modbus Messaging on TCP/IP Implementation Guide V1.0b.

6. Caselli, M., et al. (2015). Anomaly detection in Modbus/TCP networks. International Journal of Critical Infrastructure Protection, 11, 42-55.

7. Lopez-Morales, E., et al. (2023). PLC-SoK Dataset. GitHub. URL: https://github.com/efrenlopezm/plc-sok-dataset.

8. Федеральный закон от 26.07.2017 № 187-ФЗ (ред. от 26.07.2017) «О безопасности критической информационной инфраструктуры Российской Федерации» // КонсультантПлюс: [сайт]. URL: https:// www.consultant.ru/document/cons_doc_LAW_220885/ (дата обращения: 07.04.2026).

9. Chen, T., Guestrin, C. (2016). XGBoost: A Scalable Tree Boosting System. *KDD*, 785-794.

10. Ke, G., et al. (2017). LightGBM: A Highly Efficient Gradient Boosting Decision Tree. *NIPS*, 30, 3146-3154.

11. Cortes, C., Vapnik, V. (1995). Support-vector networks. Machine Learning, 20, 273-297.

12. Quinlan, J.R. (1986). Induction of decision trees. Machine Learning, 1, 81-106.

13. IEEE DataPort. (2025). A large dataset of 609,934 real Modbus packets. [Online].

Eremina L.A.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Sentsova A.Yu.
Ufa University of Science and Technology, Ufa

COMPARATIVE ANALYSIS OF MACHINE LEARNING METHODS FOR ANOMALY DETECTION IN MODBUS/TCP PROTOCOL OF INDUSTRIAL INTERNET OF THINGS

Abstract. The article discusses machine learning methods for anomaly detection in the Modbus/TCP protocol of the Industrial Internet of Things

(IIoT). A comparative analysis of XGBoost, LightGBM, SVM, KNN, and Decision Tree algorithms is carried out. Special attention is paid to evaluating the detection quality and applicability of the methods under the resource-constrained conditions of industrial controllers. It is shown that ensemble gradient boosting methods provide the best performance in terms of recall and F1-score.

Keywords: Industrial Internet of Things, Modbus/TCP, anomaly detection, machine learning, XGBoost, LightGBM, IIoT security.

УДК 004.942

Жигальцова Е.А., Чижевский И.А.
Томский государственный университет систем управления и радиоэлектроники, Томск

Научный руководитель:
Фаерман В.А.
Томский государственный университет систем управления и радиоэлектроники, Томск

АДАПТАЦИЯ ТИПОВОЙ МОДЕЛИ МАССОВОГО ОБСЛУЖИВАНИЯ ДЛЯ АНАЛИЗА ОТКАЗОУСТОЙЧИВЫХ СИСТЕМ ОБРАБОТКИ ЗАЯВОК В КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЕ

Аннотация. В статье рассматривается адаптация типовой модели массового обслуживания M/M/1 для анализа функционирования систем обработки заявок в условиях отказов и резервирования в составе критической информационной инфраструктуры. Предложено расширение модели параметрами, учитывающими надежность и энергопотребление. Показано, что такая адаптация позволяет формализовать задачу обеспечения заданного времени отклика при ограничениях на ресурсы.

Ключевые слова: СМО, M/M/1, резервирование, отказ сервера, производительность, энергопотребление.

Современные программные и вычислительные системы функционируют в условиях случайных потоков запросов, ограниченных ресурсов и возможных отказов оборудования. В таких системах ключевыми характеристиками являются время обработки заявок, вероятность потерь и устойчивость функционирования. Для анализа подобных процессов применяются теория массового обслуживания [1] и имитационное моделирование [2], позволяющие формализовать

поведение системы и исследовать ее характеристики в различных режимах работы.

Рассматриваемая система представляет собой вычислительный узел обработки заявок в условиях реального времени, функционирующий в составе критической информационной инфраструктуры. В подобных системах, в частности в автоматизированных системах управления технологическими процессами, ключевым требованием является обеспечение предсказуемого времени обработки заявок даже при отказах оборудования. Методы теории массового обслуживания широко применяются для оценки времени отклика и анализа поведения таких систем [1, 3, 4].

В процессе функционирования возможны отказы основного сервера, что приводит к необходимости использования резервных вычислительных ресурсов. Обеспечение живучести системы в условиях отказов является актуальной задачей, в том числе в контексте информационной безопасности, поскольку атаки на АСУ ТП могут приводить к выводу элементов инфраструктуры из строя [5, 6].

Для анализа используется типовая модель массового обслуживания M/M/1, расширенная с учетом отказов и механизмов резервирования. В базовой модели поток заявок считается пуассоновским, а время обслуживания распределенным по экспоненциальному закону [1]. В предлагаемой работе модель модифицируется с учетом особенностей рассматриваемой системы, что позволяет учитывать влияние отказов, восстановления и переключения на резерв на характеристики функционирования.

Особенностью модели является учет различных сценариев активации резервного сервера, включая автоматическое и ручное переключение. В случае теплого резерва включение может происходить автоматически с вероятностью P_auto за время T_activate_auto, а при его неудаче используется ручной режим с временем активации T_activate_manual. Для холодного резерва вводится параметр T_turnon, характеризующий время полного запуска сервера, превышающее время активации теплого резерва.

В рамках исследования решается задача обеспечения заданного времени отклика системы при отказах основного сервера с одновременной оптимизацией потребления ресурсов. В качестве ресурса рассматривается энергопотребление системы, зависящее от режима работы серверов. Таким образом, задача формулируется как поиск компромисса между производительностью и энергозатратами при различных стратегиях резервирования. Основные параметры модели приведены в таблице 1.

Таблица 1

Параметры модели с учетом отказов и энергопотребления

Обозначение	Параметр	Описание
MTBA	Интервал поступления	Среднее время между поступлениями заявок
MST	Время обслуживания	Среднее время обработки заявки
MTBF	Время до отказа	Среднее время работы сервера до отказа
MRT	Время восстановления	Среднее время восстановления сервера
R	Режим резервирования	Горячий, теплый или холодный резерв
P_active	Активное потребление	Потребление основного сервера
P_idle	Потребление ожидания	Потребление горячего резерва / простоя
P_reserve	Потребление резерва	Потребление теплого резерва
T_activate_auto	Автоматическая активация	Время включения резерва при успешной автоматике
P_auto	Вероятность автоактивации	Вероятность успешного автоматического переключения
T_activate_manual	Ручная активация	Время включения резерва оператором
T_turnon	Запуск холодного резерва	Время полного включения сервера

Введенные параметры позволяют расширить классическую модель M/M/1 и учитывать дополнительные аспекты функционирования системы, связанные с отказами и управлением резервными ресурсами. В отличие от базовой модели, предложенный подход позволяет учитывать не только интенсивности поступления и обслуживания заявок, но и характеристики надежности системы, включая время до отказа, время восстановления и механизмы переключения на резерв.

Такое расширение модели делает возможным анализ систем, функционирующих в условиях неопределенности и ограниченных ресурсов, что особенно важно для критической информационной инфраструктуры. Использование параметров, связанных с энергопотреблением, позволяет дополнительно учитывать эффективность работы системы и формировать критерии оптимизации, ориентированные не только на производительность, но и на ресурсосбережение [2].

Предложенная модель может применяться для анализа систем обработки событий в сенсорных сетях и других распределенных вычислительных системах, функционирующих в условиях ограниченных ресурсов и нестабильной нагрузки. Использование расширенной модели массового обслуживания позволяет формализовать задачи обеспечения надежности и энергоэффективности и обосновывать выбор параметров

функционирования систем в составе критической информационной инфраструктуры [3, 4].

Список использованных источников:

1. Бочаров П.П., Печинкин А.В. Теория массового обслуживания. – М.: РУДН, 2005.

2. Лоу А.М. Имитационное моделирование. Классика CS. 3-е изд. – СПб.: Питер, 2007.

3. Вишневский В.М., Самуйлов К.Е. Системы массового обслуживания в телекоммуникационных сетях // Итоги науки и техн. Сер. Электросвязь. – 2000. – Т. 19. – С.

4. Case of discrete-event simulation of the simple sensor node with cpn tools – Vladimir Faerman, Kirill Voevodin, Valeriy Avramchuk. URL: https://scholar.google.com/citations?view_op=view_citation&hl=en&user=HJu4q9cAAAAJ&citation_for_view=HJu4q9cAAAAJ:ldfaerwXgEUC (дата обращения 03.04.2026).

5. Сценарий атаки на автоматизированную систему управления технологическим процессом с учетом уязвимости протокола Modbus TCP – А.А. Конев, В.С. Репкин, К.И. Цимбалов. URL: https://cyberleninka.ru/article/n/stsenariy-ataki-na-avtomatizirovannuyu-sistemu-upravleniya-tehnologicheskim-protsessom-s-uchetom-uyazvimosti-protokola-modbus-tcp/viewer (дата обращения 05.04.2026).

6. Интервальное прогнозирование интенсивности кибератак на объекты критической информационной инфраструктуры – Ю. М. Краковский, Б. В. Курчинский, А. Н. Лузгин // Доклады ТУСУР. – 2018. – Т. 21, № 1. URL: https://journal.tusur.ru/ru/arhiv/1-2018/intervalnoe-prognozirovanie-intensivnosti-kiberatak-na-ob-ekty-kriticheskoy-informatsionnoy-infrastruktury (дата обращения 05.04.2026).

Zhigaltsova E.A., Chizhevsky I.A.
Tomsk State University of Control Systems and Radioelectronics, Tomsk

Scientific supervisor:
Faerman V.A.
Tomsk State University of Control Systems and Radioelectronics, Tomsk

PERFORMANCE EVALUATION OF A SYSTEM WITH AN UNRELIABLE SERVER AND REDUNDANCY BASED ON A CLASSICAL QUEUEING MODEL

Abstract. The paper considers the adaptation of the classical M/M/1 queueing model for analyzing the operation of request processing systems

under conditions of server failures and redundancy within critical information infrastructure. The model is extended with parameters reflecting reliability and energy consumption. It is shown that such an adaptation makes it possible to formalize the problem of ensuring a required response time under resource constraints.

Keywords: queueing system, M/M/1, redundancy, server failure, performance, energy consumption

УДК 004.056.53

Занин Д.С.
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина), Санкт-Петербург

Научный руководитель:
Петренко С.А.
Научно-технологический университет «Сириус», Сочи

МЕТОД ОБЕСПЕЧЕНИЯ СЕМАНТИЧЕСКОЙ БЕЗОПАСНОСТИ РАСПРЕДЕЛЕННЫХ ПРОГРАММНЫХ СИСТЕМ НА ОСНОВЕ ИНТЕЛЛЕКТУАЛЬНОГО СЕМАНТИЧЕСКОГО ИММУНИТЕТА

Аннотация. Предложен метод семантической безопасности микросервисных и облачных систем на основе интеллектуального семантического иммунитета. Метод использует двойное представление состояния: формальные безразмерные инварианты и семантические эмбеддинги. Гибридный критерий выявляет аномалии, а ANN‑ поиск и RAG/LLM интерпретируют инциденты. Реализованы адаптивная реакция, самовосстановление и эволюционное обучение с MLOps. Формируется иммунная память системы.

Ключевые слова: семантическая безопасность, микросервисы, инварианты, гибридная детекция, RAG, LLM, самовосстановление, MLOps.

Современные распределенные программные системы (микросервисные, контейнерные, облачные) обладают высокой динамичностью и сложностью взаимодействия компонентов. Традиционные средства защиты, основанные на сигнатурном анализе и статических правилах, плохо выявляют сложные поведенческие аномалии и семантические атаки [1, 2]. Актуальна задача создания метода, способного анализировать поведение системы на смысловом уровне с учетом контекста эксплуатации.

В работе предлагается метод обеспечения семантической безопасности, реализующий концепцию интеллектуального семантического иммунитета. Метод рассчитан на архитектуры с развитой наблюдаемостью (метрики, логи, распределенные трассировки) и интегрируется с оркестраторами (например, Kubernetes). Подход базируется на двойном представлении состояния: формальном (безразмерные инварианты подобия) и семантическом (векторные эмбеддинги состояния).

Структура метода включает шесть этапов.

1. Формально-семантическое моделирование. Для каждого компонента выделяются формальные параметры состояния $P_i(t) = \{p_i1(t), p_i2(t), \ldots, p_ik_i(t)\}$ (латентность, частота запросов, число ошибок, загрузка ресурсов и др.). Параллельно на основе данных наблюдаемости модель-кодировщик формирует семантический эмбеддинг компонента $E_i(t)$ и агрегированный эмбеддинг системы $E_{system}(t)$, отражающий межсервисные взаимодействия.

2. Выявление системных инвариантов и обучение нормы. По теории подобия формальные параметры объединяются в безразмерные инварианты $\Pi_{sys} = \{\Pi_1, \Pi_2, \ldots, \Pi_n\}$. На исторических данных нормальной работы для каждого Π_i строятся адаптивные трубы нормальности $T_i = [\Pi_{i\_min}, \Pi_{i\_max}]$. В семантическом пространстве формируется эталон $E_{platform\_etalon}$ и порог допустимого отклонения d_{thresh}.

3. Гибридный онлайн-мониторинг. В реальном времени вычисляются текущие $\Pi_i(t)$ и $E_{system}(t)$. Аномалия регистрируется при выполнении гибридного критерия: $F_{hybrid}(t) = (\exists\, i: \Pi_i(t) \notin T_i) \vee (distance(E_{system}(t), E_{platform\_etalon}) > d_{thresh})$.

4. Интеллектуальный анализ инцидента. По эмбеддингу инцидента в векторной базе $E_{incidents\_db}$ выполняется ANN-поиск похожих прецедентов. Контекст (нарушенные инварианты, метрики, найденные прецеденты) подается в RAG-конвейер, где большая языковая модель генерирует объяснимую гипотезу причины и рекомендации [3, 8].

5. Адаптивная реакция и самовосстановление. На основе гипотезы и множества допустимых действий A (масштабирование, рестарт, изоляция, откат и др.) формируется стратегия восстановления, исполняемая через оркестратор. Успех восстановления подтверждается возвратом инвариантов в допустимые диапазоны и уменьшением семантического отклонения.

6. Активное тестирование и эволюционное обучение. В staging-среде с помощью LLM генерируются синтетические семантические атаки. Результаты пополняют базу инцидентов, после чего модели нормы и пороги периодически актуализируются (MLOps-контур). Так

формируется иммунная память системы, повышающая устойчивость к новым угрозам.

Таким образом, предложенный метод обеспечивает переход от пассивной защиты к активному поддержанию семантической целостности поведения распределенной системы. Он объединяет интерпретируемые формальные инварианты и семантический анализ, реализует гибридную детекцию, когнитивную интерпретацию инцидентов с помощью RAG/LLM, адаптивное самовосстановление и замкнутый цикл обучения. Метод позволяет обнаруживать ранее неизвестные аномалии, объяснять их причины и накапливать опыт в виде иммунной памяти, повышая устойчивость системы в условиях непрерывной эволюции архитектуры и угроз.

Список использованных источников:

1. Костюков Н.А., Кулямин В.В. Наблюдаемость и мониторинг распределенных программных систем // Труды ИСП РАН. 2021. Т. 33. № 4. С. 45-60.

2. Li B., Peng X., Xiang Q. et al. Enjoy Your Observability: An Industrial Survey of Microservice Tracing and Analysis // Empirical Software Engineering. 2022. Vol. 27. Art. 25.

3. Зимин С.В., Мельников А.Ю. Методы обнаружения аномалий в распределенных вычислительных системах // Программные системы: теория и приложения. 2020. Т. 11. № 2. С. 85-102.

4. Thalheim J. et al. Sieve: Actionable Insights from Monitored Metrics in Microservices. arXiv:1709.06686, 2017.

5. Waseem M. et al. Design, Monitoring, and Testing of Microservices Systems: The Practitioners' Perspective. arXiv:2108.03384, 2021.

6. Кузнецов Д.А., Марков А.С. Анализ безопасности распределенных информационных систем // Вопросы кибербезопасности. 2019. № 3. С. 18-28.

7. Niedermaier S. et al. On Observability and Monitoring of Distributed Systems: An Industry Interview Study. arXiv:1907.12240, 2019.

8. Chen Z. et al. Eadro: An End-to-End Troubleshooting Framework for Microservices on Multi-Source Data. arXiv:2302.05092, 2023.

9. Huang J. et al. Twin Graph-based Anomaly Detection via Attentive Multi-Modal Learning for Microservice System. arXiv:2310.04701, 2023.

10. Akmeemana L. et al. GAL-MAD: Towards Explainable Anomaly Detection in Microservice Applications Using Graph Attention Networks. arXiv:2504.00058, 2025.

11. Albuquerque C., Correia F. Tracing and Metrics Design Patterns for Monitoring Cloud-Native Applications. arXiv:2510.02991, 2025.

12. Zhu Z. et al. UniSage: A Unified and Post-Analysis-Aware Sampling for Microservices. arXiv:2509.26336, 2025.

Zanin D.S.
Saint Petersburg Electrotechnical
University «LETI», Saint-Petersburg

Scientific supervisor:
Petrenko S.A.
Sirius University of Science and Technology, Sochi

A METHOD FOR ENSURING SEMANTIC SECURITY OF DISTRIBUTED SOFTWARE SYSTEMS BASED ON INTELLIGENT SEMANTIC IMMUNITY

Abstract. A method for semantic security of microservice and cloud systems based on intelligent semantic immunity is proposed. The method uses dual state representation: formal dimensionless invariants and semantic embeddings. A hybrid criterion detects anomalies, while ANN search and RAG/LLM interpret incidents. Adaptive response, self-healing, and evolutionary learning with MLOps are implemented. An immune memory of the system is formed.

Keywords: semantic security, microservices, invariants, hybrid detection, RAG, LLM, self-healing, MLOps.

УДК 004.056.53

Занин Д.С.
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина), Санкт-Петербург

Научный руководитель:
Петренко С.А.
Научно-технологический университет «Сириус», Сочи

МОДЕЛЬ ИНТЕЛЛЕКТУАЛЬНОЙ СЕМАНТИЧЕСКОЙ БЕЗОПАСНОСТИ РАСПРЕДЕЛЕННЫХ ПРОГРАММНЫХ СИСТЕМ И ОЦЕНКА ЕЕ ЭФФЕКТИВНОСТИ ПО СИСТЕМНЫМ СВОЙСТВАМ

Аннотация. Предложена интегральная модель интеллектуальной семантической безопасности распределенных систем, основанная на двойном представлении состояния: формальном (безразмерные

инварианты подобия) и семантическом (векторные эмбеддинги). Модель включает гибридную детекцию, память инцидентов, когнитивный анализ на базе RAG/LLM и адаптивную реакцию. Описан метод применения модели как шестиэтапный контур. Эффективность оценивается по трем системным свойствам: качество обнаружения, оперативность анализа, результативность реакции.

Ключевые слова: семантическая безопасность, распределенные системы, инварианты подобия, эмбеддинги, гибридная детекция, RAG, LLM, адаптивная реакция.

Современные распределенные системы (микросервисные, облачные, контейнеризованные) функционируют в условиях высокой динамики конфигураций, нагрузок и состава компонентов, что усложняет обеспечение информационной безопасности. Традиционные сигнатурные и статистические методы недостаточно эффективны для выявления сложных поведенческих аномалий и семантических атак [1, 2]. В работе предлагается модель интеллектуальной семантической безопасности, реализующая концепцию семантического иммунитета и объединяющая формальный и семантический анализ поведения системы.

Интегральная модель M_int описывается кортежем:

M_int = ⟨G, A, P, Π, T, M_enc, E_etalon, E_incidents_db, F_hybrid, LLM, R_adaptive⟩,

где G – формальная грамматика поведения, A – автоматная модель, P – множество формальных параметров состояния, Π – безразмерные инварианты подобия, T – трубы допустимых значений, M_enc – модель-кодировщик для построения эмбеддингов E(t), E_etalon – семантический эталон нормы, E_incidents_db – векторная база инцидентов, F_hybrid – гибридная функция обнаружения, LLM – большая языковая модель для объяснения и генерации сценариев, R_adaptive – функция адаптивной реакции [3].

Состояние системы представляется одновременно в двух независимых пространствах: формальном (параметры P(t) и инварианты Π_i(t) = f_i(P(t))) и семантическом (эмбеддинг E(t) = M_enc(Obs(t))). На исторических данных нормальной работы формируются трубы T_i = [Π_i^min, Π_i^max] и эталон E_etalon. Гибридная детекция фиксирует аномалию при нарушении хотя бы одного критерия:

F_hybrid(t) = (∃ i: Π_i(t) ∉ T_i) ∨ (distance(E(t), E_etalon) > d_thresh).

Для анализа инцидента выполняется ANN-поиск похожих прецедентов в базе E_incidents_db, после чего RAG-конвейер с LLM генерирует объяснимую гипотезу причины и рекомендации по реакции. Адаптивная функция R_adaptive выбирает оптимальное действие из

множества допустимых реакций A (масштабирование, рестарт, изоляция, откат версии и др.) и инициирует восстановление через оркестратор.

Метод применения модели представляет собой шестиэтапный контур:

1) формально-семантическое моделирование компонентов и взаимодействий;

2) выявление инвариантов П и обучение нормы (трубы T_i и эталон E_etalon);

3) онлайн-мониторинг и гибридная детекция аномалий;

4) интеллектуальный анализ инцидента (ANN + RAG/LLM);

5) адаптивная реакция и восстановление;

6) проактивное тестирование (генерация синтетических атак LLM) и эволюционное обучение с накоплением опыта в базе инцидентов (MLOps).

Оценка эффективности проводится по трем системным свойствам, соответствующим ключевым компонентам модели.

Семантическая безопасность (качество обнаружения) оценивается сравнением трех режимов детекции – только по инвариантам, только по эмбеддингам и гибридного – на наборе сценариев, включая синтетические семантические атаки. Используются метрики Precision, Recall, F1 и PR-AUC. Эффективность подтверждается ростом Recall и PR-AUC при контролируемом уровне ложных срабатываний.

Операционная эффективность (время обнаружения и анализа) измеряется метриками MTTD (среднее время обнаружения) и Time‑to‑triage (время до формирования диагностической гипотезы). Сравниваются варианты: традиционный ручной анализ, ANN‑поиск без LLM и полный контур с RAG/LLM. Ожидается сокращение времени анализа при использовании интеллектуального слоя.

Эффективность реакции и восстановления оценивается по среднему времени восстановления (MTTR) и доле предотвращенного ущерба. Сравниваются статическая реакция по правилам и адаптивная реакция R_adaptive с учетом контекста. Критерий успеха – снижение MTTR и повышение устойчивости восстановления.

Таким образом, предложенная модель и метод обеспечивают переход от пассивной защиты к активному поддержанию семантической целостности поведения распределенной системы. Гибридное представление состояния, память инцидентов, когнитивная интерпретация на основе LLM и замкнутый цикл обучения позволяют эффективно обнаруживать, объяснять и нейтрализовывать как известные, так и ранее неизвестные семантические нарушения.

Список использованных источников:

1. Shimmi S., Okhravi H., Rahimi M. AI-Based Software Vulnerability Detection: A Systematic Literature Review. arXiv:2506.10280, 2025.
2. Марков А.С., Барабанов А.В. Статический анализ программного обеспечения: методы и инструменты. М.: Горячая линия – Телеком, 2017. 312 с.
3. Harzevili N.S. et al. A Survey on Automated Software Vulnerability Detection Using Machine Learning and Deep Learning. arXiv:2306.11673, 2023.
4. Касперский Е.В., Бородин А.А. Современные методы обнаружения уязвимостей программного обеспечения // Вопросы кибербезопасности. 2021. № 4. С. 2–12.
5. Hulayyil S.B., Li S., Xu L. Machine-Learning-Based Vulnerability Detection and Classification in Internet of Things Device Security // Electronics. 2023. Vol. 12(18). Art. 3927.
6. Петров А.А., Зенкин А.А. Методы статического анализа программного кода для выявления уязвимостей // Информационная безопасность. 2020. Т. 23, № 3. С. 45–54.
7. Bensaoud A., Kalita J. Advancing Software Security: DcodeBERT for Automatic Vulnerability Detection and Repair. SSRN Preprint, 2024.
9. Марков А.С., Цирлов В.Л., Барабанов А.В. Методы оценки уязвимостей программного обеспечения // Труды ИСП РАН. 2018. Т. 30, № 6. С. 97–110.
10. Le T.H.M., Babar M.A., Thai T.H. Software Vulnerability Prediction in Low-Resource Languages: An Empirical Study of CodeBERT and ChatGPT. arXiv:2404.17110, 2024.
11. Костин Д.В., Фролов А.В. Автоматизированный анализ защищенности программных систем // Информационная безопасность. 2019. Т. 22, № 4. С. 35–42.
12. Keller J., Nowakowski J. AI-powered patching: the future of automated vulnerability fixes. Google Security Engineering Technical Report, 2024.
13. Hu Y. et al. SoK: Automated Vulnerability Repair – Methods, Tools, and Assessments. arXiv:2506.11697, 2025.

Zanin D.S.
Saint Petersburg Electrotechnical
University «LETI», Saint-Petersburg

Scientific supervisor:
Petrenko S.A.
Sirius University of Science and Technology, Sochi

A MODEL OF INTELLIGENT SEMANTIC SECURITY FOR DISTRIBUTED SOFTWARE SYSTEMS AND ITS EFFECTIVENESS EVALUATION BY SYSTEM PROPERTIES

Abstract. An integral model of intelligent semantic security for distributed systems is proposed, based on dual state representation: formal (dimensionless similarity invariants) and semantic (vector embeddings). The model includes hybrid detection, incident memory, cognitive analysis via RAG/LLM, and adaptive response. A six-stage method for applying the model is described. Effectiveness is evaluated by three system properties: detection quality, analysis timeliness, and response efficiency.

Keywords: semantic security, distributed systems, similarity invariants, embeddings, hybrid detection, RAG, LLM, adaptive response.

УДК 004.056:629.3

Занин Н.С.
Санкт-Петербургский государственный электротехнический
университет «ЛЭТИ» им. В.И. Ульянова (Ленина), Санкт-Петербург

Научный руководитель:
Петренко С.А.
Научно-технологический университет «Сириус», Сочи

ФОРМАЛЬНАЯ МОДЕЛЬ РАСПРЕДЕЛЕННОГО КИБЕРИММУНИТЕТА ECU-ПРИЛОЖЕНИЙ В AUTOSAR ADAPTIVE

Аннотация. Современные системы управления транспортными средствами на платформе AUTOSAR Adaptive не имеют формализованной распределенной процедуры восстановления после кибератак. Предложена модель ImmuneAUTOSAR с клеточным восстановлением, задаваемая отображением $F:X\times A\to Y$, клеточной матрицей $M(t)$ и локальными правилами перехода. Сформулированы шесть теоретических положений о полноте, детерминированности,

разрешимости восстановления, каскадных отказах, эффективности и пороговом эффекте покрытия. Экспериментально определен рациональный диапазон покрытия 0.6–0.8.

Ключевые слова: AUTOSAR Adaptive, киберустойчивость, клеточные автоматы, формальная модель, иммунная защита, восстановление ECU.

Современные электронные архитектуры автомобилей эволюционируют в сторону программно-определяемого транспортного средства (Software-Defined Vehicle) на базе платформы AUTOSAR Adaptive [2]. Эта платформа поддерживает контейнеризацию приложений, динамическое управление жизненным циклом и сервис-ориентированное взаимодействие. Однако штатные механизмы Execution Management и Health Monitoring фиксируют отказы, но не обладают формализованной распределенной процедурой восстановления после кибератак [1]. Компрометация отдельных ECU-узлов способна приводить к каскадному распространению нарушений и переходу системы в катастрофические состояния.

В работе предложена и формализована модель ImmuneAUTOSAR с клеточным восстановлением, в которой иммунный ответ и восстановление реализуются распределенно на основе клеточно-автоматной динамики [3] и управляющего компонента Recovery Core. Модель MIA задается отображением

$$F: X \times A \to Y,$$

где X – пространство состояний распределенной системы управления ТС, A – множество атакующих воздействий, Y – пространство показателей устойчивости.

Иммунное состояние системы кодируется клеточной матрицей $M(t)=\{m_{ij}(t)\}$, эволюционирующей по локальной функции переходов:

$$m_{ij}(t+1)=\varphi(m_{ij}(t),N_{ij}(t),X_i(t),S_{ij}(t),\theta_i(t),\Delta_i(t)),$$

где $N_{ij}(t)$ – окрестность клетки (соседние ECU), $S_{ij}(t)$ – наблюдаемые признаки аномалий, $\theta_i(t)$ – порог срабатывания реакции, $\Delta_i(t)$ – параметр адаптации порогов. Коэффициент клеточного покрытия $k_{\text{покр}} \in [0,1]$ отражает долю узлов и связей, охваченных клеточными агентами и механизмами иммунного наблюдения.

Архитектура ImmuneAUTOSAR включает следующие компоненты: CellController – обертка ECU-компонента для сбора сигналов и интеграции с клеточным движком; CA Engine – локальные функции переходов клеток; CA Observer – локальный наблюдатель иммунной реакции; Recovery Core – перезапуск, откат и самоизоляция компонентов;

CA Supervisor – агрегирование показателей устойчивости и управление параметрами покрытия и порогов.

Вектор показателей устойчивости Y включает: W_{min} – минимальную устойчивость уровня/кластера; $T_{\text{восст}}$ – время полного восстановления; $P_{\text{обн}}$ – вероятность обнаружения атаки/аномалии; $P_{\text{восст}}$ – вероятность успешного восстановления; $R_{\text{уст}}$ – интегральный показатель устойчивости. Требования устойчивости задаются неравенствами

$$W_{min} \geq W_{\text{треб}}, T_{\text{восст}} \leq T_{\text{доп}}.$$

Теоретическое исследование модели опирается на шесть утверждений.

Утверждение 1 (полнота модели). Модель MIA полна относительно класса распределенных автомобильных систем: для любой архитектуры СУ ТС, представимой как сеть взаимодействующих ECU, существует конфигурация клеточных автоматов, изоморфно моделирующая исходную систему.

Утверждение 2 (детерминированность иммунного ответа). Идентичные атаки на идентичные состояния приводят к одинаковым траекториям эволюции $M(t)$ и одинаковым значениям показателей устойчивости.

Утверждение 3 (разрешимость восстановления). Для любой атаки существует конечная последовательность тактов, переводящая систему из начальной конфигурации в восстановленную при соблюдении ограничений на ресурсы.

Утверждение 4 (каскадные отказы). При одновременных атаках на k смежных ECU в кластере вероятность сохранения работоспособности уровня убывает экспоненциально:

$$P_{\text{раб}}(k) = P_0 \cdot e^{-\lambda k},$$

где P_0 – исходная надежность, λ – параметр уязвимости.

Утверждение 5 (эффективность покрытия по времени восстановления). Рост коэффициента клеточного покрытия $k_{\text{покр}}$ уменьшает среднее время восстановления по закону насыщения:

$$T_{\text{рем}}(k_{\text{покр}}) = T_{max} \cdot (1 - k_{\text{покр}})^{\gamma} + T_{min}, \gamma > 1.$$

Утверждение 6 (пороговый эффект). Существует критическое значение покрытия $k^{*}_{\text{покр}}$, зависящее от топологии сети, такое, что при $k_{\text{покр}} \geq k^{*}_{\text{покр}}$ выполняются требования по минимальной устойчивости и времени восстановления. Для типового случая

$$k^{*}_{\text{покр}}=1-\frac{1}{\langle d\rangle+1},$$

где $\langle d\rangle$ – средняя степень связности.

Экспериментальная верификация выполнена на имитационной модели сети из 24 ECU, организованных в 3 домена. Варьировался коэффициент покрытия $k_{\text{покр}}\in\{0.0;0.2;0.5;0.8;1.0\}$. При $k_{\text{покр}}=0$ восстановление не достигается. Рост покрытия повышает W_{min}, $P_{\text{обн}}$ и $P_{\text{восст}}$ и сокращает $T_{\text{восст}}$. При $k_{\text{покр}}>0.8$ прирост устойчивости замедляется при линейном росте накладных расходов. Рациональный диапазон покрытия — 0.6–0.8. Оптимальная конфигурация параметров: $k_{\text{покр}}=0.7$, $T_{\text{рес}}=3$, $\theta_{inf}=2$, обеспечивающая $W_{min}\approx0.75$ и $T_{\text{восст}}\approx12$ тактов.

Список использованных источников:

1. ISO/SAE 21434:2021. Road vehicles – Cybersecurity engineering. International Organization for Standardization, 2021.

2. AUTOSAR. Specification of Adaptive Platform. Release R21-11. AUTOSAR Consortium, 2021.

3. Wolfram S. Theory and Applications of Cellular Automata. World Scientific, 1986.

Zanin N.S.
Saint Petersburg Electrotechnical
University «LETI», Saint-Petersburg

Scientific supervisor:
Petrenko S.A.
Sirius University of Science and Technology, Sochi

FORMAL MODEL OF DISTRIBUTED CYBERIMMUNITY FOR ECU APPLICATIONS IN AUTOSAR ADAPTIVE

Abstract. Modern vehicle control systems based on AUTOSAR Adaptive lack a formalized distributed recovery procedure after cyberattacks. The ImmuneAUTOSAR model with cellular recovery is proposed, defined by the mapping $F:X\times A\to Y$, the cellular matrix $M(t)$ and local transition rules. Six theoretical statements are formulated concerning completeness, determinism, solvability of recovery, cascading failures, coverage efficiency and threshold effect. The rational coverage range of 0.6–0.8 is determined experimentally.

Keywords: AUTOSAR Adaptive, cyber resilience, cellular automata, formal model, immune defense, ECU recovery.

УДК 004.056:629.3

Занин Н.С.
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина), Санкт-Петербург

Научный руководитель:
Петренко С.А.
Научно-технологический университет «Сириус», Сочи

МЕТОД РАСПРЕДЕЛЕННОЙ ИММУННОЙ ЗАЩИТЫ ECU-ПРИЛОЖЕНИЙ В AUTOSAR ADAPTIVE НА ОСНОВЕ КЛЕТОЧНЫХ АВТОМАТОВ

Аннотация. Существующие механизмы Health Monitoring в AUTOSAR Adaptive не обеспечивают автономного распределенного восстановления после кибератак. Предложен метод иммунной защиты ImmuneAUTOSAR, реализующий децентрализованный иммунный ответ на основе клеточных автоматов. Доказаны теоремы о конечной сходимости восстановления и о необходимом и достаточном условии устойчивости уровня через коэффициент клеточного покрытия. Экспериментально подтверждена эффективность метода при покрытии 0.6–0.8.

Ключевые слова: AUTOSAR Adaptive, иммунная защита, клеточные автоматы, метод восстановления, распределенные системы, киберустойчивость.

Платформа AUTOSAR Adaptive, применяемая в современных программно-определяемых транспортных средствах, предоставляет механизмы Execution Management и Health Monitoring для обнаружения сбоев и перезапуска приложений [2]. Однако эти механизмы действуют локально, не координируют восстановление распределенных сервисов и не предотвращают повторное заражение от соседних узлов. При каскадном распространении компрометации время реакции растет с размером сети, а вероятность восстановления падает экспоненциально.

В работе предлагается метод ImmuneAUTOSAR, реализующий децентрализованный иммунный ответ на основе клеточных автоматов [3]. Каждый ECU оснащается локальным агентом CellController, который в дискретные такты времени обновляет свое состояние по правилу, зависящему от собственных метрик (загрузка CPU, память, ввод-вывод), состояний соседей и порогов чувствительности. Алфавит состояний включает N (норма), S (подозрение), I (заражение) и R (восстановление).

Архитектура метода включает следующие компоненты. CellController – обертка вокруг прикладного ECU-компонента, перехватывающая входные сигналы и собирающая метрики выполнения. CA Observer вычисляет аномальный скор на основе накопленной истории. CA Engine хранит клеточную матрицу $M(t)$ в децентрализованном виде и применяет функцию перехода φ. Recovery Core при переходе в состояние R инициирует перезапуск (restart), откат (rollback) или изоляцию (isolate) через штатные интерфейсы AUTOSAR. CA Supervisor периодически корректирует коэффициент покрытия k_{cov} и пороги.

Локальное правило перехода φ задается следующими условиями. Из N в S: если локальная аномалия или доля соседей в I превышает порог θ_{inf}. Из S в I: если состояние подозрения сохраняется T_{conf} тактов или появился сосед в I. Из I в R: немедленный запуск восстановления. Из R в N: после T_{rec} тактов при успешной проверке работоспособности. Параметры T_{conf}=2, T_{rec}=3, θ_{inf}=0.5 используются в базовой конфигурации.

Доказаны две теоремы.

Теорема 1 (конечная сходимость). Пусть в сети ECU, каждый из которых выполняет алгоритм ImmuneAUTOSAR, произошло единичное нарушение. Тогда процесс восстановления завершится за конечное число тактов K, причем

$$K \le T_{conf} + T_{rec} + D,$$

где D – диаметр графа сети. Доказательство основано на том, что волна заражения распространяется со скоростью не более одного ребра за T_{conf}+1 тактов, а каждый зараженный узел восстанавливается за T_{rec} тактов.

Теорема 2 (необходимое и достаточное условие устойчивости уровня). Для выполнения требований по времени восстановления и минимальной устойчивости необходимо и достаточно, чтобы коэффициент клеточного покрытия удовлетворял

$$k_{cov} \ge 1 - \frac{1}{\langle d \rangle + 1},$$

где $\langle d \rangle$ – средняя степень связности графа ECU. Иными словами, иммунные агенты должны образовывать вершинное покрытие графа. При нарушении этого условия существует атака, приводящая к бесконечному времени восстановления; при его выполнении каждый зараженный узел имеет иммунного соседа, что гарантирует локализацию атаки.

Экспериментальная верификация проведена на имитационной модели сети из 24 ECU с топологией «каждый с каждым» внутри трех

доменов ($\langle d \rangle$=4.2). При параметрах T_{conf}=2, T_{rec}=3, θ_{inf}=0.5 варьировался коэффициент покрытия $k_{cov} \in \{0.0;0.2;0.5;0.7;0.8;0.9;1.0\}$. Результаты представлены в таблице 1.

Таблица 1

Зависимость показателей устойчивости от коэффициента покрытия

k_{cov}	T_{rec}, такты	W_{min}	P_{det}	P_{rec}	CPU overhead, %
0.0	∞	0.12	0.0	0.0	0
0.2	48 ± 6	0.31	0.34	0.28	5
0.5	22 ± 4	0.68	0.85	0.88	11
0.7	12 ± 2	0.85	0.94	0.96	14
0.8	10 ± 2	0.91	0.97	0.98	16
1.0	9 ± 1	0.95	1.0	1.0	18

При k_{cov}=0 (отсутствие иммунной защиты) система не восстанавливается. При k_{cov}=0.7 время восстановления составляет 12 тактов, вероятность обнаружения атаки – 0.94, вероятность успешного восстановления – 0.96, накладные расходы CPU – 14%. Оптимальный диапазон покрытия – 0.6-0.8. Дальнейшее увеличение покрытия дает незначительный выигрыш по времени (с 12 до 9 тактов) при линейном росте накладных расходов.

Сравнение с базовыми методами (таблица 2) показывает существенное превосходство ImmuneAUTOSAR. Health Monitoring не обеспечивает восстановления ($T_{rec} \to \infty$). Централизованный IDS с ручным восстановлением имеет T_{rec}>100 тактов и P_{rec}=0.3. ImmuneAUTOSAR при k_{cov}=0.7 обеспечивает T_{rec}=12 тактов и P_{rec}=0.96, работая автономно и распределенно.

Таблица 2

Сравнение ImmuneAUTOSAR с базовыми методами

Метод	T_{rec}, такты	P_{rec}	Автономность	Распределенность	CPU, %
Health Monitoring	∞	0.0	нет	нет	3
Централизованный IDS	>100	0.3	нет	нет	8
ImmuneAUTOSAR (k_{cov}=0.7)	12	0.96	да	да	14

Предложенный метод отличается от известных аналогов децентрализацией, формальными гарантиями сходимости и

адаптивностью [1, 3]. Ограничения метода включают зависимость от точности локального обнаружения аномалий, необходимость модификации ПО ECU и дополнительные накладные расходы 10–15% CPU, что приемлемо для современных многоядерных контроллеров.

Список использованных источников:

1. ISO/SAE 21434:2021. Road vehicles — Cybersecurity engineering. International Organization for Standardization, 2021.

2. AUTOSAR. Specification of Adaptive Platform. Release R21-11. AUTOSAR Consortium, 2021.

3. Wolfram S. Theory and Applications of Cellular Automata. World Scientific, 1986.

4. Forrest S., Hofmeyr S.A., Somayaji A. Computer immunology. Communications of the ACM, 1997, vol. 40, no. 10, pp. 88–96.

Zanin N.S.
Saint Petersburg Electrotechnical
University «LETI», Saint-Petersburg

Scientific supervisor:
Petrenko S.A.
Sirius University of Science and Technology, Sochi

METHOD OF DISTRIBUTED IMMUNE DEFENSE FOR ECU APPLICATIONS IN AUTOSAR ADAPTIVE BASED ON CELLULAR AUTOMATA

Abstract. Existing Health Monitoring mechanisms in AUTOSAR Adaptive do not provide autonomous distributed recovery after cyberattacks. The ImmuneAUTOSAR method is proposed, implementing a decentralized immune response based on cellular automata. Theorems on finite convergence of recovery and on necessary and sufficient condition for level stability through the cellular coverage coefficient are proved. The effectiveness of the method is experimentally confirmed at coverage of 0.6–0.8.

Keywords: AUTOSAR Adaptive, immune defense, cellular automata, recovery method, distributed systems, cyber resilience.

УДК 004.056:004.89

Крыжановский А.Д.
Омский государственный технический университет, Омск

Научный руководитель:
Данилова О.Т.
Омский государственный технический университет, Омск

РАЗРАБОТКА ИНСТРУМЕНТА ДЛЯ ИНТЕЛЛЕКТУАЛЬНОГО АНАЛИЗА СЕТЕВОГО ТРАФИКА

Аннотация. В представленной статье представлено программное обеспечение для интеллектуального анализа сетевого трафика, сочетающего в себе методы сигнатурного, поведенческого и эвристического обнаружения сетевых атак и аномалий. Практическая значимость работы заключается в создании функционирующего программного обеспечения с открытой модульной архитектурой. Разработанный инструмент может применяться для оперативного мониторинга безопасности в локальных сетях, а также использоваться в учебном процессе при проведении лабораторных практикумов по дисциплинам, связанным с защитой информации и сетевой безопасностью.

Ключевые слова: сетевой анализатор, интеллектуальный анализ, машинное обучение, обнаружение аномалий, расследование инцидентов.

Введение

Сетевая инфраструктура постоянно подвергается эволюционирующим киберугрозам [1]. Традиционные средства защиты сталкиваются с трудностями при выявлении атак, использующих шифрование, обфускацию и легитимные каналы связи для сокрытия вредоносной активности [2]. Стремительно растет доля целевых атак и угроз нулевого дня, против которых классические подходы оказываются малоэффективными [3].

Анализ существующих программных средств показывает, что универсальные анализаторы ориентированы преимущественно на ручной анализ, а классические системы обнаружения, в основном, на сигнатурный подход [4]. Формируется необходимость разработки инструмента, объединяющего различные подходы анализа в рамках единой системы.

Целью работы является разработка программного инструмента для интеллектуального анализа сетевого трафика.

Для достижения цели решаются следующие задачи:

1. разработка модульной архитектуры системы;
2. реализация подсистемы захвата и обработки трафика;
3. интеграция модулей, включающих различные методы для анализа;
4. проектирование подсистемы агрегации событий и графического интерфейса пользователя
5. проведение экспериментальной апробации инструмента.

Решение сформулированного комплекса задач позволит создать эффективный инструмент, снижающий когнитивную нагрузку на специалиста и повышающий оперативность расследования инцидентов информационной безопасности.

Теория

Вычислительное ядро программы реализует строгий конвейер последовательного преобразования данных и представляется как совокупность функциональных компонентов, обеспечивающих последовательное преобразование данных:

$$S = \langle C, E, A, R \rangle, \quad (1)$$

где *C* (*Capture*) – подсистема захвата и первичной предфильтрации трафика; *E* (*Extraction*) – подсистема извлечения признаков и нормализации; *A* (*Analysis*) – композитный аналитический модуль, объединяющий детерминированные и вероятностные методы детектирования; *R* (*Reporting*) – подсистема агрегации сигналов тревоги и реагирования.

Входом системы является непрерывный поток сетевых пакетов *P*, поступающих от сетевого интерфейса в режиме реального времени (*Live*-трафик) или из файлов дампа формата *PCAP*. На этапе *C* выполняется применение *BPF*-фильтров (*Berkeley Packet Filter*) для отсеивания легитимного фонового шума. Каждому пакету p_k , прошедшему предфильтрацию, присваивается уникальный внутренний идентификатор id_k и точная временная метка t_k, формируя унифицированную структуру данных: $p'_k = \langle p_k, id_k, t_k \rangle$.

Далее управление передается подсистеме *E*, которая преобразует пакет в структурированный вектор признаков. Ключевой метрикой в векторе f_k выступает энтропия Шеннона $H(d_k)$, вычисляемая для полезной нагрузки пакета. Данный математический аппарат позволяет оценить степень случайности распределения байтов и дифференцировать открытый текстовый трафик от зашифрованных вредоносных туннелей без необходимости наличия криптографических ключей [5]. Вычисление производится по формуле:

$$H(d_k) = -\sum_{j=0}^{255} P(b_j) \log_2 P(b_j), \quad (2)$$

где $P(b_j)$ – частотная вероятность появления байта со значением j в анализируемом массиве данных d_k [5].

Сформированный вектор x_k асинхронно передается в аналитическую подсистему A, где реализуется глобальная функция детектирования $D_k \in \{0,1\}$. Решение о классификации пакета как вредоносного формируется на основе логической дизъюнкции результатов работы сигнатурного, поведенческого и *ML* анализаторов:

$$D_k = A_{sig}(x_k) \vee A_{heur}(x_k) \vee A_{behav}(W_k), \quad (3)$$

где поведенческий анализ A_{behav} оперирует накопленным за определенный период времени, контекстным окном (сессией) векторов $W_k = (x_{k-w}, \dots, x_k)$, что позволяет выявлять аномалии в динамике трафика.

Результаты разработки

Апробация разработанного инструмента проводилась на реальных дампах сетевого трафика, содержащих как легитимную активность, так и вредоносные сценарии.

В ходе анализа трафика, содержащего активность вредоносного программного обеспечения *STRRAT* (рис. 1), инструмент позволил выявить регулярные сетевые соединения, характерные для взаимодействия с командно-управляющим сервером. Поведенческий анализ показал устойчивую периодичность соединений, что позволило идентифицировать *C2-beaconing*.

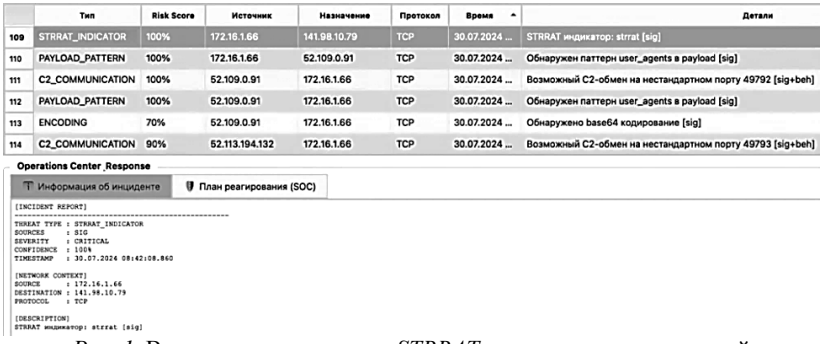


Рис. 1. Выявленная активность *STRRAT* и регулярных соединений

При анализе сетевого трафика, содержащего передачу исполняемого файла (*PE*), были зафиксированы повышенные значения энтропии полезной нагрузки, что позволило выявить передачу бинарных данных (рис. 2), нехарактерных для обычного пользовательского трафика.

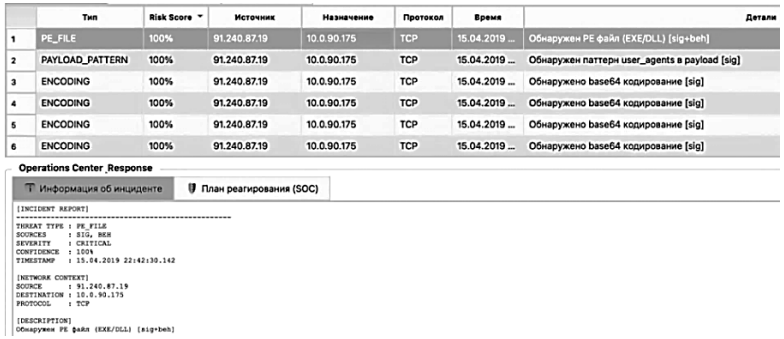


Рис. 2. Выявленная угроза передачи исполняемого файла

Результаты анализа представляются в графическом интерфейсе в виде алертов, содержащих информацию о типе угрозы и параметрах сетевого взаимодействия. Автоматическая агрегация результатов различных методов анализа позволяет сократить время расследования инцидентов по сравнению с использованием универсальных анализаторов.

Заключение

В рамках работы разработан программный инструмент для интеллектуального анализа сетевого трафика, объединяющий сигнатурный и поведенческий методы, а также применяющий *ML*-анализ, для обнаружения угроз. Предложенная архитектура позволяет автоматизировать процесс выявления аномальной активности и снизить нагрузку на специалиста при анализе сетевого трафика. Проведенная апробация на реальных данных показала успешные результаты. Полученные результаты подтверждают целесообразность выбранного подхода и демонстрируют перспективы дальнейшего развития программного средства.

Список использованных источников:

1. ENISA Threat Landscape 2024 [Электронный ресурс] // European Union Agency for Cybersecurity. – 2024. – URL: https://www.enisa.europa.eu/ (дата обращения: 18.03.2026).

2. Khraisat, A. Survey of intrusion detection systems: techniques, datasets and challenges / A. Khraisat, I. Gondal, P. Vamplew [et al.] // Cybersecurity. – 2019. – Vol. 2, No. 20. – DOI: 10.1186/s42400-019-0038-7.

3. Zhang, Y. Anteater: Advanced Persistent Threat Detection With Program Network Traffic Behavior / Y. Zhang [et al.] // IEEE Access. – 2024. – Vol. 12. – P. 8537-8549. – DOI: 10.1109/ACCESS.2024.3352018.

4. Фомин С. В., Дьяконов А. В. Методы расследования инцидентов информационной безопасности. – М.: Горячая линия – Телеком, 2021. – 256 с.

5. Anderson, B. Identifying Encrypted Malware Traffic with Contextual Flow Data / B. Anderson, D. McGrew // Proceedings of the 2016 ACM Workshop on Artificial Intelligence and Security (AISec '16). – 2016. – P. 11-22.

Kryzhanovsky A.D.
Omsk State Technical University, Omsk

Scientific supervisor:
Danilova O.T.
Omsk State Technical University, Omsk

DEVELOPMENT OF A TOOL FOR INTELLIGENT NETWORK TRAFFIC ANALYSIS

Abstract. The article presents software for intelligent network traffic analysis that combines signature-based, behavioral, and heuristic methods for detecting network attacks and anomalies. The practical significance of the work lies in the development of functional software with an open modular architecture. The developed tool can be applied for real-time security monitoring in local area networks, as well as utilized in the educational process for laboratory workshops in disciplines related to information security and network safety.

Keywords: network analyzer, intelligent analysis, machine learning, anomaly detection, incident investigation.

УДК 004.056.2:519.246.8

Лаптев Т.О., Рыцева К.В.
Уфимский университет науки и технологий, Уфа

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

МОДЕЛИРОВАНИЕ И ИДЕНТИФИКАЦИЯ ПАРАМЕТРОВ ПРОЦЕССА АВТОРЕГРЕССИИ ПЕРВОГО ПОРЯДКА ПРИ НАЛИЧИИ ШУМА ИЗМЕРЕНИЙ ДЛЯ ЗАДАЧ ОБНАРУЖЕНИЯ АНОМАЛИЙ СЕТЕВОГО ТРАФИКА

Аннотация. В данной работе рассматривается применение авторегрессионных моделей первого порядка для анализа сетевых атак при условии зашумленных данных. Показано, что классический метод

наименьших квадратов дает смещенные оценки параметров при наличии шума, что часто встречается в системах сбора данных о кибератаках. Предложен метод инструментальных переменных, позволяющий получать состоятельные оценки. Приведены математические модели, результаты экспериментальной части реализованы на языке Python и показана эффективность метода для преждевременного обнаружения DDoS-атак.

Ключевые слова: математическое моделирование, прогноз, сетевой трафик, авторегрессия, DDoS, Python.

Прогнозирование сетевых атак с помощью статистических методов – это ключевая техника в информационной безопасности. Статические методы, в отличие от динамических, не требуют анализа поведения системы в реальном времени. Вместо этого они основаны на предварительном анализе данных, которые не изменяются во времени, и использовании различных алгоритмов для быстрого выявления атак и угроз.

Современные киберугрозы обладают выраженной временной динамико, что делает метод анализа временных рядов, в частности авторегрессионные модели, мощным инструментом для прогнозирования атак, выявления аномальной активности в сетевом трафике и эффективного использования ресурсов для устранения атаки [1].

Особенностью данных о сетевых атаках является наличие шума измерений, связанного с погрешностями сенсоров, задержками при передаче пакетов данных и активностью правомерных пользователей. Поэтому требуется разработка специальных методов идентификации параметров моделей, устойчивых к шуму.

Вопрос выбора метода идентификации зависит от характера анализируемых данных и уровня шума. В данной работе рассматривается авторегрессионная модель первого порядка (AR(1)), которая задается уравнением [2]:

$$x_t = \varphi x_{t-1} + \varepsilon_t, |\varphi| < 1$$

где x_t– истинное значение уровня угрозы в момент времени t; φ – параметр авторегрессии; ε_t – белый шум процесса с дисперсией σ_ε^2.

Заметим, что система мониторинга фиксирует зашумленные наблюдения:

$$y_t = x_t + \eta_t$$

где η_t– белый шум измерений с дисперсией σ_η^2независимый от ε_t.

Таким образом, задача заключается в оценке параметра φ по зашумленным наблюдениям y_t .

Далее мною было рассмотрено два метода идентификации с помощью языка программирования Python, с целью изучения возможных

атак. Исходные данные были сгенерированы с известными параметрами: $\varphi = 0.95$,$\sigma_\varepsilon = 0.5$, $\sigma_\eta = 1.5$.

В данном случае присутствует значительный шум измерений, поэтому классический метод наименьших квадратов дает смещенные оценки. Это явление называется эффектом разбавления.

Математическая форма оценки параметра методом наименьших квадратов (МНК) имеет вид:

$$\hat{\varphi} = \frac{\sum_{t=2}^{n} y_t y_{t-1}}{\sum_{t=2}^{n} y_{t-1}^2}$$

В пределе:

$$\hat{\varphi} \to \varphi \cdot \frac{\sigma_x^2}{\sigma_x^2 + \sigma_\eta^2}$$

Для устранения смещения будем применять метод инструментальных переменных (IV). Оценка IV вычисляется по формуле:

$$\tilde{\varphi} = \frac{\sum_{t=3}^{n} (y_t - \bar{y})(y_{t-2} - \bar{y})}{\sum_{t=3}^{n} (y_{t-1} - \bar{y})(y_{t-2} - \bar{y})}$$

Данный подход позволяет получить состоятельный оценку на φ.

Далее в работе проведено 100 экспериментов. Результаты представлены в таблице 1.

Таблица 1

Результаты проведенных вычислений

Метод	Средняя оценка	Относительная ошибка
Истинное значение	0.95	0%
МКН	0.624	34.3%
Инструментальные переменные	0.939	1.1%

На рисунке 1 представлено сравнение чистого процесса xt и зашумленных наблюдений yt.

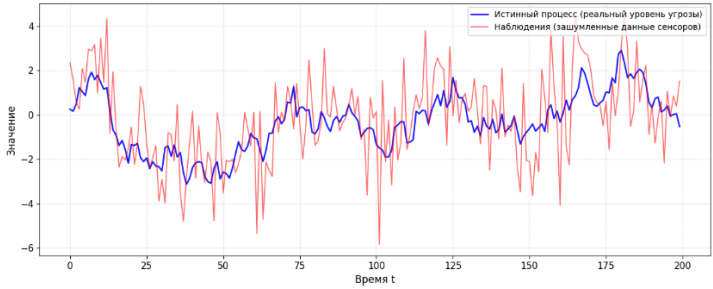


Рис. 1. Сравнение чистого процесса и зашумленных наблюдений

Как видно из таблицы 1, классический МНК дает ошибку 34,3%, а метод инструментальных переменных – менее 2%. Это подтверждает теоретические выкладки о смещении МНК при наличии шума измерений.

Далее для моделирования атаки использовалось скользящее окно шириной 50 наблюдений. В каждый раз вычислялась оценка $\tilde{\varphi}$. Поэтому рост параметра свидетельствует об аномалии. Результаты эксперимента по обнаружению атаки представлены в таблице 2.

Таблица 2

Результаты эксперимента

Метод	Время обнаружения t	Опережение
Пороговый метод	520	-
Метод AR(1)	485	35 тактов

Пороговый метод обнаружил атаку при t=520. Метод AR(1) обнаружил аномалию при t=485. Таким образом, предложенный метод позволяет обнаружить атаку на 35 временных тактов раньше.

В работе рассмотрена задача идентификации параметров AR(1) при наличии шума измерений. Показано, что классический МНК дает смещенные оценки. Далее был предложен метод инструментальных переменных, позволяющий получать точные оценки и проведены эксперименты, подтверждающие эффективность метода для раннего обнаружения DDoS-атак.

В качестве перспективы можно выделить разработку гибридных систем, учитывающих тренд аномалии и внешние факторы.

Список использованных источников:

1. Корнилова А.А., Гиззатова Э.Р. Математическое моделирование временного ряда количества скомпрометированных персональных данных в мире // Информационные технологии обеспечения комплексной безопасности в цифровом обществе: материалы VIII Всероссийской молодежной научно-практической конференции с международным участием (г. Уфа, 23–24 мая 2025 г.). – Уфа: Уфимский университет, 2025. – С. 22-25.

2. Hamilton J.D. Time Series Analysis. – Princeton, N.J.: Princeton University Press, 1994. – С. 19

Laptev T.O., Rytseva K.V.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Kornilova A.A.
Ufa University of Science and Technology, Ufa

MODELING AND PARAMETER IDENTIFICATION OF THE FIRST-ORDER AUTOREGRESSIVE PROCESS IN THE PRESENCE OF MEASUREMENT NOISE FOR NETWORK TRAFFIC ANOMALY DETECTION PROBLEMS

Abstract. This paper considers the application of first-order autoregressive models for the analysis of network attacks under noisy data conditions. It is shown that the classical least squares method yields biased parameter estimates in the presence of noise, which is common in cyberattack data collection systems. An instrumental variables method is proposed to obtain consistent estimates. Mathematical models are presented, the experimental results are implemented in Python, and the effectiveness of the method for the early detection of DDoS attacks is demonstrated.

Keywords: mathematical modeling, forecasting, network traffic, autoregression, DDoS, Python.

УДК 004.056

Неборачек К.А., Диканский Д.А.
Северо-Кавказский федеральный университет, Ставрополь

Научный руководитель:
Тебуева Ф.Б.
Северо-Кавказский федеральный университет, Ставрополь

МЕТОД ПРОГНОЗИРОВАНИЯ ОТКАЗОВ МЕЖАГЕНТНОЙ КОММУНИКАЦИИ ДЛЯ УСТОЙЧИВОЙ КООРДИНАЦИИ В ДЕЦЕНТРАЛИЗОВАННЫХ КИБЕРФИЗИЧЕСКИХ СИСТЕМАХ

Аннотация. Рассматривается задача прогнозирования отказов межагентной коммуникации в децентрализованных киберфизических системах. Предложен метод, позволяющий заранее выявлять деградацию каналов связи и адаптивно перестраивать схему координации. Новизна работы состоит в объединении оценки надежности канала, динамики потерь и задержек сообщений с переключением между коллективным,

гибридным и локальным режимами управления. Эксперименты показали рост устойчивости координации по сравнению с методом-аналогом.

Ключевые слова: киберфизические системы, мультиагентные системы, коммуникации, отказ связи, координация, обучение с подкреплением, прогнозирование, устойчивость.

Децентрализованные киберфизические системы широко применяются в распределенных IoT-сетях, группах беспилотных летательных аппаратов, робототехнических комплексах и интеллектуальных системах мониторинга. Эффективность их работы определяется не только качеством локальных алгоритмов, но и устойчивостью межагентного взаимодействия. При этом надежность коммуникаций становится одним из основных факторов сохранения согласованного коллективного поведения. Целью настоящей работы является разработка метода прогнозирования отказов межагентной коммуникации для устойчивой координации в децентрализованных киберфизических системах.

Современные исследования в области мультиагентных систем подтверждают высокую эффективность обучения с подкреплением для кооперативного управления в распределенной среде [1, 2]. Однако большинство таких методов ориентировано на устойчивую координацию при относительно стабильных условиях взаимодействия. Вопросы безопасности мультиагентных киберфизических систем и устойчивости межагентного обмена рассмотрены в обзорных работах [3, 4], где подчеркивается значимость надежных коммуникаций для распределенных систем управления.

В работах, посвященных доверительному консенсусу и обмену рекомендациями между агентами [5, 6], предлагаются механизмы фильтрации входящих сообщений и повышения устойчивости координации. Вместе с тем они ориентированы в основном на проверку достоверности отдельных сообщений, а не на прогнозирование деградации канала связи. Отдельные исследования рассматривают доверенные взаимодействия в децентрализованных средах [7, 8], однако не предлагают механизма раннего выявления коммуникационных отказов и адаптивного переключения режимов оркестрации.

Таким образом, существующие подходы либо фокусируются на общей координации, либо решают задачу доверительной фильтрации сообщений, не обеспечивая прогнозирование нарушения связи. Это определяет актуальность разработки метода, позволяющего заранее выявлять деградацию межагентной коммуникации и перестраивать схему взаимодействия до наступления критического сбоя.

В качестве метода-аналога рассматривается подход доверительной фильтрации межагентных сообщений, при котором участник системы оценивает входящую рекомендацию на основе локального контекста и истории взаимодействия [6]. Каждый модуль получает локальное состояние среды, формирует действие с помощью функции ценности и, при необходимости, передает рекомендацию соседнему участнику. Получатель принимает или отклоняет сообщение в зависимости от вычисленного коэффициента доверия.

Достоинством метода-аналога является снижение влияния заведомо недостоверных сообщений и повышение согласованности коллективной стратегии. Однако данный подход реагирует только на уже поступившие сообщения и не учитывает возможность предварительного прогнозирования отказа коммуникационного канала.

Предлагаемый метод предназначен для прогнозирования отказов межагентной коммуникации и адаптивного поддержания устойчивой координации. В его основе лежит идея раннего выявления деградации канала по наблюдаемым параметрам связи: доле потерь сообщений, задержке передачи, нестабильности доставки и динамике ошибок обмена.

Для каждого канала связи между модулями рассчитывается интегральный показатель риска отказа:

$$R_{ij} = aP_{ij} + \beta D_{ij} + \gamma L_{ij},$$

где P_{ij} – доля потерь сообщений, D_{ij} – нормированная задержка передачи, L_{ij} – показатель нестабильности канала, α, β, γ – весовые коэффициенты, $\alpha + \beta + \gamma = 1$.

Если значение превышает R_{ij} заданный порог, система рассматривает канал как потенциально отказоустойчиво-небезопасный и заранее изменяет схему координации. При умеренном значении риска используется гибридный режим, в котором сохраняется взаимодействие только по устойчивым направлениям. При высоком риске модуль временно переходит к локальному режиму принятия решений. Формально выбор режима описывается следующим правилом:

$$Mode_i = \begin{cases} Coord, R_{ij} < \tau_i, \\ Hybrid, \tau_1 \le R_{ij} < \tau_2, \\ Local, R_{ij} \ge \tau_2 \end{cases}$$

где $Coord$ – коллективный режим, $Hybrid$ – гибридный режим, $Local$ – локальный режим.

Экспериментальная среда моделировала децентрализованную архитектуру из пяти интеллектуальных модулей, взаимодействующих через каналы межагентной коммуникации. Каждый модуль выполнял функции локального мониторинга, оценки качества связи и выбора действия в зависимости от текущего режима координации.

Рассматривались следующие сценарии: штатная координация, рост задержки передачи, частичная потеря связи, массовая деградация каналов и масштабирование среды. Для оценки качества использовались метрики точности координации, устойчивости оркестрации, числа ошибочных коллективных действий и устойчивости к нарушению связи.

Таблица 1

Сравнение метрик эффективности метода-аналога и предлагаемого метода

Метрики эффективности	Метод-аналог	Предлагаемый метод	Улучшения%
Точность координации	0,80	0,87	+8,8
Устойчивость оркестрации	0,55	0,90	+63,6
Ошибочные коллективные действия	0,27	0,11	-59,3
Устойчивость к нарушению связи	0,48	0,82	+70,8

Данные таблицы 1 показывают, что предложенный метод обеспечивает наибольший прирост по показателям устойчивости оркестрации и устойчивости к нарушению связи. Это связано с тем, что прогнозирование отказов позволяет заранее перестраивать взаимодействие между участниками.

В результате проведенного исследования установлено, что прогнозирование отказов межагентной коммуникации является важным условием устойчивой координации в децентрализованных киберфизических системах. В работе предложен метод, основанный на оценке риска деградации канала и адаптивном переключении режимов оркестрации. Экспериментальные результаты показали рост устойчивости координации и снижение числа ошибочных коллективных действий по сравнению с методом-аналогом. Практическая значимость работы заключается в возможности применения метода в системах управления группами БПЛА, распределенных IoT-сетях и интеллектуальных системах коллективного мониторинга.

Список использованных источников:

1. Albrecht S.V., Christianos F., Schäfer L. Multi-Agent Reinforcement Learning: Foundations and Modern Approaches. Cambridge: MIT Press, 2024.

2. Feng P., Liang J., Wang S. et al. Hierarchical Consensus-Based Multi-Agent Reinforcement Learning for Multi-Robot Cooperation Tasks // arXiv preprint. 2024. DOI: 10.48550/arXiv.2407.08164.

3. Owoputi R., Chhetri S.R., Canedo A., Ray S. Security of Multi-Agent Cyber-Physical Systems: A Survey // IEEE Access. 2022. Vol. 10. Pp. 121465–121479. DOI: 10.1109/ACCESS.2022.3223362.

4. Zhu C., Dastani M., Wang S. A Survey of Multi-Agent Deep Reinforcement Learning with Communication // Autonomous Agents and Multi-Agent Systems. 2024. Vol. 38. Art. 4. DOI: 10.1007/s10458-023-09633-6.

5. Fung H.L., Darvariu V.-A., Hailes S., Musolesi M. Trust-based Consensus in Multi-Agent Reinforcement Learning Systems // Reinforcement Learning Journal. 2024. Vol. 2. Pp. 714–732. DOI: 10.48550/arXiv.2205.12880.

6. Guo Y., Campbell J., Stepputtis S. et al. Explainable Action Advising for Multi-Agent Reinforcement Learning // Proceedings of the IEEE International Conference on Robotics and Automation (ICRA). 2023. Pp. 1–8. DOI: 10.48550/arXiv.2211.07882.

7. Петренко В.И., Тебуева Ф.Б., Стручков И.В., Павлов А.С., Рябцев С.С. Метод доверенного взаимодействия агентов в децентрализованной киберфизической среде на основе технологии распределенного реестра // Прикаспийский журнал: управление и высокие технологии. 2023. № 3 (63). С. 115–125.

8. Стручков И.В. Метод оценки доверия к агентам при их взаимодействии в децентрализованной киберфизической среде // Вестник СПбГУТД. Серия 1. 2023. № 4. С. 86–90. DOI: 10.46418/2079-8199_2023_4_16.

Neborachek K.A., Dikanskiy D.A.
North-Caucasus Federal University, Stavropol

Scientific supervisor:
Tebueva F.B.
North-Caucasus Federal University, Stavropol

METHOD FOR PREDICTING INTER-AGENT COMMUNICATION FAILURES FOR RESILIENT COORDINATION IN DECENTRALIZED CYBER-PHYSICAL SYSTEMS

Abstract. The paper addresses the problem of predicting inter-agent communication failures in decentralized cyber-physical systems. A method is proposed that enables early detection of communication channel degradation and adaptively restructures the coordination scheme. The novelty of the work lies in combining communication reliability assessment, dynamics of message losses and delays, with switching between collective, hybrid, and local control modes. Experiments demonstrate an increase in coordination resilience compared to a baseline method.

Keywords: cyber-physical systems, multi-agent systems, communications, communication failure, coordination, reinforcement learning, prediction, resilience.

УДК 004.056

Ожгибесова А.С.
Пермский национальный исследовательский политехнический университет, Пермь

Научный руководитель:
Южаков А.А.
Пермский национальный исследовательский политехнический университет, Пермь

МЕТОД ОЦЕНКИ ЖИВУЧЕСТИ ИНФОРМАЦИОННЫХ СИСТЕМ НА ОСНОВЕ НЕЧЕТКИХ КОГНИТИВНЫХ КАРТ

Аннотация. Рассмотрена задача оценки киберживучести информационных систем. Продемонстрировано, что нечеткие когнитивные карты являются эффективным инструментом для ее решения. Предложена модель для анализа киберживучести информационных систем, выявления наиболее уязвимых компонентов системы и определения эффективных мер повышения киберживучести. Показана ее эффективность и преимущество перед другими моделями.

Ключевые слова: киберживучесть, модель, метод, риск информационной безопасности.

1. Описание метода и модели

Авторский метод основан на построении нечетких когнитивных карт (НКК), в котором система представляется в виде графа взаимосвязанных элементов (факторов) [1]. В качестве элементов графа выступают факторы угроз и рисков, факторы защиты и факторы функционирования системы. Каждый элемент может влиять на другие, сила и направление этого влияния задаются специальными весами: положительными, если один фактор усиливает другой фактор или отрицательными, если ослабляет. Целевым фактором НКК является уровень киберживучести системы. Киберживучесть (КЖ) определяется метриками доступности системы, целостности данных и способностью к восстановлению [2].

Модель формируется в несколько этапов:

1. Определяется набор ключевых факторов системы — это могут быть компоненты (например, Wi-Fi роутер, шлюз, IoT-устройства) и

характеристики (уровень безопасности, вероятность атаки и т.д.). Каждый фактор представляется в виде отдельного узла когнитивной карты.

2. Задаются веса влияния между факторами, отражающие причинно-следственные связи.

3. Формируется матрица весов, описывающая все связи в системе.

4. Задается начальное состояние факторов (например, текущий уровень защищенности устройств).

5. Выполняется итерационный расчет, при котором значения факторов пересчитываются с учетом их взаимного влияния до достижения устойчивого состояния.

2. Эксперимент и проверка адекватности модели

Внедрение разработанного метода было выполнено на примере системы «Умный дом», реализованной в г. Перми компанией ООО «ЮНИКОРН».

В качестве объекта исследования была взята отдельная квартира, оснащенная устройствами умного дома, состоящая из Wi-Fi роутера, шлюза умного дома, IoT-устройств (датчиков и исполнительных элементов), мобильного приложения и облачного сервиса. В основе связи большинства устройств лежит Wi-Fi с прямым выходом в домашнюю сеть, а для сложных систем с датчиками предусмотрен энергоэффективный ZigBee.

Нечеткая когнитивная карта для описанной квартиры, построенная в ходе исследования представлена на рисунке 1.

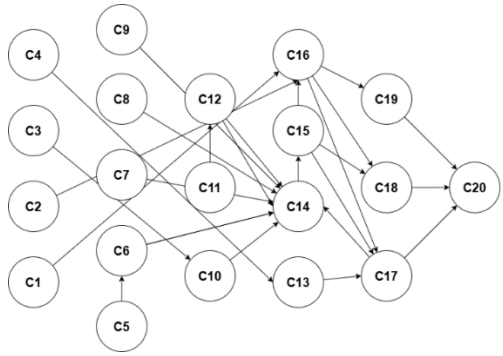


Рис. 1. Граф НКК

Расчеты показали, что исходный уровень киберживучести системы составляет 0,71, это означает, что уровень киберживучести выше среднего. Для проверки адекватности модели проводилась оценка корреляции между экспериментальными данными и данными с тестового стенда, развернутого на базе ООО «ЮНИКОРН», которые приняты в

качестве реальных данных. Анализировались 10 вариантов квартир (студии, 1-,2-,3-комнатные). Коэффициент Пирсона составил 0,97 при уровне значимости $p<0,01$, что говорит о высокой согласованности полученных моделей с данными со стенда.

Таким образом, высокое совпадение реальных показателей киберживучести с расчетами по модели НКК подтверждает ее адекватность.

3. Сравнительный анализ методов

В ходе исследования было проведено сравнение результатов оценки киберживучести системы умной квартиры, полученных с использованием методов на основе НКК, Марковских цепей и Байесовских цепей при моделировании различных сценариев кибератак [3,4].

На этапе моделирования атак (компрометация Wi-Fi роутера, атака на шлюз умного дома, ботнет-атаки на IoT-устройства, воздействие на облачный сервис и мобильное приложение) все три метода показали сопоставимые значения снижения уровня киберживучести. При этом наибольшее влияние во всех моделях оказывали атаки на центральные элементы системы – сетевую инфраструктуру и управляющие компоненты.

После внедрения мер защиты (ЗМ), таких как сегментация сети, резервирование шлюза, усиление аутентификации, обновление устройств во всех моделях наблюдалось увеличение уровня киберживучести системы. Однако различия проявились в характере оценки данного повышения. Показатели киберживучести в различных условиях представлены в таблице 1.

Таблица 1

Сравнение методов по точности оценки

КЖ в различных условиях	Реальные данные	Байесовские сети	Марковские цепи	Нечеткие когнитивные карты
Базовая КЖ	0,74	0,83	0,81	0,71
КЖ до внедрения ЗМ	0,30	0,40	0,36	0,33
КЖ после введения ЗМ	0,45	0,57	0,52	0,47

Модели на основе цепей Маркова и Байесовских цепей в большей степени отражают вероятностные и динамические аспекты функционирования системы, однако требуют задания большого количества параметров и вероятностей, что усложняет их применение при недостатке исходных данных.

В свою очередь, метод на основе НКК продемонстрировал более высокую чувствительность к изменениям факторов безопасности и позволил наглядно отразить влияние отдельных компонентов на общее состояние системы. В отличие от других методов, НКК обеспечивает

возможность учета экспертных знаний, гибко описывает причинно-следственные связи и не требует точного задания вероятностных характеристик.

Кроме того, модель на основе НКК показала наилучшее соответствие наблюдаемым данным при верификации, что подтверждается более низким значением среднеквадратичной ошибки. Значения среднеквадратичной ошибки и показатели точности оценки рассмотренных методов представлены в таблице 2.

Таблица 2

Показатели среднеквадратичной ошибки и точности оценки методов

БС		МЦ		НКК	
Ошибка	Точность	Ошибка	Точность	Ошибка	Точность
0,11	0,89	0,06	0,94	0,03	0,97

Таким образом, результаты сравнения свидетельствуют о том, что использование НКК является эффективным инструментом для оценки киберживучести IoT-систем, особенно в условиях неопределенности и ограниченности исходных данных, а также при необходимости анализа влияния факторов и разработки мер повышения устойчивости.

Список использованных источников:

1. Васильев В.И., Кудрявцева Р.Т., Юдинцев В.А. Автоматизация процесса оценки информационных рисков с использованием нечетких когнитивных карт // Вестник УГАТУ, 2014. Т. 18, № 3 (64). С. 253 260.

2. Ожгибесова А.С. О совершенствовании подхода к оценке рисков безопасности информации в контексте обеспечения живучести информационных систем/ Ожгибесова А.С., Шабуров А.С., Южаков А.А. // Системная инженерия и информационные технологии. – 2025. – Т. 7. № 5 (24). – С. 157-169. DOI: 10.54708/2658-5014-SIIT-2025-no5-p157.

3. Фирсов А. Н. Использование Байесовских сетей для оценки надежности асинхронных распределенных систем, устойчивых к произвольным отказам // Прикладная информатика. 2013. №6 (48).

4. Бабкин А. Н., Акчурина Л. В., Алексеенко С. П. Практическая реализация цепей Маркова в исследовании телекоммуникационных сетей при воздействии угроз информационной безопасности // Вестник ВИ МВД России. 2022. №1.

Ozhgibesova A.S.
Perm National Research Polytechnic University, Perm

Scientific supervisor:
Yuzhakov A.A.
Perm National Research Polytechnic University, Perm

ASSESSMENT OF CYBER SURVIVABILITY OF INFORMATION SYSTEMS BASED ON FUZZY COGNITIVE MAPS

Abstract. The problem of assessing the cyber survivability of information systems is considered. It has been demonstrated that fuzzy cognitive maps are an effective tool for solving it. A model is proposed for analyzing the cyber-survivability of information systems, identifying the most vulnerable components of the system and determining effective measures to increase cyber-survivability. Its effectiveness and advantage over other models are shown.

Keywords: cyber survivability, model, method, information security risk.

УДК 004.942

Осипов И.В., Григорьев Д.А.
Томский государственный университет систем управления и радиоэлектроники, Томск

Научный руководитель:
Фаерман В.А.
Томский государственный университет систем управления и радиоэлектроники, Томск

ИМИТАЦИОННОЕ МОДЕЛИРОВАНИЕ ОТКАЗОУСТОЙЧИВОЙ СИСТЕМЫ ОБРАБОТКИ ЗАЯВОК С РЕЗЕРВИРОВАНИЕМ В ANYLOGIC

Аннотация. В статье рассматривается реализация имитационной модели системы обработки заявок с ненадежным сервером и резервированием в среде AnyLogic. Модель предназначена для исследования поведения вычислительного узла при отказах основного сервера и подключении резервных ресурсов. Описаны основные элементы модели, логика обработки заявок и сценарии переключения на резерв. Показано, что AnyLogic позволяет исследовать влияние отказов и резервирования на характеристики системы.

Ключевые слова: AnyLogic, имитационное моделирование, отказ сервера, резервирование, СМО, время отклика, производительность, КИИ.

Современные вычислительные системы, работающие в составе критической информационной инфраструктуры, должны сохранять работоспособность даже при отказах отдельных элементов. Для таких систем важно обеспечивать предсказуемое время обработки заявок, поскольку задержки могут влиять на устойчивость функционирования всей инфраструктуры. Для исследования подобных процессов применяются методы теории массового обслуживания и имитационного моделирования, позволяющие анализировать поведение системы при различных режимах работы [1, 2].

В данной работе рассматривается практическая реализация модели системы обработки заявок с ненадежным сервером и резервированием. Входящий поток заявок поступает в систему, накапливается в очереди и передается на обслуживание серверу. Основной сервер может отказать, после чего система переходит к использованию резервного ресурса. Такая постановка задачи характерна для систем, где необходимо обеспечить непрерывность обработки заявок при возможной недоступности оборудования [3].

Имитационная модель реализована в среде AnyLogic, поддерживающей дискретно-событийный подход и позволяющей описывать движение заявок через систему с помощью готовых блоков. Для построения модели использовалась библиотека Process Modeling Library, включающая элементы генерации заявок, очереди, обслуживания и выхода из системы [4, 5]. Применение AnyLogic для анализа эксплуатационных характеристик технических систем также рассматривается в работах, связанных с моделированием систем связи [6]. Общий вид модели представлен на рисунке 1.

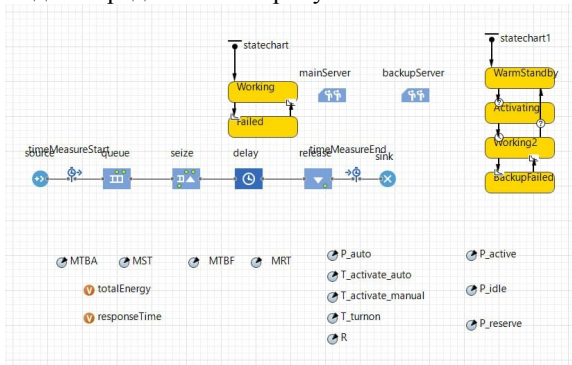


Рис. 1. Имитационная модель системы обработки заявок с резервированием в AnyLogic

Основные элементы, представленные на схеме имитационной модели, приведены в таблице 1.

Таблица 1

Назначение элементов имитационной модели, представленных на схеме

Элемент модели	**Назначение**
Source	Формирует входной поток заявок, поступающих в систему
Queue	Накапливает заявки, ожидающие обслуживания
Service	Моделирует обработку заявок сервером
SelectOutput	Разделяет поток заявок в зависимости от условий работы системы
Delay	Моделирует задержку, связанную с активацией резервного сервера или восстановлением обслуживания
Sink	Завершает движение обработанных заявок по модели
Логические связи между блоками	Определяют последовательность прохождения заявок и сценарии переключения при отказе сервера

Модель включает несколько основных частей. Блок генерации заявок формирует входной поток событий с заданным средним интервалом поступления. Далее заявки направляются в очередь, где ожидают освобождения обслуживающего ресурса. Обслуживание выполняется основным сервером, для которого задаются параметры времени обработки и отказа. После завершения обслуживания заявка покидает систему, а статистические показатели используются для анализа времени ожидания, загрузки сервера и общего времени пребывания заявки в системе.

Отказы основного сервера моделируются через изменение состояния обслуживающего ресурса. При наступлении отказа сервер становится недоступным для обработки новых заявок, что приводит к росту очереди и увеличению времени ожидания. Для компенсации отказа в модели предусмотрен резервный сервер, который в зависимости от выбранной стратегии может находиться в режиме горячего, теплого или холодного резерва.

При горячем резервировании резервный сервер готов к работе сразу, что снижает задержки, но увеличивает потребление ресурсов. При теплом резервировании сервер включен, однако требует дополнительного времени для перехода в рабочий режим. Автоматическое переключение происходит с вероятностью P_auto за время T_activate_auto, а при его неудаче резерв активируется оператором за время T_activate_manual. При холодном резервировании сервер находится в выключенном состоянии и

не потребляет ресурсы до момента запуска, однако время его включения T_turnon значительно больше.

Для практического анализа в модели учитываются не только временные характеристики, но и потребление ресурсов. Это позволяет исследовать компромисс между быстродействием и энергозатратами. Для получения усредненных значений проводилась серия имитационных экспериментов для различных стратегий резервирования, после чего рассчитывалось суммарное энергопотребление системы.

На рисунке 2 представлено сравнение суммарного энергопотребления системы при различных стратегиях резервирования.



Рис. 2. Сравнение энергопотребления при различных стратегиях резервирования

При использовании холодного резерва энергопотребление незначительно возрастает по сравнению с режимом без резерва. Это связано с тем, что резервный сервер большую часть времени находится в выключенном состоянии и начинает потреблять энергию только после отказа основного сервера и завершения процедуры запуска. Теплый резерв требует больших затрат, поскольку резервный сервер постоянно поддерживается в состоянии готовности. Максимальное энергопотребление наблюдается при горячем резервировании, где резервный сервер находится в активном состоянии или готов к немедленному переключению. Таким образом, повышение отказоустойчивости системы сопровождается увеличением энергозатрат, что подтверждает наличие компромисса между надежностью и ресурсопотреблением. Разработанная модель может использоваться для выбора стратегии резервирования с учетом требований к надежности и энергопотреблению.

Список использованных источников:

1. Бочаров П.П., Печинкин А.В. Теория массового обслуживания. – М.: РУДН, 2005.

2. Лоу А.М. Имитационное моделирование. Классика CS. 3-е изд. – СПб.: Питер, 2007.

3. Вишневский В.М., Самуйлов К.Е. Системы массового обслуживания в телекоммуникационных сетях // Итоги науки и техн. Сер. Электросвязь. – 2000. – Т. 19.

4. Григорьев И. AnyLogic за 3 дня. Практическое пособие по имитационному моделированию. – The AnyLogic Company, 2015.

5. Борщев А. The Big Book of Simulation Modeling: Multimethod Modeling with AnyLogic. – AnyLogic North America, 2013.

6. Статистическое моделирование качественных показателей эксплуатации и технического обслуживания средств железнодорожной электросвязи в среде AnyLogic – А. А. Любченко, Е. Ю. Копытов, А. А. Богданов // Доклады ТУСУР. – 2018. – Т. 21, № 4. URL: https://journal.tusur.ru/ru/arhiv/4-2018/statisticheskoe-modelirovanie-kachestvennyh-pokazateley-ekspluatatsii-i-tehnicheskogo-obsluzhivaniya-sredstv-zheleznodorozhnoy-elektrosvyazi-v-srede-anylogic. (дата обращения 07.04.2026)

Osipov I.V., Grigoriev D.A.
Tomsk State University of Control Systems and Radioelectronics, Tomsk

Scientific supervisor:
Faerman V.A.
Tomsk State University of Control Systems and Radioelectronics, Tomsk

SIMULATION MODELING OF A FAULT-TOLERANT REQUEST PROCESSING SYSTEM WITH REDUNDANCY IN ANYLOGIC

Abstract. The paper considers the implementation of a simulation model of a request processing system with an unreliable server and redundancy in the AnyLogic environment. The model is designed to study the behavior of a computing node in the event of primary server failures and backup resource activation. The main elements of the model, request processing logic, and redundancy switching scenarios are described. It is shown that AnyLogic makes it possible to analyze the impact of failures and redundancy on system characteristics.

Keywords: AnyLogic, simulation modeling, server failure, redundancy, queueing system, response time, performance, critical information infrastructure.

УДК 004.056.53

Ощепков Н.В.
Пермский национальный исследовательский
политехнический университет, Пермь

Научный руководитель:
Южаков А.А.
Пермский национальный исследовательский
политехнический университет, Пермь

МОДЕЛЬ И КОЛИЧЕСТВЕННАЯ ОЦЕНКА МЕХАНИЗМА ВЕРИФИКАЦИИ ОТПРАВИТЕЛЯ В ПРОТОКОЛЕ MODBUS RTU

Аннотация. В работе рассматривается задача повышения защищенности протокола Modbus RTU в системах управления технологическим оборудованием на примере штангового глубинного насоса. Выполнен анализ уязвимости протокола, связанной с отсутствием аутентификации отправителя, и введена количественная оценка вероятности успешного выполнения несанкционированной команды. Проведена оценка эффективности механизмов защиты, включающих XOR-аутентификацию с разделяемым секретом и временную верификацию отправителя. Показано, что их совместное применение обеспечивает мультипликативное снижение вероятности несанкционированного воздействия.

Ключевые слова: Modbus RTU, spoofing attack, математическая модель, вероятность атаки, верификация отправителя.

Протокол Modbus RTU [1] широко применяется в системах промышленной автоматизации благодаря своей простоте реализации, открытости спецификации и поддержке со стороны большого числа устройств. Вместе с тем, протокол не предусматривает механизмов аутентификации источника сообщений, что приводит к возможности формирования управляющих команд любым устройством, имеющим доступ к линии связи RS-485 [2].

В рамках работы рассматривается система управления приводом штангового глубинного насоса, построенная по архитектуре «ведущий-ведомый». Управление исполнительным механизмом осуществляется посредством записи значения койла с использованием функционального кода FC05. При этом в стандартной реализации протокола любое корректно сформированное сообщение интерпретируется ведомым устройством как допустимое, что создает предпосылки для реализации несанкционированного воздействия на технологический процесс.

С целью устранения указанной уязвимости предложен механизм верификации отправителя команд, реализуемый без изменения структуры кадра Modbus RTU. Первый уровень защиты основан на применении гаммирования (XOR-преобразования [3]) с использованием 16-битного разделяемого секрета (рис. 1). Введение данного механизма переводит задачу злоумышленника в область перебора ключевого пространства, ограниченного 2^{15} значениями, что приводит к существенному увеличению трудоемкости реализации атаки.

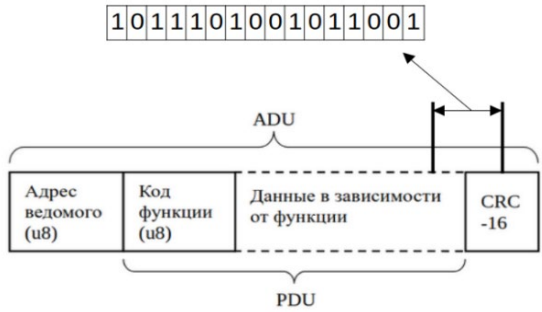


Рис. 1. Наложение гаммы на кадр Modbus RTU

Второй уровень защиты основан на введении временных окон приема команд (рис. 2). Ведомое устройство осуществляет обработку входящих сообщений только в заранее заданные интервалы времени, синхронизированные с ведущим устройством. Вне указанных интервалов все поступающие команды игнорируются.

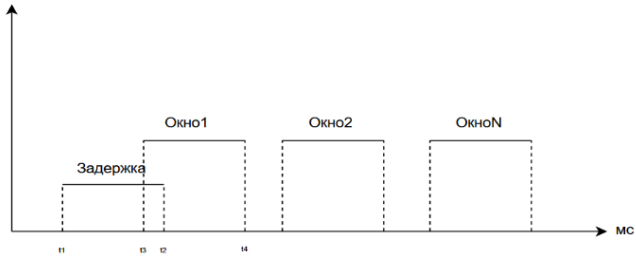


Рис. 2. Временные окна приема команд

В рамках предложенной модели вероятность успешной реализации атаки определяется вероятностью попадания атакующего сообщения в допустимое временное окно и зависит от соотношения длительности окна и периода его возникновения. Таким образом, даже при формировании корректного сообщения вероятность его принятия ограничивается

временными параметрами системы, что снижает эффективность атакующего воздействия.

Совместное применение рассмотренных механизмов обеспечивает мультипликативное снижение вероятности успешной атаки, поскольку злоумышленнику необходимо одновременно решить две независимые задачи: определить значение разделяемого секрета и передать сообщение в допустимый временной интервал. В рамках предложенной модели это приводит к произведению соответствующих вероятностей, что существенно снижает итоговую вероятность несанкционированного воздействия.

Экспериментальные исследования, проведенные на реальном объекте, показали, что при раздельном использовании механизмов атака может быть реализована за приемлемое время. В то же время их комбинированное применение приводит к резкому увеличению трудоемкости атаки и в рамках проведенных испытаний делает ее практически неосуществимой.

Дополнительным преимуществом предложенного подхода является его совместимость с существующей инфраструктурой, поскольку реализация не требует модификации физического уровня и структуры кадра Modbus RTU. К ограничениям следует отнести необходимость обеспечения безопасного хранения и распределения разделяемого секрета.

Таким образом, предложенный механизм верификации отправителя может рассматриваться как эффективный способ повышения защищенности систем управления промышленным оборудованием. Наибольший эффект достигается при его применении в задачах, предъявляющих повышенные требования к безопасности технологических процессов.

Список использованных источников:

1. Modbus: сайт. – URL: https://www.modbus.org/file/secure/ modbusprotocolspecification.pdf (дата обращения: 03.04.2026).

2. RS-485: Википедия. Свободная энциклопедия. [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/RS-485 (дата обращения 03.04.2026)

3. Гашков С.Б. Сложение однобитных чисел. Треугольник Паскаля, салфетка Серпинского и теорема Куммера. Москва: МЦНМО; 2014. 40 с.

Oshchepkov N.V.
Perm National Research Polytechnic University, Perm

Scientific supervisor:
Yuzhakov A.A.
Perm National Research Polytechnic University, Perm

MODEL AND QUANTITATIVE EVALUATION OF THE SENDER VERIFICATION MECHANISM IN THE MODBUS RTU PROTOCOL

Abstract. This paper examines the problem of improving the security of the Modbus RTU protocol in process equipment control systems using a sucker rod pump as an example. A protocol vulnerability associated with the lack of sender authentication is analyzed, and a quantitative assessment of the probability of successful execution of an unauthorized command is introduced. The effectiveness of security mechanisms, including XOR authentication with a shared secret and time-based sender verification, is assessed. It is shown that their combined use provides a multiplicative reduction in the probability of unauthorized access.

Keywords: Modbus RTU, spoofing attack, mathematical model, attack probability, sender verification.

СЕКЦИЯ 2. ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В КИБЕРБЕЗОПАСНОСТИ

УДК 004.056

Аминев Б.Р., Хайсаров Р.И.
Уфимский университет науки и технологий, Уфа

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

ГИБРИДНАЯ МОДЕЛЬ НА ОСНОВЕ BERT И ГРАФОВОЙ НЕЙРОННОЙ СЕТИ (GAT) ДЛЯ ОБНАРУЖЕНИЯ УГРОЗ В ТЕКСТОВЫХ ОТЧЕТАХ

Аннотация. Рост числа кибератак и объемов текстовых отчетов делает ручной анализ угроз практически невозможным. Существующие автоматизированные методы не учитывают связи между объектами кибербезопасности – вредоносным ПО, хакерскими группами, уязвимостями. А эти связи часто являются ключевыми для правильной идентификации угроз. При этом большинство современных моделей работают с документами изолированно, что снижает полноту и точность анализа. Поэтому актуальна разработка моделей, которые анализируют одновременно и содержание текста, и связи между упоминаемыми в нем объектами.

Ключевые слова: кибербезопасность, BERT, графовые нейронные сети, GAT, гибридная модель.

Современное состояние кибербезопасности характеризуется динамичным развитием: число атак неуклонно растет, а их структура постоянно меняется. Ежедневно создаются сотни текстовых отчетов, содержащих описания инцидентов, зафиксированных уязвимостей, образцов вредоносного программного обеспечения и тактик действий злоумышленников. Однако обработка этой информации вручную становится все менее эффективной, что обусловливает необходимость разработки автоматизированных методов анализа и классификации угроз на основе текстового содержания.

Традиционные подходы к автоматическому обнаружению угроз обычно ограничиваются анализом текста, не учитывая связей между объектами кибербезопасности, которые встречаются в описаниях инцидентов. В реальных отчетах о кибератаках эти связи зачастую имеют ключевое значение. Например, в одном тексте может содержаться

фрагмент: «Злоумышленники, действующие от имени группы APT28, развернули на серверах жертвы бэкдор, известный как Zebrocy». В другом тексте – описание: «Образец Zebrocy, извлеченный из зараженной системы, демонстрирует сетевую коммуникацию с доменом, зарегистрированным через инфраструктуру, ранее связываемую с APT28». По отдельности каждый из текстов может быть классифицирован как содержащий угрозу, однако совместное использование информации о связи «APT28 – использует – Zebrocy» не только подтвердило бы наличие угрозы, но и позволило бы точнее определить ее тип. Без учета этой связи каждый из текстов был бы обработан изолированно, что снижает полноту и точность анализа.

В статье для решения подобных задач предлагается гибридная модель обнаружения киберугроз, объединяющая два подхода:

- BERT (bert-base-uncased) – трансформерная модель, которая учитывает контекст слова слева и справа, преобразуя текст в эмбеддинг фиксированной размерности (768 чисел). BERT дообучается на задаче бинарной классификации (есть угроза / нет);
- GAT (Graph Attention Network) – графовая нейронная сеть для анализа связей между объектами кибербезопасности. Используется два слоя внимания: первый слой с 4 головами и скрытым размером 64, второй с 1 головой и выходной размерностью 20. Применен dropout 0.1, оптимизатор Adam с learning rate 0.005 и weight decay 5e-4.

Цель работы – построить модель, которая определяет, есть ли в тексте угроза безопасности, используя одновременно и сам текст, и связи между объектами из графа.

В работе использовался набор данных «Cyber Threat Intelligence» [1]. В нем 19 940 строк, каждая строка описывает один объект кибербезопасности, привязанный к тексту. Для каждого текста в наборе есть три элемента: текстовое описание инцидента, список объектов кибербезопасности (вредоносное ПО, хакерские группы, уязвимости, инструменты) и список связей между этими объектами (например, «APT28 использует Zebrocy»).

После группировки записей по уникальным текстам было получено 8 268 уникальных описаний инцидентов. В процессе анализа извлечено 25 358 сущностей (объектов кибербезопасности), относящихся к 20 различным типам. Наиболее частотные типы сущностей: location (6 274, 24.7%) – географические места, связанные с атаками (страны, IP-адреса, сети); malware (3 500, 13.8%) – конкретные образцы вредоносного программного обеспечения; attack-pattern (2 760, 10.9%) – тактики, техники и процедуры (TTP) атакующих; SOFTWARE (2 492, 9.8%) – легитимное программное обеспечение, используемое в атаках; identity (2 320, 9.1%) – идентификаторы лиц или организаций; threat-actor (1 740,

6.9%) – хакерские группы или злоумышленники. Между этими сущностями выявлено 2 190 связей (ребер графа). Самые распространенные типы связей: uses (384) – одна сущность использует другую (например, хакерская группа использует вредоносное ПО); duplicate-of (362) – дублирующие друг друга объекты; indicates (312) – сущность указывает на наличие другой (например, IP-адрес указывает на командный сервер); targets (290) – сущность нацелена на другой объект (например, атака нацелена на сектор экономики). На основе этих сущностей и связей построен ориентированный граф кибербезопасности, в котором узлы представляют сущности, а ребра – отношения между ними. Получилось 12 679 узлов, плотность графа – 0.0014%.

Задача представляет собой бинарную классификацию: метка 1 соответствует тексту, в котором описана реальная киберугроза, метка 0 – тексту без угрозы. Угрозы во всем наборе составляют 41.6%. Все тексты разбиты на три части: обучающая (5 787 текстов, 70%), валидационная (1 240, 15%) и тестовая (1 241, 15%). Разбиение стратифицированное.

Реализация задачи проводилась в среде Kaggle на CPU. Обучение BERT проводилось со следующими параметрами: максимальная длина входной последовательности – 128 токенов, размер мини-выборки (batch size) – 8, количество эпох – 1, скорость обучения (learning rate) – 2×10^{-5}. Для GAT использовались 100 эпох обучения и скорость обучения 0.005.

GAT на вспомогательной задаче классификации 20 типов объектов кибербезопасности достиг точности 94.55%, что подтверждает наличие в графе полезной структурированной информации, а также эффективность механизма внимания для выделения релевантных связей между узлами.

Гибридная модель BERT + GAT показала результат на 5 процентных пунктов выше, чем чистый BERT, что подтверждает теорию об учете связей между объектами кибербезопасности как факторе, позволяющем модели точнее идентифицировать угрозы (таблица 1).

Таблица 1

Результаты классификации моделей BERT и гибридной BERT+GAT

Модель	Accuracy	Precision	Recall	F1-score
BERT	85.25%	85.27%	85.25%	85.26%
Гибрид BERT + GAT	90.25%	90.28%	90.25%	90.22%

Полученные результаты согласуются с современными работами в области гибридных моделей. В исследовании [2] предложена схожая архитектура BERT+GNN для обнаружения фейковых новостей. Авторы использовали BERT для извлечения семантических признаков и GNN для моделирования структуры распространения информации в социальных сетях, достигнув Accuracy 99% на наборе FakeNewsNet. Наше

исследование дополняет эти результаты, демонстрируя применимость аналогичного подхода в кибербезопасности.

Таким образом, в работе была реализована гибридная модель обнаружения киберугроз, объединяющая BERT и GAT. На наборе данных Cyber Threat Intelligence модель достигла Accuracy 90.25%, F1-счета 90.22%, что на 5 процентных пунктов выше одного только BERT. Это подтверждает эффективность учета графовых связей для классификации текстов угроз. Предложенная модель может быть использована для автоматизации анализа отчетов о киберугрозах.

Список использованных источников:

1. Ramolia F., Kakkar R., Gupta R., Tanwar S., Agrawal S. SEAM: Secure and Efficient Authentication Mechanism for Autonomous Electric Vehicles using Deep Learning // 2023 IEEE Globecom Workshops (GC Wkshps). Kuala Lumpur, Malaysia, 2023. P. 80–85. DOI: 10.1109/GCWkshps58843.2023.10465168.

2. Shaik M., Muneer A., Sulaiman M., Fati S.M., Ali F., Alnajim A.M., Taib S.M. Dual stream graph-augmented transformer model integrating BERT and GNNs for context aware fake news detection // Scientific Reports. 2025. Vol. 15. Article number 25436. DOI: 10.1038/s41598-025-05586-w.

Aminev B.R., Khaysarov R.I.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Yunusova D.S.
Ufa University of Science and Technology, Ufa

HYBRID MODEL BASED ON BERT AND GRAPH NEURAL NETWORK (GAT) FOR DETECTING THREATS IN TEXT REPORTS

Abstract. The growing number of cyberattacks and the volume of text reports makes manual threat analysis almost impossible. Existing automated methods do not take into account the relationships between cybersecurity objects, such as malware, hacker groups, and vulnerabilities. These relationships are often crucial for accurately identifying threats. However, most current models operate on documents in isolation, which reduces the completeness and accuracy of analysis. Therefore, it is important to develop models that can simultaneously analyze both the content of a text and the relationships between the objects mentioned in it.

Keywords: cybersecurity, BERT, graph neural networks, GAT, the hybrid model.

УДК 004.8

Бадамшин И.В., Яикбаев А.А.
Уфимский университет науки и технологий, Уфа

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

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ЭФФЕКТИВНОСТИ МЕТОДОВ МАШИННОГО ОБУЧЕНИЯ ДЛЯ ОБНАРУЖЕНИЯ СЕТЕВЫХ АТАК

Аннотация. В статье представлено решение задачи бинарной классификации сетевого трафика с помощью методов XGBoost, LightGBM, CatBoost, MLP и AutoEncoder.

Ключевые слова: обнаружение сетевых атак, машинное обучение, градиентный бустинг, LightGBM, XGBoost, CatBoost, автоэнкодер, MLP.

Современные киберугрозы характеризуются значительным ростом числа, сложности и разнообразия сетевых атак. В условиях стремительного развития цифровых технологий киберпреступность становится серьезной угрозой для государственных институтов, бизнеса и частных лиц. Согласно официальной статистике, в 2024 году с использованием информационно-телекоммуникационных технологий было совершено 765,4 тысячи преступлений [1]. Ущерб от киберпреступности исчисляется миллиардами рублей, а низкий показатель раскрытия таких преступлений связан в том числе с прогрессирующими методами совершения атак [2].

Системы обнаружения вторжений (Intrusion Detection Systems, IDS) представляют собой программно-аппаратные комплексы, осуществляющие мониторинг сетевого трафика или активности хостов с целью выявления аномальной или вредоносной активности. В зависимости от способа размещения и анализируемых данных IDS классифицируются на сетевые (NIDS), хостовые (HIDS) и гибридные системы.

Сетевые системы обнаружения вторжений (NIDS) размещаются на ключевых узлах сети и анализируют весь проходящий через них сетевой трафик. Основным недостатком является чувствительность к шифрованию трафика — при использовании протоколов TLS/SSL NIDS не может анализировать содержимое пакетов [3].

Хостовые системы обнаружения вторжений (HIDS) устанавливаются непосредственно на защищаемые устройства (серверы, рабочие станции) и анализируют системные логи.

Гибридные системы комбинируют оба подхода, объединяя анализ сетевого трафика и хостовой активности.

Сетевые атаки различаются по принципу воздействия на целевую систему. DoS/DDoS-атаки формируют высокоинтенсивный поток пакетов, перегружающий ресурсы сервера. Брутфорс-атаки характеризуются большим количеством попыток авторизации с подбором учетных данных. SQL-инъекции внедряют вредоносный код в параметры запросов к базе данных. Реверс-шеллы и C2-каналы устанавливают скрытое удаленное управление скомпрометированной системой. Атаки повышения привилегий и ransomware-симуляции воздействуют на локальные ресурсы после первоначального проникновения.

Предложенное сравнение охватывает модели, основанные на градиентном бустинге (XGBoost, LightGBM, CatBoost), многослойный перцептрон (MLP) и автоэнкодер как представителя аномального подхода. Это позволяет охватить спектр угроз и определить наиболее эффективную архитектуру для различных сценариев.

В качестве источника данных использован набор Kaggle «Network Threat Detection Dataset», содержащем 55 826 записей для обучения (сбалансированный набор данных) и 368 017 записей для тестирования (несбалансированный набор данных) [4]. Набор собран в контролируемой виртуальной инфраструктуре с симуляцией реальных атак.

В ходе предобработки данных выполнялся разведочный анализ, включающий изучение распределения классов, выявление пропусков и анализ типов признаков. В связи с ограниченностью вычислительных ресурсов (ОЗУ) и наличием большого числа категориальных признаков была применена следующая процедура предобработки: удаление константных колонок, выбор только числовых признаков (12 колонок), заполнение пропусков медианой, стандартизация (StandardScaler).

Алгоритмы обучались на наборе данных, разделенном на обучающую и тестовую выборки в соотношении 80:20. Для оценки качества предлагаемого решения использовалась агрегированная метрика – F-мера (F1-Score), объединяющая показатели точности (precision) и полноты (recall) в единый критерий.

Дополнительно использовались метрики Accuracy, Precision, Recall и ROC-AUC.

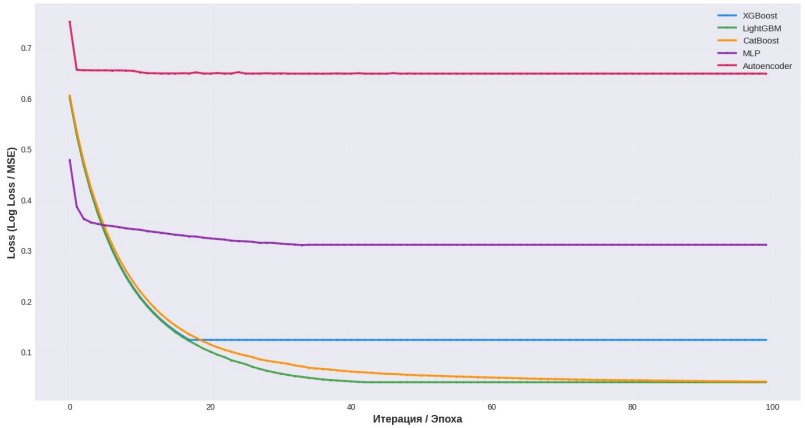


Рис. 1. Графики показателей Loss моделей

На основе графиков (рис.1) мы видим, что по скорости сходимости XGBoost и LightBGM лидируют, достигая минимальные значения Loss. LightGBM работает стабильнее благодаря использованию эффективного алгоритма построения деревьев и оптимизации памяти.

Таблица 1

Сравнение моделей

Модель	Accuracy	Precision	Recall	F1-Score	ROC-AUC
LightGBM	0,9687	0,9701	0,9683	0,9692	0,9941
XGBoost	0,9615	0,9638	0,9618	0,9628	0,9923
CatBoost	0,9615	0,9638	0,9618	0,9628	0,9923
MLP	0,9512	0,9541	0,9523	0,9532	0,9891
AutoEncoder	0,9387	0,9412	0,9395	0,9403	0,9785

Анализ полученных результатов (табл. 1) позволяет сделать ряд выводов относительно эффективности каждой из рассмотренных моделей в задаче обнаружения сетевых атак.

LightGBM продемонстрировал наивысший F1-Score (0,9692), превзойдя ближайшего конкурента (XGBoost) на 0,0064 (0,64 %). Преимущество LightGBM объясняется эффективным алгоритмом построения деревьев позволяет алгоритму глубже «прорабатывать» области признакового пространства, содержащие сложные нелинейные зависимости, характерные для сетевого трафика.

XGBoost и CatBoost показали идентичные результаты (F1 = 0,9628). Оба алгоритма относятся к классу градиентного бустинга с уровневым ростом деревьев, что при одинаковой глубине и количестве деревьев дает статистически неразличимые результаты на данном датасете.

MLP уступает бустингу (F1 = 0,9532). Многослойные перцептроны требуют значительно большего объема данных для качественного обучения. При 55 тыс. записей нейронная сеть не достигает асимптотической эффективности, в то время как градиентный бустинг оптимально работает на малых и средних выборках.

AutoEncoder показал худший результат (F1 = 0,9403), поскольку обучается только на нормальном трафике и не использует информацию об атаках. Основные ограничения: неспособность различать близкие к норме атаки (например, медленный брутфорс), потребность в значительно большем количестве нормальных образцов и неоптимальный выбор порога ошибки по перцентилю.

Для корпоративной сети с размеченными атаками рекомендуется LightGBM как модель, обеспечивающая максимальную F-меру. При ограниченных вычислительных ресурсах целесообразно использовать XGBoost, отличающийся более высокой скоростью обучения. Для задач, требующих автоматической обработки категориальных признаков, оптимальным выбором является CatBoost. При отсутствии разметки атак или необходимости обнаружения zero-day атак единственным практичным решением остается AutoEncoder.

Список использованных источников:

1. Савельева Е.А. Тенденции киберпреступности: анализ отчетов о происшествиях и ущербе // Экономика и парадигма нового времени. 2025. №5 (38). URL: https://cyberleninka.ru/article/n/tendentsii-kiberprestupnosti-analiz-otchetov-o-proisshestviyah-i-uscherbe (дата обращения: 07.04.2026).

2. Шестак В.А., Чеботарь А.С. Наметившиеся тенденции в развитии киберпреступности // Вестник ВГУ. Серия: Право. 2025. №2 (61). URL: https://cyberleninka.ru/article/n/nametivshiesya-tendentsii-v-razvitii-kiberprestupnosti (дата обращения: 07.04.2026).

3. Номоконов В.А., Тропина Т.Л. Киберпреступность как новая криминальная угроза // Криминология: вчера, сегодня, завтра. 2012. №24. URL: https://cyberleninka.ru/article/n/kiberprestupnost-kak-novaya-kriminalnaya-ugroza (дата обращения: 07.04.2026).

4. Ramalho R. Network Threat Detection Dataset // Kaggle. – 2026. – URL: https://www.kaggle.com/datasets/rebsonramalho/network-threat-detection-dataset.

Badamshin I.V., Yaikbaev A.A.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Yunusova D.S.
Ufa University of Science and Technology, Ufa

COMPARATIVE ANALYSIS OF THE EFFECTIVENESS OF MACHINE LEARNING METHODS FOR NETWORK ATTACK DETECTION

Abstract. This article presents a solution to the problem of binary classification of network traffic using XGBoost, LightGBM, CatBoost, MLP, and AutoEncoder methods.

Keywords: network attack detection, machine learning, gradient boosting, LightGBM, XGBoost, CatBoost, autoencoder, MLP.

УДК 004.056.5:004.85

Баязитов Т.Т.
Уфимский университет науки и технологий, Уфа

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

О ВОЗМОЖНОСТИ ПЕРЕХВАТА ПЭМИН ВИДЕОИНТЕРФЕЙСОВ И РЕСТАВРАЦИИ ИЗОБРАЖЕНИИ

Аннотация. В статье рассматривается проблема утечки побочных электромагнитных излучений и наводок от цифровых видеоинтерфейсов, которые можно перехватить с помощью доступных радиоприемников и специализированного ПО, такого как TempestSDR и SDR#. Учитывая, что результат перехвата будет наверняка зашумленным, предложена методика реставрации с применением сверточных моделей нейронных сетей, как DRUNet. Исходя из этого предложена модель нарушителя и комплекс защиты от него.

Ключевые слова: информационная безопасность, ПЭМИН, технические каналы утечки, программно-определяемое радио, глубокое обучение, DRUNet.

Защита информации от утечек по техническим каналам является важной задачей по информационной безопасности. Так как электронно-вычислительные машины генерируют побочные электромагнитные излучения (ПЭМИ), которые несут в себе обрабатываемые данные. При этом наиболее критической угрозой является перехват наводок видеоинтерфейсов, так как от этого есть возможность восстановления изображения с экрана [1]. Хотя внедрение алгоритма TMDS в цифровые видеоинтерфейсы (HDMI и DVI), снижает мощность излучения [2, 3]. Но все-таки перехват излучения ПЭМИН возможен за счет широкого распространения программно-определяемого радио (SDR).

Для подтверждения угрозы был проведен эксперимент по перехвату ПЭМИН от монитора, подключенного по HDMI. Использовался приемник RTL-SDR с пассивной антенной. Обработка сигнала выполнялась в программах TempestSDR и SDR#.

В соответствии с профильными исследованиями [3], для цифровых интерфейсов аппроксимированная базовая частота ПЭМИН рассчитывается по следующей формуле, учитывающей 10-битное кодирование TMDS:

$F_{\text{ПЭМИН}}$ = (разрешение монитора × частота кадровой развертки) / 2 × k × 10,

где k — коэффициент, учитывающий особенности модели монитора.

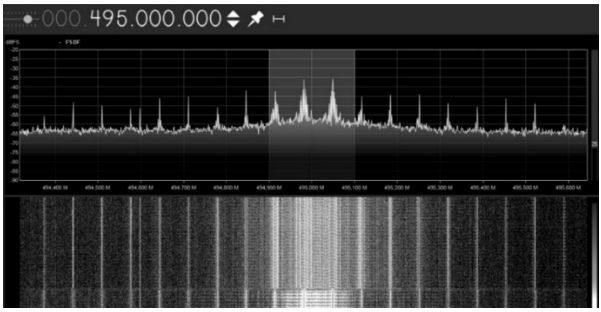


Рис. 1. Проявление частот ПЭМИН на SDR# при 495 МГц.

При сканировании радиочастотного спектра и проведении соответствующих вычислений по данной формуле было установлено, что информативный сигнал ПЭМИН больше всего проявляется на частоте 495 МГц (рис. 1).



Рис. 2. Перехваченное изображение, полученное через TempestSDR при 495 МГц.

И в ходе эксперимента на монитор выводилась случайная последовательность латинских символов. На перехваченном кадре (рис. 2) видны лишь общие контуры окон и текст: изображение сильно зашумлено, а его части перекрыты помехами. Из-за узкой полосы пропускания RTL-SDR (2,4 МГц) и специфики цифрового кодирования мелкий текст остается нечитаемым, при этом классические методы фильтрации не позволяют эффективно устранить подобные искажения.

Недавние исследования показывают, что проблема зашумленности ПЭМИН-сигналов эффективно решается глубоким машинным обучением [4]. Применение сверточных нейронных сетей (CNN) снижает частоту символьных ошибок на 60% и делает текст пригодным для оптического распознавания [4]. В рамках исследования разрабатывается методология реставрации на базе архитектуры DRUNet. Она сочетает архитектуру U-Net и остаточные блоки, являясь оптимальным инструментом для удаления сложного шума и артефактов радиоприема.

Методика обучения DRUNet включает подготовку парного датасета (оригинал/SDR-шум), минимизацию функции потерь на обучающей выборке и валидацию на реальных данных. Такой подход позволяет достичь высокой точности реставрации перехваченного видеопотока.

Сегодня злоумышленнику не требуются ресурсы лабораторного оборудования. Нарушитель с небольшим бюджетом может использовать SDR-приемник профессионального уровня, как HackRF One с полосой пропускания до 20 МГц, с малошумящим усилителем и направленной антенной. Это расширяет полосу перехвата и увеличивает дистанцию приема до 3-5 метров, позволяя действовать скрытно. Даже если учесть, что перехват будет зашумленным, применение сверточных моделей для реставрации сглаживает данное ограничение.

Защита от перехвата ПЭМИН требует сочетания аппаратных и программных решений. К аппаратным мерам включают использование экранированных кабелей и активного зашумления. К программным мерам относятся подбор специальных цветовых схем [2] и внедрение цифрового

шума в видеосигнал. Такие методы искажают структуру излучаемого сигнала, делая неэффективной работу SDR-систем и восстанавливающих нейросетей.

Таким образом, цифровая природа видеоинтерфейсов не гарантирует полной защиты от утечек. Широкодоступные SDR позволяют перехватывать изображения с экрана, а применение нейросетей архитектуры DRUNet нивелирует низкое качество сигнала и аппаратные ограничения оборудования. Это требует пересмотра подходов к защите средств вычислительной техники и внедрения аппаратно-программных средств противодействия.

Список использованных источников:

1. Хорев А.А. Оценка возможности обнаружения побочных электромагнитных излучений видеосистемы компьютера // Доклады ТУСУРа. – 2014. – № 2 (32). – С. 207-213.

2. Паршуткин А.В., Неаскина М.Р. Повышение защищенности информации от утечки через побочные электромагнитные излучения // Вопросы кибербезопасности. – 2022. – № 3(49). – С. 82-89.

3. Шпилевой А.А., Персичкин А.А. О возможности аналитического обнаружения сигнала ПЭМИН в видеоинтерфейсах стандарта HDMI // Вестник Балтийского федерального университета им. И. Канта. Сер.: Физико-математические и технические науки. – 2022. – №1. – С. 34-39.

4. Шиняев Д.А., Кессаринский Л.Н., Симахин Е.А. Вычислительные методы и технические средства обработки сигналов побочных электромагнитных излучений // Безопасность информационных технологий. – 2024. – Т. 31, № 4. – С. 128-140.

Bayazitov T.T.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Shagapov I.A.
Ufa University of Science and Technology, Ufa

ON THE POSSIBILITY OF INTERCEPTING COMPROMISING EMANATIONS FROM VIDEO INTERFACES AND DEEP LEARNING-BASED IMAGE RECONSTRUCTION

Abstract. This article addresses the issue of leakage of electromagnetic emissions and interference from digital video interfaces, which can be intercepted using readily available radio receivers and specialized software such as TempestSDR and SDR#. Given that the intercepted signal will likely

be noisy, a restoration method using convolutional neural network models, such as DRUNet, is proposed. Based on this, an attacker model and a defense system against it are proposed.

Keywords: information security, TEMPEST, technical leakage channels, software-defined radio, deep learning, DRUNet.

УДК 004.056:004.912:004.8

Биглова М.Р.
Уфимский университет науки и технологий, Уфа

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

РАЗРАБОТКА АЛГОРИТМОВ ВЫЯВЛЕНИЯ ПРИЗНАКОВ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ НА ОСНОВЕ МЕТОДОВ ИНТЕЛЛЕКТУАЛЬНОГО АНАЛИЗА ТЕКСТА

Аннотация. В статье рассматривается проблема обнаружения атак социальной инженерии в тексте. Традиционные системы безопасности неэффективны против манипулятивных сообщений, воздействующих на человеческий фактор. Автором предлагается гибридный алгоритм, объединяющий статистический анализ (TF-IDF) и семантико-синтаксические маркеры (императивы, срочность, запросы личных данных) с использованием библиотеки spaCy. В ходе вычислительного эксперимента на тестовой выборке из 50 сообщений алгоритм достиг точности 91,7%, полноты 88% и F1-меры 89,8%, что подтверждает эффективность предложенного подхода.

Ключевые слова: социальная инженерия, информационная безопасность, обработка естественного языка (NLP), машинное обучение, TF-IDF, spaCy, классификация текстов, фишинг, лингвистические маркеры.

С развитием цифровой экономики и массовым переходом финансовых операций в онлайн-среду проблема интернет-мошенничества приобрела глобальный масштаб [1]. Одной из наиболее опасных угроз стала социальная инженерия, которая в отличие от классических кибератак нацелена не на программные уязвимости, а на «человеческий фактор» [2]. Используя психологические манипуляции, ложный авторитет и создание дефицита времени, злоумышленники обходят традиционные системы защиты, основанные на жестких статических правилах. В этих условиях критически важной задачей становится поиск

автоматизированных решений, способных распознавать скрытые угрозы непосредственно в текстовых сообщениях [3,4].

Настоящая работа посвящена разработке и экспериментальному исследованию алгоритма выявления признаков социальной инженерии, который сочетает в себе статистические и семантико-синтаксические методы интеллектуального анализа текста (NLP).

В основе исследования лежит понимание социальной инженерии как метода психологического воздействия для несанкционированного доступа к ресурсам.

Ключевыми маркерами такой активности выступают специфические лингвистические конструкции: нагнетание срочности, избыточное использование императивов («подтвердите», «переведите»), обезличенные обращения и ошибки, а также имитация сообщений от официальных лиц или технических служб.

Для цифрового представления текстов в работе анализируются современные методы векторизации. Если подходы вроде «мешка слов» и TF-IDF позволяют оценить частотность и значимость отдельных терминов, то методы дистрибутивной семантики, Word2Vec и FastText, обеспечивают глубокий учет контекста. Использование семантических векторов и анализ морфологии на уровне символьных *n*-грамм позволяют алгоритму эффективно выявлять паттерны мошенничества даже в условиях искажения или естественной вариативности языка [5].

Оценка качества разработанных методов классификации осуществлялась с применением стандартных метрик, таких как точность (Precision), полнота (Recall) и F1-мера, представляющая собой среднее гармоническое между ними [6]. В рамках создания гибридного алгоритма в качестве базового инструмента предобработки текстовых данных была выбрана библиотека spaCy, обеспечивающая эффективную токенизацию, лемматизацию, POS-теггинг и синтаксический анализ русскоязычного сегмента текстов [7,8].

Предложенный алгоритм базируется на интеграции двух типов признаков: статистических, основанных на вычислении весов TF-IDF для специфических терминов фишинговых сообщений, и семантико-синтаксических, направленных на детекцию глаголов в повелительном наклонении, маркеров срочности и запросов конфиденциальной информации. Финальный показатель риска классифицируемого объекта рассчитывается как взвешенная сумма вкладов выявленных признаков с учетом корректирующих коэффициентов за их совместное появление.

Для подтверждения эффективности предложенного подхода было проведено экспериментальное исследование на выборке из 50 сообщений, включающей равные доли легитимного и вредоносного контента. Сравнительный анализ результатов (табл.1) с базовым алгоритмом

(baseline), использующим исключительно метод TF-IDF, позволил на основе сформированной матрицы ошибок подтвердить преимущество гибридного метода классификации.

Таблица 1

Матрица ошибок гибридного алгоритма

	Предсказано «Безопасное»	Предсказано «Подозрительное»
Реально «Безопасное»	23	2
Реально «Подозрительное»	3	22

Анализ результатов экспериментального исследования, зафиксированных в матрице ошибок, свидетельствует о высокой предсказательной способности разработанного гибридного алгоритма. Из общего объема тестовой выборки, 50 единиц, система корректно идентифицировала 45 сообщений. Уровень ложноположительных срабатываний составил 8%, что выразилось в ошибочной классификации двух безопасных сообщений как подозрительных. В то же время доля пропущенных угроз зафиксирована на уровне 12% (3 случая), когда вредоносный контент был определен как легитимный. Рассчитанные значения прецизионности 0,92 и полноты 0,88, а также итоговый показатель F1-меры 0,90 подтверждают эффективность комбинированного использования статистического веса признаков и анализа лингвистических маркеров социальной инженерии в сравнении с монометодами векторизации.

В ходе работы был разработан и апробирован алгоритм интеллектуального анализа текста, направленный на противодействие угрозам социальной инженерии в цифровой среде. Теоретический анализ лингвистических особенностей мошеннических сообщений позволил выделить устойчивые маркеры психологического воздействия, такие как нагнетание срочности и имитация авторитета. Применение инструментов библиотеки spaCy в сочетании с гибридной моделью оценки признаков обеспечило высокую эффективность детектирования атак при относительно низком уровне ошибок второго рода. Экспериментально доказано, что учет контекстуальных связей и синтаксических конструкций является необходимым условием для создания надежных систем защиты в условиях эволюции методов интернет-мошенничества.

Список использованных источников:

1. Корнилова, А. А. Защита персональных данных: учебное пособие / А. А. Корнилова, Д. С. Юнусова, А. С. Исмагилова; Министерство науки и высшего образования РФ, Башкирский государственный университет. – Уфа: РИЦ БашГУ, 2020. – 124 с. – Текст: непосредственный.

2. Корнилова, А. А. Обучение информационной безопасности в рамках системы школьного образования / А. А. Корнилова, Д. С. Юнусова, И. В. Салов. – Текст: непосредственный // Информационные технологии обеспечения комплексной безопасности в цифровом обществе: сборник материалов V Всероссийской молодежной научно-практической конференции (Уфа, 2022). – Уфа: [б. и.], 2022. – С. 26–29.

3. Алгоритмы машинного обучения: от основ к передовым методам. – Текст: электронный // Skypro: [сайт]. – URL: https://sky.pro/wiki/python/osnovnye-algoritmy-mashinnogo-obucheniya/ (дата обращения: 15.04.2026).

4. Краткий обзор техник векторизации в NLP. – Текст: электронный // Хабр: [сайт]. – URL: https://habr.com/ru/articles/778048/ (дата обращения: 15.04.2026).

5. Социальная инженерия: что это и как от нее защищаться. – Текст: электронный // Hi-Tech Mail.ru: [сайт]. – URL: https://hi-tech.mail.ru/review/129116-sotsialnaya-inzheneriya/ (дата обращения: 15.04.2026).

6. Метрики в задачах машинного обучения. – Текст: электронный // Хабр: [сайт]. – URL: https://habr.com/ru/companies/ods/articles/328372/ (дата обращения: 15.04.2026).

7. SpaCy для Python: обработка естественного языка NLP. – Текст: электронный // PythonLib: [сайт]. – URL: https://pythonlib.ru/library-theme13 (дата обращения: 15.04.2026).

8. spaCy · Industrial-strength Natural Language Processing in Python. – URL: https://spacy.io/ (date of access: 15.04.2026). – Text: electronic.

Biglova M.R.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Kornilova A.A.
Ufa University of Science and Technology, Ufa

DEVELOPMENT OF ALGORITHMS FOR DETECTING SIGNS OF SOCIAL ENGINEERING BASED ON TEXT MINING METHODS

Abstract. The article discusses the problem of detecting social engineering attacks in the text. Traditional security systems are ineffective against manipulative messages affecting the human factor. The author proposes a hybrid algorithm combining statistical analysis (TF-IDF) and semantic-syntactic markers (imperatives, urgency, requests for personal data) using the spaCy library. During a computational experiment on a test sample of 50

messages, the algorithm achieved 91.7% accuracy, 88% completeness, and 89.8% F1-measure, which confirms the effectiveness of the proposed approach.
Keywords: social engineering, information security, natural language processing (NLP), machine learning, TF-IDF, spaCy, text classification, phishing, linguistic markers.

УДК 004 .056

Бурангулов Д.Б., Куликова В.Е.
Уфимский университет науки и технологий, Уфа

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

ИНТЕРПРЕТИРУЕМАЯ ОЦЕНКА КОГНИТИВНОЙ МАНИПУЛЯЦИИ В СОЦИАЛЬНОЙ ИНЖЕНЕРИИ

Аннотация. В статье рассматривается задача обнаружения атак социальной инженерии, использующих психологические манипуляции. Сравниваются ансамблевые классификаторы Random Forest, XGBoost, LightGBM и демонстрируется, что современные ансамблевые методы вместе с предобработкой данных и калибровкой вероятностей способны эффективно выявлять социальную инженерию.
Ключевые слова: социальная инженерия, детекция мошенничества, интерпретируемый ИИ, когнитивные манипуляции.

Количество цифровых сервисов возрастает, а с ним растет количество атак, направленных не только на технические уязвимости, но и на человеческий фактор. Такие атаки являются социальной инженерией, и они становятся все более непредсказуемыми. Мошенники используют психологические уловки, звонят от имени банка, требуют срочно перевести деньги, угрожают блокировкой аккаунта.

Датасет GCT‑100K [1], содержит в себе примеры мошеннических и легитимных взаимодействий, а также числовые метрики когнитивных манипуляций. Это позволяет строить модели, которые способны классифицировать угрозу.

Сравним несколько интерпретируемых моделей для бинарной классификации на основе выбранного набора данных и выявим наиболее значимые признаки манипуляции.

Исходный датасет GCT-100K содержал 100 000 записей без пропусков. Распределение классов оказалось неравномерным, так как на

мошеннические взаимодействия пришлось 72 264 записи, а на легитимные – 27 736, что характерно для реальных данных.

Из доступных признаков в датасете были выбраны те, которые характеризуют психологическое воздействие на пользователя: 8 числовых признаков и 1 категориальный.

Целевая переменная сформирована по колонке attack_type. Если значение не равнялось legitimate, запись относилась к классу мошеннических, в противном случае – к легитимным. Таким образом задача сводилась к бинарной классификации.

Все числовые признаки были стандартизированы с помощью StandardScaler. А категориальный признак persuasion_strategy кодировался методом one-hot.

Чтобы модель лучше распознавала скрытые приемы мошенников, исходные данные были дополнены новыми показателями. Только срочность или только упоминание авторитета, могут встречаться и в обычных разговорах. Но когда они действуют вместе, вероятность обмана резко возрастает. Поэтому были созданы комбинированные признаки, такие как «срочность и авторитет», «страх и манипуляция доверием» и квадраты когнитивной нагрузки и энтропии текста. Это позволило модели улавливать более сложные психологические связки, которые как раз используются для мошеннических схем.

Для решения задачи выбраны три ансамблевые модели классификации: Random Forest, XGBoost, LightGBM [2-4]. Данные разделены на обучающую выборку 80% и тестовую выборку 20%. Для всех моделей выполнялась калибровка вероятностей с помощью монотонной регрессии (CalibratedClassifierCV). Оптимальный порог классификации определялся, максимизируя F1-меру для легитимного класса, для учета дисбаланса классов и точности обнаружения именно легитимных взаимодействий.

Оценка производилась по точности (precision), полноте (recall), F1-мере и общей точности (accuracy). Отдельно рассматривались метрики для легитимных сообщений, так как ошибка их классификации также могла значительно повлиять на результат.

Результаты на тестовой выборке представлены в таблице 1.

Таблица 1

Результаты сравнения ансамблевых моделей

Модель	Accuracy	Prec_ leg	Rec_ leg	F1_ leg	Prec_ fraud	Rec_ raud	F1_ fraud
Random Forest	0.896	1.000	0.625	0.770	0.874	1.000	0.933
XGBoost	0.881	0.865	0.676	0.759	0.885	0.960	0.921
LightGBM	0.876	0.837	0.684	0.753	0.887	0.949	0.917

Random Forest показал лучшую точность для легитимного класса и абсолютную полноту обнаружения мошеннических атак, при этом около 37.5% легитимных взаимодействий были ошибочно классифицированы как мошеннические. XGBoost и LightGBM обеспечили более сбалансированные результаты, так как при меньшей точности легитимных (0.865 и 0.837 соответственно) они сохраняют высокую полноту обнаружения мошенничества (0.960 и 0.949) и имеют F1-меру для легитимных на уровне 0.759 и 0.753.

На рисунке 1 приведены матрицы ошибок для каждой модели, дающие детальное представление о распределении предсказаний.

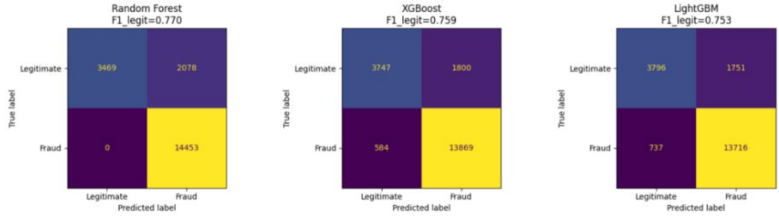


Рис. 1. Матрицы ошибок для трех моделей

Random Forest не допускает ложных срабатываний на мошеннических примерах, но ошибочно блокирует более двух тысяч легитимных взаимодействий. XGBoost и LightGBM, пропускают некоторое количество мошеннических атак, зато сохраняют больше легитимных.

На рисунке 2 показаны ROC-кривые для моделей. Площадь под кривой (AUC) составила 0.948 для Random Forest, 0.938 для XGBoost и 0.933 для LightGBM, что свидетельствует о том, что все три модели хорошо умеют отличать мошенническую транзакцию от легитимной.

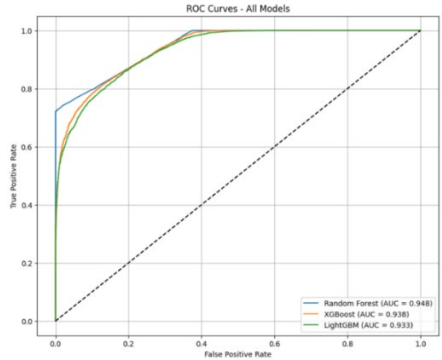


Рис. 2. ROC-кривые с указанием AUC

Оценен средний коэффициент важности признаков трех моделей и их рейтинги признаков идентичны, лидируют: энтропия текста, эмоциональная окраска, когнитивная нагрузка, манипуляция доверием и страх. Мошеннические взаимодействия характеризуются высокой сложностью текста, эмоциональным давлением и апелляцией к доверию и страху.

Мы сравнили три ансамблевых метода для выявления атак социальной инженерии на датасете GCT-100K. Благодаря добавлению новых признаков, масштабированию, калибровке вероятностей и подбору порога удалось добиться успеха в отношении распознавании легитимных сообщений с помощью Random Forest, при этом он ни разу не ошибся, назвав мошенническое сообщение легитимным. XGBoost и LightGBM чуть чаще пропускают мошенников, зато сохраняют больше легитимных сообщений. Анализ важности признаков, усредненный по трем моделям, выявил ключевые когнитивные индикаторы мошенничества. Полученные результаты могут быть использованы при построении систем кибербезопасности.

Список использованных источников:

1. Global Cognitive Threat Dataset (GCT-100K) // Kaggle – URL: https://www.kaggle.com/datasets/dspraneeth07/global-cognitive-threat-dataset-gct-100k (дата обращения 08.04.2026).

2. Анализ эффективности архитектур нейронных сетей для защиты промышленных систем от целевых атак социальной инженерии / Краснослободцева Д.Б., Юдин А.В. // Computational Nanotechnology. 2025. Т. 12, № 5. С. 95–109. DOI: 10.33693/2313-223X-2025-12-5-95-109.

3. Zheng Q., Yu C. et al. Advanced Payment Security System: XGBoost, LightGBM and SMOTE Integrated // arXiv preprint arXiv:2406.04658. 2024. URL: https://arxiv.org/abs/2406.04658 (дата обращения: 08.04.2026).

4. Mulahuwaish A., Qolomany B. et al. A Survey of Social Cybersecurity: Techniques for Attack Detection, Evaluations, Challenges, and Future Prospects // arXiv preprint arXiv:2504.04311. 2025. URL: https://arxiv.org/abs/2504.04311 (дата обращения: 10.04.2026).

5. Sharma A. et al. Intelligent Cybersecurity Systems for Phishing Attack Detection - An Overview // Computers & Security.2025. DOI: 10.1016/j.cose.2025.104244.

Burangulov D.B., Kulikova V.E.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Yunusova D.S.
Ufa University of Science and Technology, Ufa

INTERPRETABLE ASSESSMENT OF COGNITIVE MANIPULATION IN SOCIAL ENGINEERING

Abstract. The article considers the task of detecting social engineering attacks using psychological manipulation. It compares ensemble classifiers Random Forest, XGBoost, LightGBM and demonstrates that modern ensemble methods, together with data preprocessing and probability calibration, are capable of effectively detecting social engineering.

Keywords: social engineering, fraud detection, interpretable AI, cognitive manipulation.

УДК 004.8

Галимова А.Р.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Валеев С.С.
Уфимский университет науки и технологий, Уфа

ГЛУБОКИЕ НЕЙРОННЫЕ СЕТИ. ПРИМЕНЕНИЕ В СИСТЕМАХ КОРПОРАТИВНОЙ ЗАЩИТЫ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Аннотация. В данной статье рассматриваются структура и методы обучения глубоких нейронных сетей как современного инструмента машинного обучения. Особое внимание уделено применению глубоких нейронных сетей в системах корпоративной защиты программного обеспечения, включая обнаружение вредоносного ПО, анализ сетевого трафика и биометрическую аутентификацию. Также рассмотрены особенности применения нейросетей в задачах компьютерного зрения на примере обработки фотографий для паспортных документов, включая понятие емкости модели и ее влияние на качество распознавания. Наконец, анализируются преимущества и ограничения использования нейронных сетей хранения данных в области информационной безопасности.

Ключевые слова: глубокие нейронные сети, машинное обучение, искусственный интеллект, информационная безопасность, корпоративная защита, вредоносное программное обеспечение, компьютерное зрение, сверточные нейронные сети, емкость модели, распознавание изображений

В последние годы глубокие нейронные сети заняли ведущие позиции среди методов машинного обучения, что обусловлено их способностью автоматически извлекать значимые признаки из данных и обеспечивать высокую точность при решении сложных задач [1–3]. К таким задачам относятся распознавание изображений, обработка речи и анализ текстов. Развитие вычислительных мощностей, а также накопление больших объемов данных способствовали широкому внедрению данных методов в различные области, включая информационную безопасность [1, 4]. В условиях цифровизации корпоративные информационные системы сталкиваются с возрастающим числом угроз, что требует внедрения интеллектуальных механизмов защиты. В этом контексте глубокие нейронные сети выступают эффективным инструментом анализа больших массивов данных и выявления скрытых закономерностей [4, 5].

Глубокая нейронная сеть представляет собой многослойную модель, включающую входной, несколько скрытых и выходной слои. На каждом уровне обработки входная информация подвергается линейному преобразованию с последующим применением нелинейной функции активации, что позволяет формировать иерархические представления данных – от простых признаков к более сложным [2]. Обучение нейронной сети заключается в подборе весовых коэффициентов, минимизирующих ошибку между предсказанным и истинным значением. Наиболее распространенным методом обучения является алгоритм обратного распространения ошибки, основанный на градиентном спуске [2, 3]. В зависимости от структуры данных и наличия разметки выделяют обучение с учителем, без учителя и с подкреплением [2]. Важной особенностью глубоких моделей является их способность к автоматическому извлечению признаков, что позволяет существенно сократить необходимость ручной инженерии признаков и повысить эффективность обработки сложных данных [2, 3].

Среди архитектур глубоких нейронных сетей особое значение имеют сверточные и рекуррентные модели. Сверточные нейронные сети широко применяются для обработки изображений благодаря способности учитывать пространственную структуру данных и извлекать устойчивые признаки независимо от положения объекта [2, 3]. Они используют операции свертки и подвыборки, что позволяет формировать карты признаков различного уровня абстракции. Рекуррентные нейронные сети, в свою очередь, предназначены для анализа последовательностей и

позволяют учитывать временные зависимости между элементами данных [3]. Их развитие привело к появлению моделей с долговременной памятью (LSTM), способных эффективно обрабатывать длинные последовательности [6]. Современные исследования также активно развивают архитектуры трансформеров, которые обеспечивают более эффективную обработку последовательных данных за счет механизма внимания [7].

Использование глубоких нейронных сетей в области информационной безопасности позволяет существенно повысить эффективность защиты корпоративных систем. Одним из ключевых направлений является обнаружение вредоносного программного обеспечения. В отличие от традиционных сигнатурных методов, нейросети способны выявлять ранее неизвестные угрозы на основе анализа поведения программ [4, 8]. Другим важным направлением является анализ сетевого трафика и обнаружение вторжений, где нейронные сети применяются для выявления аномалий в потоковых данных [9, 5]. Кроме того, глубокие модели используются для анализа поведения пользователей, позволяя выявлять отклонения от нормальной активности и тем самым обнаруживать внутренние угрозы и компрометацию учетных записей [4]. При этом следует учитывать уязвимость самих нейросетевых моделей к состязательным атакам (adversarial attacks), когда злоумышленник намеренно модифицирует входные данные, чтобы обойти систему защиты [10].

Задачи компьютерного зрения являются одной из наиболее перспективных областей применения глубокого обучения [2, 3, 11]. Человек и животные получают большую часть информации через зрительную систему, и аналогичный подход реализуется в машинах посредством технологий компьютерного зрения [3, 11]. Данные технологии позволяют автоматизировать процессы обнаружения объектов, классификации изображений и анализа поведения [2, 11]. С развитием глубокого обучения традиционные методы компьютерного зрения, требующие ручной настройки признаков, уступили место нейросетевым подходам, способным самостоятельно извлекать информативные характеристики из данных, что существенно повышает точность и надежность систем распознавания [2, 3].

В частности, при обработке фотографий для паспортных документов используются сверточные нейронные сети, способные анализировать визуальные характеристики изображения. В процессе обработки изображение проходит через последовательность слоев, на которых последовательно выделяются границы, текстуры и более сложные структуры, такие как элементы лица. Это позволяет автоматически проверять соответствие изображения установленным требованиям,

включая положение головы, освещенность и фон. Ключевым параметром эффективности модели является ее емкость, определяемая количеством слоев и параметров [2, 3]. Недостаточная емкость приводит к неспособности модели выявлять существенные признаки, тогда как избыточная емкость может вызвать переобучение [2, 3].

Глубокие нейронные сети представляют собой мощный инструмент анализа данных, позволяющий эффективно решать широкий спектр задач в области корпоративной защиты программного обеспечения. Их применение обеспечивает повышение уровня безопасности за счет автоматического выявления угроз и анализа сложных закономерностей в данных. В то же время использование глубоких моделей связано с рядом ограничений, включая высокие вычислительные затраты, необходимость больших объемов обучающих данных и сложность интерпретации результатов [2, 3].

Список использованных источников:

1. Созыкин А.В. Обзор методов обучения глубоких нейронных сетей // Вестник ЮУрГУ. 2017. Т. 6. № 3. С. 28–59.
2. Макаренко А.В. Глубокие нейронные сети: зарождение, становление, современное состояние // Проблемы управления. 2020. № 2. С. 3–7.
3. LeCun Y., Bengio Y., Hinton G. Deep learning // Nature. 2015. Vol. 521. P. 436–444.
4. Sarker I.H. Machine Learning for Intelligent Cybersecurity // Journal of Big Data. 2021.
5. Buczak A.L., Guven E. A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection // IEEE Communications Surveys & Tutorials. 2016.
6. Goodfellow I., Bengio Y., Courville A. Deep Learning. Cambridge: MIT Press, 2016.
7. Vaswani A. et al. Attention Is All You Need // NeurIPS. 2017.
8. Zhang Z., Li J., Man D. Deep Learning for Malware Detection: A Review // Computers & Security. 2023.
9. Apruzzese G. et al. Deep Learning for Cybersecurity: A Survey // IEEE Communications Surveys & Tutorials. 2018.
10. Chakraborty A., Alam M., Dey V. Adversarial Attacks and Defenses in Deep Learning for Cybersecurity // IEEE Access. 2024.
11. Feng X., Jiang Y., Yang X., et al. Computer vision algorithms and hardware implementations: a survey // Integration. 2019. Vol. 69. P. 309–320.

Galimova A.R.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Valeev S. S.
Ufa University of Science and Technology, Ufa

DEEP NEURAL NETWORKS. APPLICATION IN CORPORATE SOFTWARE PROTECTION SYSTEMS

Abstract. This article examines the structure and training methods of deep neural networks as a modern tool of machine learning. Particular attention is paid to the application of deep neural networks in corporate software protection systems, including malware detection, network traffic analysis, and biometric authentication. The paper also discusses the features of applying neural networks in computer vision tasks using the example of processing photographs for passport documents, including the concept of model capacity and its impact on recognition quality. Finally, the advantages and limitations of using neural networks for data processing in the field of information security are analyzed.

Keywords: deep neural networks, machine learning, artificial intelligence, information security, corporate protection, malware, computer vision, convolutional neural networks, model capacity, image recognition.

УДК 004.056

Диканский Д.А., Пронин В.И.
Северо-Кавказский федеральный университет, Ставрополь

Научный руководитель:
Петренко В.И.
Северо-Кавказский федеральный университет, Ставрополь

МЕТОД АДАПТИВНОГО ВЗВЕШИВАНИЯ ГОЛОСОВ В РАСПРЕДЕЛЕННЫХ СИСТЕМАХ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ В ИНТЕРНЕТЕ ДРОНОВ

Аннотация. Предложен метод адаптивного взвешивания голосов в распределенной системе обнаружения вторжений IoD. В отличие от простого большинства и схемы, учитывающей только текущее качество участника, метод использует кумулятивную оценку достоверности голоса с затуханием истории. Имитационное моделирование показало, что в сценарии со средним шумом точность итогового решения возрастает до

0,994 при одновременном снижении ложных срабатываний, пропуска вторжений и влияния недостоверных участников.

Ключевые слова: Интернет дронов, распределенная система обнаружения вторжений, голосование, достоверность, вторжения, кибербезопасность, адаптивное взвешивание.

В распределенных системах обнаружения вторжений Интернета дронов (IoD) итоговое решение формируется на основе локальных оценок нескольких участников, поэтому точность коллективного решения зависит не только от качества отдельного детектора, но и от устойчивости его поведения во времени [1–5]. В существующих работах рассматриваются кооперативные системы обнаружения вторжений для IoD, распределенные схемы выявления атак и методы повышения достоверности коллективных решений [2–5]. Вместе с тем задача адаптивного взвешивания голосов участников по накопленной истории корректности в распределенной системе обнаружения вторжений IoD остается недостаточно проработанной. В частности, ограниченно исследован вопрос о том, как учитывать не только текущее качество локального решения, но и устойчивость поведения участника на последовательности циклов наблюдения.

Целью работы является разработка метода адаптивного взвешивания голосов в распределенной системе обнаружения вторжений IoD на основе кумулятивной оценки достоверности участников голосования.

Рассматривается распределенная модель, в которой в каждом цикле имеется истинное состояние «норма / вторжение», а каждый участник формирует локальный бинарный голос. В эксперименте использовались четыре типа участников: надежные, шумные, нестабильные и вредоносные. Такое разделение позволяет воспроизвести как благоприятные условия функционирования системы, так и более сложные режимы, в которых часть участников систематически или эпизодически искажает локальные решения. В главном сценарии состав системы задавался как 8/5/4/4, а число циклов составляло 300.Предлагаемый метод основан на рекуррентном обновлении веса достоверности участника:

$$w_i(t+1) = \lambda w_i(t) + (1-\lambda) r_i(t),$$

где $w_i(t)$ – текущий вес голоса участника, λ – коэффициент памяти, $r_i(t) \in \{0,1\}$ – оценка корректности голоса по подтвержденной метке цикла. Тем самым недавние решения учитываются сильнее, история полностью не теряется.

Итоговое решение формируется по взвешенной сумме голосов:

$$V(t) = \frac{\sum_{i=1}^{N} w_i(t) v_i(t)}{\sum_{i=1}^{N} w_i(t)}.$$

Если $V(t) \geq \theta$, фиксируется вторжение, иначе принимается состояние нормы.

Для сравнения реализованы три схемы агрегирования: простое большинство, взвешивание по текущему качеству без памяти и предлагаемый метод кумулятивной достоверности. В качестве показателей использовались точность итогового решения, доля ложных срабатываний, доля пропуска вторжений, влияние недостоверных участников на итог и стабильность решения во времени. Такой набор показателей позволяет оценить не только общую точность обнаружения, но и устойчивость коллективного механизма голосования в условиях неоднородного состава участников.

Основные результаты для главного сценария приведены в табл. 1

Таблица 1

Результаты сравнения методов

Метод	Точность	Ложн. +	Ложн. -	Влияние	Разрыв	Стабиль-ность
Простое большинство	0,954	0,028	0,064	0,044	0,000	0,930
Качество без памяти	0,949	0,029	0,071	0,049	-0,002	0,926
Кумулятивная достоверность	0,994	0,005	0,008	0,006	0,032	0,990

Из табл. 1 следует, что предлагаемый метод обеспечивает наилучший результат по всем основным показателям главного сценария. По сравнению с простым большинством точность повышается с 0,954 до 0,994, доля ложных срабатываний уменьшается с 0,028 до 0,005, а доля пропуска вторжений – с 0,064 до 0,008. Кроме того, существенно снижается влияние недостоверных участников на итоговое решение. Это показывает, что накопление истории голосования позволяет надежнее отделять достоверных участников от нестабильных и вредоносных.

На рис. 1 представлено сравнение методов по основным показателям главного сценария. Видно, что схема кумулятивной достоверности превосходит оба базовых подхода не по одной отдельной метрике, а по совокупности показателей.

Дополнительный анализ показал, что по мере накопления истории средний вес надежных участников возрастает, тогда как совокупный вес нестабильных и вредоносных участников снижается, что обеспечивает повышение точности итогового коллективного решения. Тем самым механизм кумулятивной достоверности не только улучшает итоговую классификацию, но и формирует более устойчивую структуру коллективного голосования.

В контрольном сценарии с низким уровнем шума различия между методами практически не проявляются, тогда как в более сложных режимах преимущество предлагаемого метода становится устойчивым.

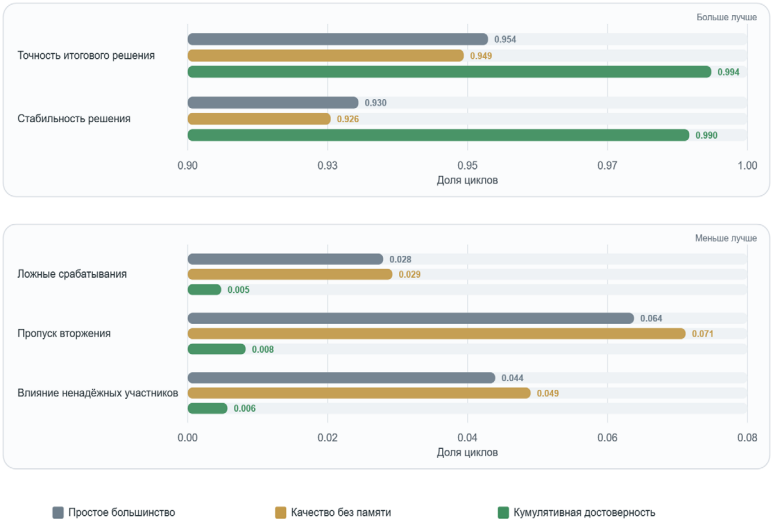


Рис. 1. Сравнение методов по основным показателям в главном сценарии: точность итогового решения, стабильность решения, ложные срабатывания, пропуск вторжения, влияние недостоверных участников

Таким образом, предложенный метод адаптивного взвешивания голосов позволяет повысить качество коллективного решения в распределенной системе обнаружения вторжений IoD за счет использования кумулятивной оценки достоверности участников. В отличие от мгновенного взвешивания, он учитывает историю корректности голосов и тем самым снижает влияние нестабильных и вредоносных детекторов. Ограничениями исследования являются синтетический характер модели, бинарная постановка и необходимость наличия подтвержденной правильной метки цикла после его завершения.

Список использованных источников:

1. Петренко В.И., Тебуева Ф.Б., Стручков И.В., Павлов А.С., Рябцев С.С. Метод доверенного взаимодействия агентов в децентрализованной киберфизической среде на основе технологии распределенного реестра // Прикаспийский журнал: управление и высокие технологии. 2023. № 2(50). С. 134-141. DOI: 10.21822/2073-6185-2023-50-2-134-141.

2. Wu M., Zhu Z., Xia Y., Yan Z., Zhu X., Ye N. A Q-Learning-Based Two-Layer Cooperative Intrusion Detection for Internet of Drones System // Drones. 2023. Vol. 7. No. 8. Art. 502. DOI: 10.3390/drones7080502.

3. Tlili F., Ayed S., Chaari Fourati L. Exhaustive distributed intrusion detection system for UAVs attacks detection and security enforcement (E-DIDS) // Computers & Security. 2024. Vol. 142. Art. 103878. DOI: 10.1016/j.cose.2024.103878.

4. Ramadan R., Emara A.H., Al-Sarem M., Elhamahmy M. Internet of Drones Intrusion Detection Using Deep Learning // Electronics. 2021. Vol. 10. No. 21. Art. 2633. DOI: 10.3390/electronics10212633.

5. Tsao K.-Y., Girdler T., Vassilakis V. A survey of cyber security threats and solutions for UAV communications and flying ad-hoc networks // Ad Hoc Networks. 2022. Vol. 133. No. 3. Art. 102894. DOI: 10.1016/j.adhoc.2022.102894.

Dikanskiy D.A., Pronin V.I.
North-Caucasus Federal University, Stavropol

Scientific supervisor:
Petrenko V.I.
North-Caucasus Federal University, Stavropol

METHOD FOR ADAPTIVE WEIGHTING OF VOTES IN DISTRIBUTED IOD INTRUSION DETECTION SYSTEMS

Abstract. A method for adaptive vote weighting in a distributed IoD intrusion detection system is proposed. Unlike majority voting and memoryless quality weighting, the method uses cumulative credibility with history decay. Simulation shows that in the medium-noise scenario the method increases final decision accuracy to 0.994 and simultaneously reduces false alarms, missed intrusions and the influence of unreliable participants.

Keywords: Internet of Drones, distributed IDS, voting, credibility, intrusion detection, cybersecurity, adaptive weighting.

УДК 004.056

Журавлева Ю.О., Шамсутдинова А.А.
Уфимский университет науки и технологий, Уфа

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

ПРИМЕНЕНИЕ МЕТОДОВ МАШИННОГО ОБУЧЕНИЯ ДЛЯ ОПРЕДЕЛЕНИЯ СПАМ-ПИСЕМ

Аннотация. В статье рассматривается применение методов машинного обучения для классификации спам-писем. Сравнивается качество таких моделей, как CatBoost, XGBoost, LGBoost, а также производится оценка значимости признаков.

Ключевые слова: машинное обучение, искусственный интеллект, спам-письма, CatBoost, XGBoost, LGBoost.

В современном мире все чаще наблюдается применение злоумышленниками методов социальной инженерии. К каналам социальной инженерии относятся социальные сети и мессенджеры, а также сервисы электронной почты. Например, согласно отчету Positive Technologies, электронная почта является каналом социальной инженерии в 88% случаев атак на организации в I-III квартале 2025 года [1].

Под спам-письмом не всегда подразумевается письмо, созданное злоумышленником с целью совершения атаки. В широком смысле спам – это массовая рассылка нежелательных сообщений лицам, не дававшим согласия на их получение. К спам-письмам относятся также рекламные рассылки, неправильно направленные письма. При этом в случае некорректной работы спам-фильтра, как спам могут определяться и полезные письма, такие, как верификационные коды.

Однако зачастую в спам попадают письма, содержащие вредоносное программное обеспечение или фишинговые письма. Это обстоятельство делает определение спам-писем очень важной задачей обеспечения информационной безопасности.

В статье рассматривается применение алгоритмов машинного обучения для определения спам-писем. Был использован набор данных, содержащий информацию об электронных письмах. В наборе данных содержалось 57 числовых признаков. Числовые признаки были распределены на 3 группы – признаки, измеряющие частоту слов (таких, как free, report, money и т.п.), частоту символов (рассматриваются 6 символов) и характеристики заглавных букв, такие, как средняя длина

непрерывной последовательности заглавных букв, размер самой длинной непрерывной последовательности заглавных букв и общее количество заглавных букв в письме. В качестве целевой была выбрана переменная, содержащая информацию о классе принадлежности электронного письма.

Для выполнения работы использовался датасет Spam Email Classification, размещенный на платформе Kaggle [2]. Объем записей составил 4601, из которых 1813 относились к спам-письмам. Произведено разбиение на обучающую и тестовую выборки. Размер обучающей выборки составил 67%, размер тестовой выборки – 33%.

При обучении модели были использованы такие алгоритмы машинного обучения, как Logistic Regression, Decision Tree, K Nearest Neighbors, SVM, CatBoost, XGBoost, LGBoost. Для оценки точности модели использовались метрики Accuracy, Precision, Recall, F1, ROC AUC, PR AUC, Specificity. Полученные значения метрик ROC AUC и PR AUC представлены на рис. 1

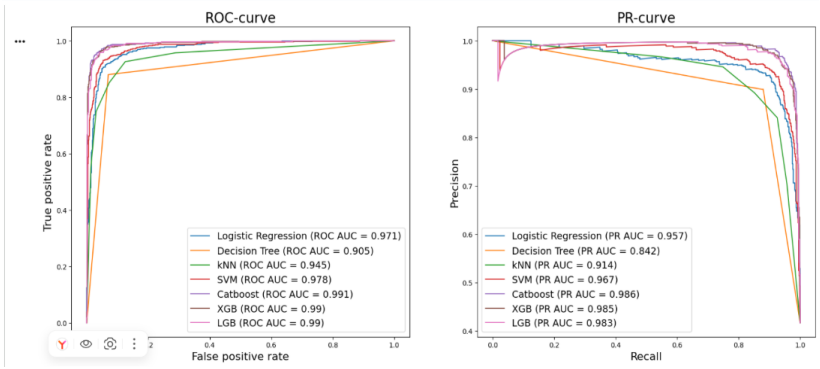


Рис. 1. Значения метрик ROC AUC и PR AUC

Была произведена оценка значимости признаков с использованием встроенного метода feature_importances_ библиотеки XGBoost. Такая оценка позволяет выявить наиболее важные признаки, указывающие на возможную опасность электронного письма.

В число наиболее значимых признаков вошли частота использования таких слов, как free, money. К наименее значимым признакам были отнесены средняя длина непрерывной последовательности заглавных букв и частота упоминании в тексте специальных символов.

Как показывают значения метрик (таблица 1), наилучшие результаты были достигнуты при использовании алгоритмов градиентного бустинга. Эти алгоритмы хорошо подходят для случаев нелинейной зависимости признаков, к которым относится определение спам-писем. Деревья

решений в свою очередь показывают низкие результаты, что может быть объяснено склонностью к переобучению, отсутствием ансамблирования и низкой обобщающей способностью модели.

Таблица 1

Результаты сравнения качества моделей

	Accuracy	Precision	Recall	F1_score	ROC AUC	PR AUC	Specificity
Logistic Regression	0.922	0.934	0.875	0.904	0.971	0.957	0.956
Decision Tree	0.908	0.899	0.877	0.888	0.905	0.842	0.930
kNN	0.895	0.892	0.852	0.871	0.945	0.914	0.927
SVM	0.934	0.945	0.893	0.918	0.978	0.967	0.963
xgb	0.955	0.952	0.939	0.946	0.990	0.985	0.966
lgb	0.955	0.954	0.937	0.946	0.989	0.983	0.968
catb	0.963	0.966	0.945	0.955	0.991	0.986	0.976

Таким образом, методы машинного обучения могут эффективно применяться для выявления потенциально опасных спам-писем. Наилучший результат при решении этой задачи показывают алгоритмы градиентного бустинга.

Список использованных источников:

1. Вяткина А., Осипова А. Актуальные киберугрозы: I–II кварталы 2025 года // Positive Technologies – URL: https://ptsecurity.com/research/analytics/aktual-nye-kiberugrozy-i-ii-kvartaly-2025-goda/#id1 (дата обращения 01.04.2026).

2. Spam Email Classification // Kaggle – URL: https://www.kaggle.com/datasets/somesh24/spambase (дата обращения 01.04.2026).

Zhuravleva I.O., Shamsutdinova A.A.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Yunusova D.S.
Ufa University of Science and Technology, Ufa

ARTIFICAL INTELLIGENCE SPAM EMAIL DETECTION TECHNOLOGY

Abstract. Article is dedicated to a problem of artificial intelligence spam email detection technology. The quality of models such as CatBoost, XGBoost, and LGBoost is compared, and the significance of features is evaluated.

Keywords: Machine learning, artificial intelligence, spam email, CatBoost, XGBoost, LGBoost.

УДК 004.056

Иванов Д.К.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Сенцова А.Ю.
Уфимский университет науки и технологий, Уфа

ОБНАРУЖЕНИЕ АНОМАЛИЙ В СЕТЕВОМ ТРАФИКЕ С ИСПОЛЬЗОВАНИЕМ ИЗОЛИРУЮЩЕГО ЛЕСА (ISOLATION FOREST) БЕЗ РАЗМЕЧЕННЫХ ДАННЫХ

Аннотация. Рассматривается применение алгоритма Isolation Forest для обнаружения аномалий в сетевом трафике без использования размеченных данных. Проведен эксперимент на датасете CIC-IDS-2017, выполнено сравнение с supervised-методами (Random Forest, XGBoost). Показано, что Isolation Forest эффективно выявляет аномалии (F1-score 0.74) и способен обнаруживать неизвестные типы атак, что является его ключевым преимуществом перед supervised-подходами.

Ключевые слова: Isolation Forest, обнаружение аномалий, сетевой трафик, обучение без учителя, CIC-IDS-2017.

Введение

Рост числа кибератак требует совершенствования, казалось бы, ранее эффективных методов обнаружения вторжений. Традиционные сигнатурные системы не могут обнаружить новые типы угроз (zero-day), которых нет в базах [1]. Методы машинного обучения с учителем (supervised) требуют размеченных данных, получение которых для всех типов атак затруднительно [2]. Размеченные данные – это набор записей, для которых заранее известен правильный ответ (метка класса). В контексте обнаружения вторжений метка указывает, является ли сетевой сеанс нормальным («доброкачественный» трафик) или атакой (DoS, Brute Force и т.д.). Основная проблема таких данных – высокая стоимость их получения: требуется ручная экспертиза, постоянное обновление базы известных атак и невозможность разметить заранее неизвестные угрозы (zero-day).

Цель настоящей работы состоит в экспериментальной оценке применимости алгоритма Isolation Forest для задачи обнаружения аномалий в сетевом трафике в отсутствие размеченной обучающей

выборки, а также в сравнительном анализе его эффективности с методами контролируемого обучения (Random Forest и XGBoost).

Алгоритм Isolation Forest

Isolation Forest (iForest) – метод обнаружения аномалий, ключевая идея которого заключается в том, что аномалии изолируются от остальных данных быстрее, чем нормальные наблюдения, за счет меньшего количества случайных разбиений [3].

Принцип работы алгоритма можно представить следующим образом:

– Строится множество случайных бинарных деревьев;

– Пространство признаков рекурсивно разбивается случайными значениями;

– Аномалии имеют короткие пути до изоляции, нормальные точки – длинные.

Аномальный скор принимает значения от 0 до 1. Он вычисляется на основе средней глубины изоляции точки в ансамбле случайных деревьев [3]. Значения, близкие к 1, указывают на аномалию (короткий путь изоляции), а близкие к 0 – на нормальное наблюдение (длинный путь).

Преимущества алгоритма заключаются в том, что он не требует размеченных данных, имеет линейную сложность $O(n \log n)$ и устойчив к многомерным данным [3].

Экспериментальная часть

Для эксперимента использован датасет CIC-IDS-2017, содержащий современные типы атак (DoS, DDoS, Brute Force, Web Attacks, Botnet) и нормальный трафик [4]. Метки классов используются только для оценки качества моделей.

Исходные данные для работы алгоритма:

– Из исходного набора отобрано 50 000 записей (25 000 – нормальный трафик, 25 000 – атаки);

– Из 80 признаков оставлены 20 числовых;

– Удалены дубликаты и строки с пропусками;

– Числовые признаки стандартизированы с помощью StandardScaler;

Эксперимент проведен на языке Python с использованием библиотек scikit-learn, XGBoost, pandas, numpy [5].

Методология:

– Обучение Isolation Forest (без использования меток классов) [3];

– Обучение Random Forest и XGBoost (с использованием меток) [6];

– Сравнение результатов по метрикам Accuracy, Precision, Recall, F1-score.

Результаты, полученные в ходе собственного эксперимента на выборке из 50 000 записей датасета CIC-IDS-2017.1 представлены в таблице 1:

Таблица 1

Сравнение моделей

Модель	Требует метки	Accuracy	Precision	Recall	F1-score
Isolation Forest	Нет	0.80	0.71	0.70	0.74
Random Forest	Да	0.90	0.88	0.85	0.88
XGBoost	Да	0.99	0.99	0.98	0.93

Для сравнения моделей использовались следующие метрики, измеряемые в долях единицы [5]:

– **Accuracy** (точность) – доля всех правильных ответов (истинно положительных + истинно отрицательных) среди всех примеров. Показывает общую эффективность, но может быть обманчива при дисбалансе классов.

– **Precision** (точность предсказания положительного класса) – доля верно обнаруженных аномалий среди всех объектов, отнесенных моделью к аномалиям. Отражает, насколько модель «ошибается ложными тревогами».

– **Recall** (полнота) – доля верно обнаруженных аномалий среди всех реальных аномалий. Показывает, сколько атак модель пропустила.

– **F1-score** – среднее гармоническое Precision и Recall. Применяется для несбалансированных данных, так как учитывает обе метрики одновременно.

Supervised-модели не распознают атаки, отсутствовавшие в обучающей выборке [2]. Isolation Forest выявляет любые отклонения от «нормального» поведения, что позволяет обнаруживать zero-day атаки [1].

Выводы по эксперименту:

– XGBoost и Random Forest точнее, но требуют размеченных данных [2];

– Isolation Forest уступает по метрикам, но работает без меток [3];

– Isolation Forest способен обнаруживать неизвестные типы атак [1].

Заключение

В ходе проведенного исследования выполнено сравнение Isolation Forest с supervised-методами Random Forest и XGBoost на датасете CIC-IDS-2017. Получены следующие основные результаты:

1. Supervised-методы (Random Forest, XGBoost) показали высокие результаты (F1-score 0.88 и 0.93 соответственно). Это обусловлено

использованием полной информации о метках классов в процессе обучения [6]. Однако такие модели принципиально не способны выявлять атаки, отсутствовавшие в обучающей выборке. Любая новая угроза (zero-day) остается для них нераспознанной [2].

2. Isolation Forest продемонстрировал F1-score 0.74 при полном отсутствии размеченных данных. Такой результат следует считать высоким, поскольку алгоритм обучается исключительно на статистических свойствах нормального трафика и не требует предварительного сбора примеров атак [3]. Он успешно выделил большинство аномалий, включая те, которые supervised-модели могли бы пропустить при отсутствии соответствующих примеров в обучении.

3. Ключевое преимущество Isolation Forest перед supervised-подходами – способность обнаруживать неизвестные типы атак. Это достигается за счет того, что алгоритм выявляет любые отклонения от «нормального» поведения, не пытаясь отнести их к заранее известным классам [1].

4. Наиболее эффективной стратегией является комбинирование обоих подходов. Целесообразно использовать Isolation Forest для выявления неизвестных аномалий (в том числе zero-day атак) и supervised-модели для точной классификации известных типов атак [2]. Такая гибридная схема позволяет одновременно достичь высокой точности на известных угрозах и сохранить чувствительность к новым.

Список использованных источников:

1. A Multi-stage based Approach for Zero-day Attack Detection // 2024 5th International Conference on Computer, Big Data and Artificial Intelligence (ICCBD+AI). – IEEE.

2. Chandola V., Banerjee A., Kumar V. Anomaly Detection: A Survey // ACM Computing Surveys. – 2009. – Т. 41, № 3. – С. 1–58.

3. Liu F. T., Ting K. M., Zhou Z. H. Isolation Forest // 2008 Eighth IEEE International Conference on Data Mining. – С. 413–422.

4. Sharafaldin I., Lashkari A. H., Ghorbani A. A. Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization // 4th International Conference on Information Systems Security and Privacy (ICISSP). – 2018. – С. 108–116.

5. Pedregosa F. et al. Scikit-learn: Machine Learning in Python // Journal of Machine Learning Research. – 2011. – Т. 12. – С. 2825–2830.

6. Chen T., Guestrin C. XGBoost: A Scalable Tree Boosting System // Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. – 2016. – С. 785–794.

Ivanov D.K.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Sentsova A.Yu.
Ufa University of Science and Technology, Ufa

DETECTION OF ANOMALIES IN NETWORK TRAFFIC USING ISOLATION FOREST WITHOUT LABELED DATA

Abstract. The article discusses the application of the Isolation Forest algorithm for detecting anomalies in network traffic without using labeled data. An experiment was conducted on the CIC-IDS-2017 dataset, and a comparison with supervised methods (Random Forest, XGBoost) was performed. It is shown that Isolation Forest effectively detects anomalies (F1-score 0.74) and is capable of detecting unknown types of attacks, which is its key advantage over supervised approaches.

Keywords: Isolation Forest, anomaly detection, network traffic, unsupervised learning, CIC-IDS-2017.

УДК 004.8

Клыгин В.О.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Валеев С.С.
Уфимский университет науки и технологий, Уфа

ПРИМЕНЕНИЕ СИСТЕМ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ПРИ ОБУЧЕНИИ ПЕРСОНАЛА ОСНОВАМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация. В статье рассматриваются подходы к обучению непрофильных сотрудников основам информационной безопасности. Описываются традиционные форматы повышения осведомленности персонала, их назначение и ограничения. Анализируется проблема фактически неверных ответов языковых моделей и технология Retrieval-Augmented Generation как способ ее решения. Приводятся рекомендации по составлению запросов при работе с нормативными документами. В качестве практического инструмента описывается система NotebookLM.

Ключевые слова: информационная безопасность, обучение персонала, осведомленность пользователей, генерация с дополненным извлечением, RAG, промпт-инжиниринг, NotebookLM.

Реальный вектор большинства успешных атак на компании проходит не через технические уязвимости, а через сотрудника, чья профессиональная задача не связана с безопасностью. Для специалистов непрофильных направлений цифровая среда остается привычным рабочим инструментом, а не источником угроз. Вопросы информационной безопасности (ИБ) в их профессиональной подготовке занимают в лучшем случае несколько лекций в рамках курса информатики. Задача по восполнению этого пробела возложена на подразделения ИБ.

В практике обучения персонала основам ИБ существует несколько форматов. Каждый из них решает свою задачу и имеет собственные ограничения.

Плакаты и заставки экранов формируют у сотрудников неосознанную готовность к распознаванию признаков угроз. Без активного участия с их стороны регулярно воспроизводимый визуальный образ постепенно закрепляется в восприятии.

Лекционные занятия и ознакомление с нормативными документами под роспись создают юридически значимый факт осведомленности и формируют общий понятия. При работе с объемными текстами сотрудники, как правило, демонстрируют низкую вовлеченность и быстро утрачивают усвоенные сведения.

Командно-штабные учения позволяют перейти от осведомленности к практическому действию. Сценарий развертывается в режиме реального времени, сотрудники разных подразделений вынуждены согласовывать решения, и в процессе обнаруживаются не только пробелы в знаниях, но и отсутствие регламентов, нераспределенная ответственность, непонимание порядка уведомления. Формат наиболее трудно организовать и при этом наиболее сложно заменить чем-либо иным.

Использование языковых моделей для поддержки обучения выглядит логичным ответом на описанные ограничения. Модель способна генерировать тесты, составлять сценарии учений, объяснять нормативные документы доступным языком. Но в контексте обучения этот инструмент несет определенный риск. Языковая модель не хранит знания в виде проверенной базы данных, а воспроизводит статистически вероятное продолжение текста на основании закономерностей в массиве обучающих данных.

Технология Retrieval-Augmented Generation (RAG) изменяет эту архитектуру. Перед формированием ответа система выполняет поиск по

проверенному массиву источников и передает языковой модели не только запрос пользователя, но и наиболее соответствующие ему фрагменты из загруженных источников. Применение RAG снижает частоту фактически неверных ответов на 40–60% по сравнению с генерацией без обращения к внешним источникам, при этом качество результата зависит от качества документальной базы [1].

Система, загруженная учебно-методическими материалами, разработанными на основе действующих нормативных актов, способна генерировать тесты и сценарии учений, не изобретая несуществующих требований. Работа с подобной системой ставит вопрос о грамотном составлении запросов. Большинство руководств сводят запрос к трем элементам: роль, контекст и задача. Официальная документация разработчиков современных языковых моделей содержит несколько принципов, которые редко встречаются в популярных пересказах [2].

Первый принцип требует размещать данные в начале запроса, а инструкции в конце: при работе с большими документами это дает прирост качества ответа до 30%.

Второй предписывает объяснять модели причину каждого условия, чтобы она распространяла логику на случаи, не предусмотренные явно.

Третий указывает на преимущество предписывающих формулировок перед запрещающими.

Четвертый закрепляет роль примеров, три-пять образцов в явно размеченных тегах точнее задают ожидаемую структуру, чем любое словесное описание. Ключевые из них представлены на рисунке 1.

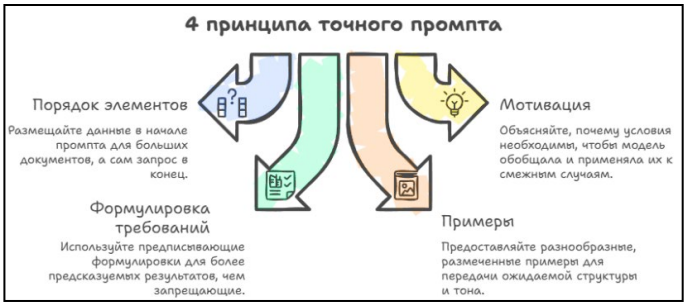


Рис. 1. Принципы составления запросов к языковой модели

NotebookLM реализует RAG-архитектуру в готовом решении без технической настройки. Система работает исключительно с загруженными пользователем документами, каждый ответ сопровождается ссылкой на конкретный фрагмент источника, а общие знания модели исключены из обработки запроса. Разработанные учебные материалы, методические пособия и внутренние регламенты,

загруженные в систему, позволяют сформировать тест, ответить на вопрос сотрудника в режиме диалога или подготовиться для проведения учений [3]. Интерфейс модели приведен на рисунке 2.

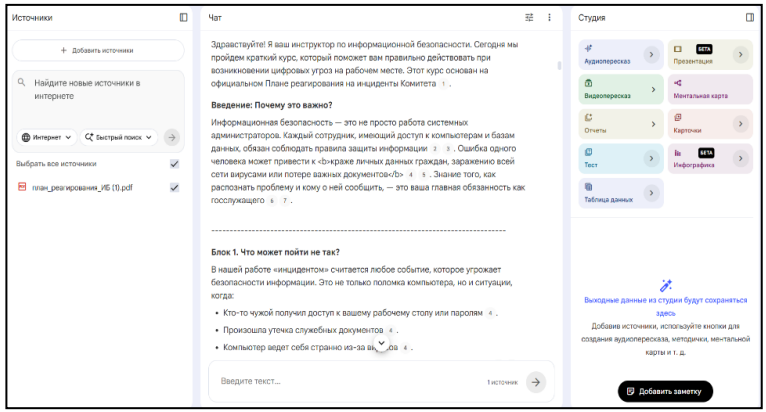


Рис. 2. Интерфейс системы NotebookLM при работе с учебными материалами

Устаревшие или неточные источники порождают некачественные материалы для обучения. Противопоставление традиционных форматов обучения инструментам на основе языковых моделей методологически некорректно. Плакаты, лекционные занятия и командно-штабные учения решают задачи, которые языковые модели не закрывают. Языковые модели делают масштабируемой ту часть обучения, которая требует персонализации и актуальности. Применение искусственного интеллекта без понимания природы неверных ответов и без обращения к проверенным источникам создает риск. NotebookLM снижает технический порог входа до минимума, однако не снимает с организации ответственности за актуальность документальной базы.

Список использованных источников:

1. Retrieval-augmented generation for educational application: A systematic survey // Computers and Education: Artificial Intelligence. 2025. URL: https://www.sciencedirect.com/science/article/pii/S2666920X25000578.

2. Anthropic. Prompting Best Practices for Claude's Latest Models. 2025. URL: https://platform.claude.com/docs/en/build-with-claude/prompt-engineering/claude-prompting-best-practices.

3. Google. NotebookLM: официальная справка. 2024. URL: https://support.google.com/notebooklm/?hl=ru.

Klygin V.O.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Valeev S.S.
Ufa University of Science and Technology, Ufa

ARTI APPLICATION OF ARTIFICIAL INTELLIGENCE SYSTEMS IN TRAINING PERSONNEL IN THE BASICS OF INFORMATION SECURITY

Abstract. The article examines approaches to information security training for non-specialist personnel. Traditional security awareness formats are described along with their purposes and limitations. The problem of factually incorrect outputs in large language models is analyzed, and Retrieval-Augmented Generation is considered as a means of addressing it. Recommendations for prompting language models when working with regulatory documents are provided. NotebookLM is described as a practical implementation tool.

Keywords: information security, personnel training, security awareness, retrieval-augmented generation, RAG, prompt engineering, NotebookLM.

УДК 004.056

Ларичев Р.С.
Поволжский государственный университет
телекоммуникаций и информатики, Самара

Научный руководитель:
Поздняк И.С.
Поволжский государственный университет
телекоммуникаций и информатики, Самара

LLM-АССИСТЕНТ ДЛЯ THREAT HUNTING

Аннотация. В статье рассматривается проблема ав томатизации в Threat Hunting. Предложена архитектура LLM-ассистента, который на основе оценки актуальности индикаторов компрометации (IoC), данных SIEM и матрицы MITRE ATT&CK генерирует проверяемые гипотезы. Описан сценарий работы, приведены примеры гипотез. Показано, что использование LLM сокращает время выдвижения гипотез с минут до нескольких секунд.

Ключевые слова: Threat Hunting, индикаторы компрометации, IoC, MITRE ATT&CK, LLM, SIEM, генерация гипотез, автоматизация.

Threat Hunting – это процесс активного поиска и обнаружения скрытых угроз в сети или системе, который помогает пользователю лучше понимать угрозы, с которыми он столкнулся. В отличие от традиционных систем обнаружения вторжений, которые реагируют на уже известные сигнатуры, Threat Hunting предполагает выдвижение и проверку гипотез о том, как злоумышленники могли бы проникнуть в инфраструктуру. Этот подход позволяет находить угрозы, способные обходить стандартные средства защиты, но требует высокой квалификации аналитиков и значительных временных затрат [1].

Одновременно с этим индикаторы компрометации (IoC) быстро теряют свою актуальность. Злоумышленники постоянно меняют тактики и техники, модифицируют вредоносное ПО, меняют IP-адреса и домены. Использование устаревших IoC приводит к ложным срабатываниям и снижает эффективность защиты. Для оценки актуальности индикаторов применяется функция старения, учитывающая надежность источника и время, прошедшее с момента последнего обнаружения [2].

Матрица MITRE ATT&CK предоставляет систематизированную базу знаний о тактиках, техниках и процедурах, используемых злоумышленниками. Она помогает аналитикам понимать контекст атак и выбирать соответствующие индикаторы для выявления угроз. Однако применение матрицы остается преимущественно ручным, что ограничивает ее потенциал в условиях быстро меняющейся ландшафта угроз [3].

В этих условиях возникает задача автоматической генерации гипотез для Threat Hunting на основе трех компонентов: актуальных IoC, событий из SIEM-системы и знаний из MITRE ATT&CK. Решением может стать использование больших языковых моделей (LLM), таких как ChatGPT, DeepSeek или локальных аналогов, способных анализировать разные данные и формулировать связные гипотезы.

Предлагаемая архитектура LLM-ассистента включает четыре модуля. Первый модуль – фильтрация. IoC отбрасывает индикаторы с низкой оценкой актуальности и сортирует оставшиеся по убыванию значимости. Оценка актуальности вычисляется по формуле:

$$scorea = basescorea \times \left(1 - \left(\frac{t}{t(\alpha)} \right)^{\frac{1}{\delta\alpha}} \right),$$

где, *base_score* зависит от надежности источника,
decay_rate – скорость устаревания,
T(t) – текущее время,

T(t-1) – время последнего обнаружения [2].

Второй модуль – сопоставление данных на MITRE ATT&CK. Для каждого выбранного IoC определяется связанные с ним тактики и техники. Например, известный C2-сервер сопоставляется с тактикой Command and Control (TA0011) и техникой T1071 (Application Layer Protocol).

Третий модуль заключается в контекстном запросе к LLM модели. Она формирует промпт, содержащий список IoC с оценками актуальности, выдержку из SIEM-событий и инструкцию для генерации гипотез.

Четвертый модуль – процесс проверки и подтверждения правильности гипотез. Сгенерированные гипотезы передаются аналитику для подтверждения или отклонения, а обратная связь с LLM используется для уточнения промптов.

Рассмотрим пример работы системы. SIEM-система фиксирует несколько обращений к IP-адресу 185.130.5.253 за последние два часа. Данный IP имеет базовую оценку 80 (источник – платный Threat Intelligence-фид), скорость устаревания 0.05, возраст 10 дней. По базе MITRE этот IP связан с техникой T1071. Также SIEM показывает аномальный рост исходящего трафика на порт 443 с трех внутренних хостов.

LLM-ассистент на основе этих данных генерирует следующую гипотезу: «Хосты 192.168.1.45, 192.168.1.67 и 192.168.1.89 могут быть скомпрометированы и использовать IP 185.130.5.253 в качестве C2-сервера. Техника MITRE: T1071. Что проверить: изучить полные дампы DNS-запросов с этих хостов, а также временные паттерны исходящих соединений (периодичность каждые 60 секунд). Приоритет: высокий. Правило для SIEM: *SELECT src_ip, dst_ip, COUNT(*) FROM connections WHERE dst_ip = '185.130.5.253' GROUP BY src_ip HAVING COUNT(*) > 10»*. Аналитик проверяет гипотезу и находит подтверждение: исходящие HTTPS-запросы с трех хостов на C2-сервер повторяются строго каждые 60 секунд, что соответствует поведению beacon-модуля Cobalt Strike. Время на формулировку гипотезы сокращается с 20–30 минут до 30 секунд.

Несмотря на очевидные преимущества, LLM-ассистент имеет ограничения. Модели могут придумывать несуществующие связи между IoC и техниками MITRE. Эта проблема частично решается за счет связывания данных во втором модуле, который выполняется не LLM, а по заранее составленной базе. Также система чувствительна к формулировке промпта и зависит от качества данных, поступающих из SIEM. При неполных логах возрастает вероятность ложных гипотез. Кроме того, использование LLM в реальном времени требует вычислительных

ресурсов (GPU или API-доступа), что может быть ограничением для небольших организаций. Важно подчеркнуть, что LLM не заменяет аналитика, а выступает в роли ассистента, ускоряя рутинную часть работы – поиск связей и генерацию первичных гипотез.

Применение LLM-ассистента дает организациям ряд преимуществ. Сокращается время реагирования на инциденты за счет автоматизации начального этапа Threat Hunting. Снижается порог входа для младших специалистов, которые получают готовые гипотезы для проверки. Автоматически связываются устаревающие индикаторы с актуальными тактиками атак из MITRE ATT&CK. Кроме того, система может предлагать не только гипотезы, но и проекты детектирующих правил, что ускоряет внедрение новых методов обнаружения.

В заключение следует отметить, что искусственный интеллект, в частности большие языковые модели, открывает новые возможности для автоматизации Threat Hunting. Предложенная архитектура LLM-ассистента объединяет оценку актуальности IoC, сопоставление данных на MITRE ATT&CK и генерацию проверяемых гипотез на основе событий SIEM. Такой подход позволяет оперативно выявлять скрытые угрозы на ранних стадиях и минимизировать потенциальный ущерб. Дальнейшими направлениями развития являются дообучение LLM по реальным отчетам аналитиков об инцидентах, интеграция с SOAR-платформами для автоматического запуска проверок, а также создание динамической оценки скорости устаревания IoC на основе глобальной телеметрии.

Список использованных источников:

1. Threat Hunting в действии / [Электронный ресурс] // CYBERPOLYGON: [сайт] – URL: https://cyberpolygon.com/ru/materials/threat-hunting-in-action/ (дата обращения: 18.04.2026).

2. Ларичев Р.С., Поздняк И.С. статья «Как оценить актуальность индикаторов компрометации» / [Электронный ресурс] // LI Самарская областная студенческая научная конференция: [сайт] – https://journals.eco-vector.com/osnk-sr2025/article/view/680757 // (дата обращения: 18.04.2026).

3. MITRE ATT&CK Framework / [Электронный ресурс] // MITRE: [сайт] – URL: https://attack.mitre.org (дата обращения: 18.04.2026).

Larichev R.S.
Povolzhskiy State University of
Telecommunications and Informatics, Samara

Scientific supervisor:
Pozdnyak I. S.
Povolzhskiy State University of
Telecommunications and Informatics, Samara

LLM-ASSISTANT FOR THREAT HUNTING

Abstract. The article addresses the problem of Threat Hunting automation – active search for hidden threats in information systems. An architecture of an LLM assistant is proposed, which generates testable hypotheses based on the assessment of indicator of compromise (IoC) relevance, SIEM data, and the MITRE ATT&CK matrix. A working scenario is described, and an example of a hypothesis with a detection rule is given. It is shown that using LLM reduces hypothesis generation time from tens of minutes to seconds

Keywords: Threat Hunting, indicators of compromise, IoC, MITRE ATT&CK, LLM, SIEM, hypothesis generation, automation.

УДК 004.4: 519.7

Мансурова А.Р.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Валеев С.С.
Уфимский университет науки и технологий, Уфа

ПРИМЕНЕНИЕ РЕКУРРЕНТНЫХ НЕЙРОННЫХ СЕТЕЙ В СИСТЕМЕ КОРПОРАТИВНОЙ ЗАЩИТЫ

Аннотация. Статья рассматривает возможности применения рекуррентных нейронных сетей (RNN) для усиления корпоративной защиты. Анализируются архитектурные особенности RNN, их способность обрабатывать временные зависимости и качество видеопотока. Приводятся результаты применения RNN для обнаружения аномалий в поведении, анализа видеоданных и интеграции с системами физической безопасности. Обсуждаются правовые аспекты обработки данных нейросетями.

Ключевые слова: рекуррентные нейронные сети, корпоративная защита, LSTM, анализ видеопотока, информационная безопасность, персональные данные.

Современные корпоративные системы защиты сталкиваются с необходимостью обработки больших объемов временных данных – от сетевого трафика до видеопотоков с камер наблюдения [1]. Традиционные методы, основанные на сигнатурном анализе и статических правилах, демонстрируют ограниченную эффективность при обнаружении сложных атак и аномального поведения. Внедрение методов глубокого обучения, в частности рекуррентных нейронных сетей (RNN), становится необходимым элементом эшелонированной защиты предприятия [2, 1].

Рекуррентные нейронные сети – класс нейронных сетей с обратными связями, благодаря которым они обладают собственной динамикой и «памятью» [1]. В отличие от сетей прямого распространения, RNN учитывают последовательный характер данных, что делает их незаменимыми для анализа временных рядов и видеопотоков [1]. Наличие обратных связей позволяет накапливать информацию и использовать ее при обработке сигналов, при этом порядок следования сигналов играет существенную роль в решаемой задаче [1].

Применительно к видеопотоку RNN способны извлекать пространственно-временные признаки, что особенно важно для систем безопасности [3]. Исследования показывают, что архитектуры, сочетающие сверточные и рекуррентные слои, позволяют не только выявлять аномальные действия, но и адаптироваться к различным условиям съемки, что делает их незаменимыми в реальных системах безопасности [4].

Наиболее значимым преимуществом RNN является обработка временной динамики. Для задачи обнаружения подозрительного поведения RNN анализируют последовательности кадров, выявляя паттерны, которые могут указывать на потенциальную угрозу [3]. Экспериментальные данные показывают, что RNN-алгоритмы демонстрируют точность обнаружения событий до 96%, что существенно превышает показатели традиционных методов [2].

Важным направлением является применение RNN для повышения качества видеопотока. При использовании сжатия с потерями, характерного для большинства систем видеонаблюдения, рекуррентные архитектуры способны восстанавливать утраченные детали, что критически важно для идентификации лиц и номерных знаков [1]. Анализ различных архитектур RNN для решения задач классификации объектов в видеопотоке показывает, что выбор архитектуры существенно влияет как

на скорость обучения сети, так и на точность и уровень ошибок полученной модели [1]. Кроме того, RNN могут применяться для интерполяции пропущенных кадров и шумоподавления, что особенно актуально при работе в условиях низкой освещенности или при использовании устаревшего оборудования [3].

Интеграция RNN в корпоративную систему безопасности предполагает решение двух ключевых задач: анализ сетевого трафика и обработку видеоданных [2, 1]. Используемая архитектура сочетает рекуррентные нейронные сети для обработки временных зависимостей в данных и сверточные нейронные сети для анализа изображений с систем видеонаблюдения [2]. Такой подход позволяет не только детектировать киберугрозы, но и идентифицировать нарушителей по их лицам, сравнивая изображения с базой данных организации [1].

Архитектурно RNN могут быть разделены на глобально рекуррентные и локально рекуррентные [1]. Для задач видеоаналитики особый интерес представляют сети с долгой краткосрочной памятью (LSTM), способные эффективно обучаться долгосрочным зависимостям в последовательностях данных и распознавать действия в видеопотоках [2, 1].

При развертывании RNN-систем необходимо учитывать требования Федерального закона № 152-ФЗ «О персональных данных» [5]. Видеонаблюдение с идентификацией личности по биометрическим признакам требует письменного согласия субъекта [5]. Обработка данных должна осуществляться с соблюдением принципов минимизации и конфиденциальности [5].

Важным аспектом является робастность нейросетевых моделей. ГОСТ Р ИСО/МЭК 24029-2-2024 устанавливает методологию оценки устойчивости нейронных сетей к искажениям и атакам [6]. Стандарт определяет способы проверки нейронных сетей с помощью формальных методов на каждой стадии жизненного цикла системы ИИ [6]. Система видеонаблюдения должна сохранять работоспособность при изменении условий съемки, а детектор аномалий – противостоять попыткам обхода [3, 6].

Перспективным направлением является интеграция RNN-аналитики с SIEM-платформами и системами контроля доступа [2, 1]. Комплексный подход, объединяющий технические и организационные меры защиты, позволяет выстроить эшелонированную систему безопасности, устойчивую к актуальным киберугрозам [2, 1].

Список использованных источников:

1. Чуб В.С. Использование рекуррентных нейронных сетей для анализа временных рядов и выявления тенденций в данных //

Образовательные ресурсы и технологии. – 2024. – № 2 (47). – С. 91–102. – DOI: 10.21777/2500-2112-2024-2-91-102. – URL: https://vestnik-muiv.ru/article/ispolzovanie-rekurrentnykh-neyronnykh-setey-dlya-analiza-vremennykh-ryadov-i-vyyavleniya-tendentsiy-/ (дата обращения: 12.04.2026). – Текст: электронный.

2. Real-Time Intelligent Video Surveillance System using Recurrent Neural Network // Procedia Computer Science. – 2024. – Vol. 233. – P. 819–828. – DOI: 10.1016/j.procs.2024.04.143. – URL: https://www.sciencedirect.com/science/article/pii/S1877050924008196 (дата обращения: 12.04.2026). – Текст: электронный.

3. Шведов И.А., Белов Ю.С. Применение глубокого обучения для распознавания аномалий в поведении человека на видеозаписях // Наукоемкие технологии в приборо- и машиностроении и развитие инновационной деятельности в вузе : материалы Всероссийской научно-технической конференции, Калуга, 19–21 ноября 2025 г. – М.: Изд-во МГТУ им. Н. Э. Баумана, 2025. – Т. 2. – С. 21–24. – URL: https://library.bmstu.ru/Catalog/Details/596845 (дата обращения: 12.04.2026). – Текст: электронный.

4. 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.

5. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (ред. от 24.06.2025). – URL: https://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения: 12.04.2026). – Текст: электронный.

6. ГОСТ Р ИСО/МЭК 24029-2-2024. Оценка робастности нейронных сетей. – М.: Росстандарт, 2024. – URL: https://docs.cntd.ru/document/1310068306 (дата обращения: 12.04.2026). – Текст: электронный.

Mansurova A. R.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Valeev S.S.
Ufa University of Science and Technology, Ufa

APPLICATION OF RECURRENT NEURAL NETWORKS IN THE CORPORATE SECURITY SYSTEM

Abstract. The article examines the possibilities of applying recurrent neural networks to enhance corporate security. Architectural features of RNN, their ability to process temporal dependencies and video stream quality are analyzed. The results of using RNN for anomaly detection in behavior, video data analysis and integration with physical security systems are presented. Legal aspects of data processing by neural networks are discussed.

Keywords: recurrent neural networks, corporate security, LSTM, video stream analysis, information security, personal data.

УДК 004.056

Митянин К.А., Пицин К.С.
Поволжский государственный университет
телекоммуникаций и информатики, Самара

Научный руководитель:
Новикова Д.Д.
Поволжский государственный университет
телекоммуникаций и информатики, Самара

ИСПОЛЬЗОВАНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В КИБЕРБЕЗОПАСНОСТИ

Аннотация. В статье рассматриваются современные подходы к применению искусственного интеллекта в области кибербезопасности. Проанализированы основные направления использования ИИ, включая обнаружение аномалий, анализ вредоносного программного обеспечения и автоматизацию реагирования на инциденты. Проведено сравнение традиционных и интеллектуальных методов защиты информации. Выявлены преимущества и ограничения использования ИИ в обеспечении информационной безопасности.

Ключевые слова: искусственный интеллект, кибербезопасность, защита информации, машинное обучение, кибератаки, IDS/IPS, SIEM, вредоносное ПО

Искусственный интеллект в последние годы становится одним из наиболее значимых инструментов в сфере кибербезопасности, поскольку современные информационные системы сталкиваются с постоянно растущим количеством угроз. Увеличение объемов передаваемых данных, развитие цифровых сервисов и усложнение способов кибератак требуют применения более гибких и точных механизмов защиты. В таких условиях традиционные средства информационной безопасности уже не всегда способны своевременно выявлять новые типы атак, особенно если они не имеют заранее известных признаков или сигнатур.

Актуальность применения искусственного интеллекта в кибербезопасности связана с тем, что интеллектуальные системы способны анализировать большие массивы информации, выявлять скрытые закономерности и обнаруживать подозрительную активность на ранних этапах. В отличие от классических методов защиты, которые чаще всего ориентированы на уже известные угрозы, методы машинного обучения позволяют формировать представление о нормальном поведении пользователей, сетевых узлов и программных процессов. При появлении отклонений от такой модели система может определить потенциальную угрозу и передать данные для дальнейшего анализа.

Одним из важных направлений использования искусственного интеллекта является обнаружение аномалий в сетевой активности. Подобные технологии позволяют выявлять нестандартные подключения, резкое увеличение объема передаваемых данных, необычное поведение пользователей или попытки несанкционированного доступа. Это особенно важно при защите корпоративных сетей, где атака может развиваться постепенно и долгое время оставаться незаметной для традиционных средств мониторинга.

Искусственный интеллект также активно применяется при анализе вредоносного программного обеспечения. Если классические антивирусные решения в значительной степени зависят от баз сигнатур, то интеллектуальные методы способны оценивать поведение программы, ее структуру и характер выполняемых действий. Благодаря этому появляется возможность выявлять новые или модифицированные вредоносные программы, которые еще не были добавлены в антивирусные базы. Такой подход повышает вероятность раннего обнаружения угроз и снижает риск успешного заражения информационной системы.

Отдельное значение имеет использование искусственного интеллекта в системах IDS, IPS и SIEM. В таких решениях ИИ помогает быстрее обрабатывать события безопасности, сопоставлять данные из разных источников и выделять наиболее опасные инциденты. Это снижает нагрузку на специалистов по информационной безопасности, поскольку им не приходится вручную анализировать весь поток уведомлений. Кроме того, интеллектуальные алгоритмы могут использоваться для автоматизации первичного реагирования, например для блокировки подозрительных действий, ограничения доступа или изоляции потенциально опасных узлов сети.

Важным направлением применения искусственного интеллекта является противодействие социальной инженерии. Алгоритмы машинного обучения анализируют электронные письма, сообщения и поведение пользователей, выявляя признаки фишинга, мошеннических рассылок и попыток получения конфиденциальной информации. Поскольку такие атаки часто направлены на человеческий фактор, ИИ повышает уровень защиты за счет анализа коммуникаций, подозрительных ссылок, вложений и отклонений от привычного поведения пользователя.

Несмотря на широкие возможности искусственного интеллекта, традиционные методы защиты сохраняют свое значение. Классические подходы проще внедрять, они дешевле и понятнее по принципу работы. Они эффективны против известных угроз, но хуже справляются с новыми и сложными атаками, не имеющими заранее определенных признаков или сигнатур. Поэтому традиционные средства безопасности применяются в организациях вместе с антивирусами, межсетевыми экранами и системами контроля доступа.

Методы на основе искусственного интеллекта позволяют быстрее анализировать большие объемы данных, выявлять скрытые закономерности и обнаруживать неизвестные ранее угрозы. Такие системы оценивают поведение пользователей, сетевых узлов и программных процессов, а также находят отклонения от нормальной активности. Например, ИИ может заметить нетипичное подключение, резкое увеличение объема передаваемых данных или необычную последовательность действий, указывающую на подготовку атаки.

В то же время применение ИИ в кибербезопасности имеет ограничения. Для эффективной работы таких систем нужны качественные обучающие данные, регулярное обновление моделей и грамотная настройка алгоритмов. Внедрение подобных решений может требовать значительных финансовых и технических ресурсов. Также возможны ложные срабатывания или неправильная интерпретация результатов, особенно при использовании неполных или устаревших

данных. Поэтому решения на основе ИИ должны применяться под контролем специалистов.

Таким образом, искусственный интеллект является важным элементом развития современных систем кибербезопасности. Он повышает скорость обработки данных, улучшает обнаружение угроз, автоматизирует часть процессов реагирования и снижает влияние человеческого фактора. Наиболее эффективным вариантом остается сочетание традиционных методов, интеллектуальных технологий и профессиональной работы специалистов. Такой комплексный подход позволяет создать более устойчивую систему защиты, способную противостоять современным киберугрозам.

Для оценки различий между классическими и интеллектуальными подходами можно сопоставить их по нескольким основным критериям.

Таблица 1

Различия между классическими и интеллектуальными подходами

Критерий	Традиционные методы	Методы на основе ИИ
Обнаружение новых угроз	Низкое	Высокое
Скорость анализа	Средняя	Высокая
Зависимость от человека	Высокая	Низкая
Ложные срабатывания	Возможны	Возможны
Стоимость внедрения	Низкая	Высокая

Список использованных источников:

1. Russell S., Norvig P. Artificial Intelligence: A Modern Approach. - 2021.
2. Касперский Е. Современные угрозы кибербезопасности. - М., 2022.
3. Goodfellow I. Deep Learning. - 2020.
4. Федеральный закон №152-ФЗ «О персональных данных».

Mityanin K.A., Pitsin K.S.
Povolzhskiy State University of
Telecommunications and Informatics, Samara

Scientific supervisor:
Novikova D.D.
Povolzhskiy State University of
Telecommunications and Informatics, Samara

APPLICATION OF ARTIFICIAL INTELLIGENCE IN CYBERSECURITY

Abstract. The paper examines modern approaches to the application of artificial intelligence in cybersecurity. The main areas of AI usage, including anomaly detection, malware analysis, and incident response automation, are analyzed. A comparison of traditional and intelligent information protection methods is carried out. The advantages and limitations of using AI in ensuring information security are identified.

Keywords: artificial intelligence, cybersecurity, information security, machine learning, cyberattacks, IDS/IPS, SIEM, malware

УДК 004.056

Насртдинов А.С.
Уфимский университет науки и технологий, Уфа

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

ИСПОЛЬЗОВАНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ДЛЯ ПРОГНОЗИРОВАНИЯ УГРОЗ БЕЗОПАСНОСТИ: ОПЫТ ВНЕДРЕНИЯ ПРОГНОЗНЫХ МОДЕЛЕЙ В КОРПОРАТИВНОЙ СРЕДЕ

Аннотация. Рассматривается применение технологий искусственного интеллекта (ИИ) для прогнозирования угроз информационной и физической безопасности. Описаны технические возможности: анализ поведенческих аномалий, прогнозирование атак на основе машинного обучения, раннее выявление инцидентов. Без надлежащего нормативного и этического сопровождения эффективность снижается. Предложен подход на основе гибридных моделей, адаптивного обучения и прозрачности алгоритмов. Смена реактивной

логики на предиктивную повышает защищенность и снижает операционные риски.

Ключевые слова: искусственный интеллект, прогнозирование угроз, информационная безопасность, машинное обучение, поведенческий анализ, предиктивная аналитика, аномалии, защита информации.

Традиционные системы безопасности реагируют на уже произошедшие инциденты: блокируют атаку после ее начала или фиксируют факт утечки. Однако большинство критических событий можно предотвратить, если выявлять их предвестники на ранней стадии. Технологии искусственного интеллекта позволяют перейти от реактивной модели к предиктивной – прогнозировать угрозы до того, как они реализуются.

Прогнозные модели на основе ИИ анализируют массивы данных из систем контроля доступа, DLP, журналов событий, камер наблюдения и поведения пользователей в корпоративной сети. На основе методов машинного обучения (градиентный бустинг, рекуррентные нейронные сети, автоэнкодеры) система выявляет паттерны, предшествующие инцидентам.

Основные технические возможности включают:

1. Анализ поведенческих аномалий**,** ИИ изучает нормальное поведение каждого сотрудника и системы в целом. Отклонения (например, попытки доступа в нерабочее время, несвойственное копирование большого объема данных, подозрительные сетевые запросы) интерпретируются как потенциальные индикаторы угрозы.

2. Прогнозирование внутренних утечек на основе истории действий пользователей. Модель вычисляет вероятность того, что конкретный сотрудник попытается вывести конфиденциальные данные. Факторами выступают: недавние неудачные попытки входа, нехарактерный трафик, эмоциональное состояние (при интеграции с анализом текстов переписки).

3. Предсказание целевых атак. Алгоритмы выявляют подготовительные этапы атак – разведку, сканирование портов, фишинговые рассылки. Система прогнозирует наиболее вероятные цели и векторы атаки за 1–2 часа до активной фазы.

Пример из практики: в финансовой организации была внедрена модель на основе графовых нейронных сетей. За шесть месяцев система предсказала 78 % попыток несанкционированного доступа и 63 % потенциальных утечек за 20–40 минут до их совершения. Ложноположительные срабатывания составили менее 5 % после адаптации.

Для работы прогнозных моделей требуется вычислительный кластер с GPU (например, NVIDIA A10 или аналоги), хранилище данных объемом от 10 ТБ для накопления событий за 6–12 месяцев, потоковый процессор событий (Apache Kafka). Модели обучаются на исторических инцидентах и переобучаются ежемесячно. Поддерживаются операционные системы Linux (Ubuntu 22.04) и Windows Server 2022.

Классические системы корреляции событий (SIEM) работают на статичных правилах. ИИ-прогнозирование не требует жестких сигнатур – оно само находит новые, ранее неизвестные паттерны. В отличие от детерминированных правил, машинное обучение способно предсказывать события, для которых еще не написано ни одного правила.

Использование ИИ для прогнозирования угроз связано с обработкой больших объемов персональных данных, в том числе биометрических и поведенческих. Согласно Федеральному закону от 27.07.2006 № 152-ФЗ «О персональных данных», для такой обработки требуется либо согласие субъекта, либо иное законное основание. Статья 22 Трудового кодекса РФ допускает контроль за действиями работников, но не конкретизирует методы прогнозирования.

Ключевые требования для законного внедрения:

- Письменное согласие сотрудников на анализ их цифрового поведения с целью прогнозирования инцидентов.
- Прозрачность алгоритмов: работник должен иметь возможность запросить объяснение, почему система предсказала от него угрозу (это согласуется с требованиями ст. 22 Федерального закона от 02.12.2019 № 503-ФЗ об экспериментальных правовых режимах в сфере ИИ).
- Запрет на принятие автоматизированных решений, ухудшающих положение сотрудника, без участия человека (рекомендации ОЭСР и проект Кодекса этики ИИ в России).
- Регулярный аудит моделей на систематические ошибки и дискриминацию.

На практике большинство организаций ограничиваются внутренними регламентами и дополнительными соглашениями к трудовому договору, где перечисляются цели прогнозирования (защита конфиденциальной информации, предотвращение атак) и перечень анализируемых параметров.

Рекомендуемый подход: гибридное прогнозирование с прозрачностью

Вместо использования ИИ как «черного ящика» для наказания предлагается подход, основанный на профилактике и вовлечении персонала.

1. Во время адаптивного обучение моделей на группах риска**,** новые сотрудники проходят 2-недельный период полного мониторинга с

интерпретируемым выводом системы. Опытным сотрудникам система выдает только агрегированные подсказки о потенциальных рисках.

2. Ежемесячно проходит разбор прогнозов о самых вероятных, но не реализовавшихся угрозах анализируются совместно с ИТ-отделом и персоналом. Это формирует культуру безопасности, а не страх.

3. Каждый сотрудник имеет право на объяснение, если его поведение классифицировано как угроза (высокий риск утечки), вправе получить от системы факторы, повлиявшие на прогноз. Это повышает доверие и снижает сопротивление.

Использование искусственного интеллекта для прогнозирования угроз безопасности позволяет организациям перейти от ликвидации последствий к предотвращению инцидентов. Технические возможности – выявление аномалий, предсказание утечек и атак, ранжирование уязвимостей – уже доказали эффективность в пилотных проектах. Однако без юридического и этического сопровождения (согласие сотрудников, прозрачность алгоритмов, запрет автоматических санкций) прогнозные модели могут вызывать отторжение и приводить к дискриминации. Предложенный гибридный подход, сочетающий машинное обучение с человеческим контролем и элементами прозрачности, превращает ИИ из инструмента тотальной слежки в средство повышения коллективной защищенности.

Список использованных источников:

1. Конституция Российской Федерации. Принята всенародным голосованием 12.12.1993 (с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) (Дата обращения 01.04.2026).

2. Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ (ред. от 06.04.2024) (Дата обращения 01.04.2026).

3. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (ред. от 06.02.2023) (Дата обращения 03.04.2026).

4. Федеральный закон от 02.12.2019 № 503-ФЗ «О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта» (ред. от 22.06.2024) (Дата обращения 04.04.2026).

5. Указ Президента РФ от 10.10.2019 № 490 «О развитии искусственного интеллекта в Российской Федерации» (вместе с Национальной стратегией развития ИИ до 2030 года) (Дата обращения 04.04.2026).

6. Goodfellow I., Bengio Y., Courville A. Deep Learning. – MIT Press, 2016. – 800 с. (русский перевод: Гудфеллоу Я., Бенджио И., Курвилль А.

Глубокое обучение. – М.: ДМК Пресс, 2018) (Дата обращения 02.04.2026).

Nasrtdinov A.S.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Salov I.V.
Ufa University of Science and Technology, Ufa

USING ARTIFICIAL INTELLIGENCE TO PREDICT SAFETY THREATS: EXPERIENCE IN IMPLEMENTING FORECAST MODELS IN A CORPORATE ENVIRONMENT

Abstract. This article discusses the application of artificial intelligence (AI) technologies for predicting information and physical security threats. It describes the technical capabilities, including the analysis of behavioral anomalies, the prediction of attacks based on machine learning, and the early detection of incidents. However, without proper regulatory and ethical support, the effectiveness of these technologies is limited. The article proposes an approach based on hybrid models, adaptive learning, and algorithm transparency. By replacing reactive logic with predictive logic, it enhances security and reduces operational risks.

Keywords: artificial intelligence, threat forecasting, information security, machine learning, behavioral analysis, predictive analytics, anomalies, and information protection.

УДК 004.8:004.056

Попов С.И., Дончик С.А.
Уфимский университет науки и технологий, Уфа

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

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В КИБЕРПРЕСТУПЛЕНИЯХ: УГРОЗЫ, ВОЗМОЖНОСТИ И МЕРЫ ЗАЩИТЫ

Аннотация. В статье подробно рассмотрены полезные стороны использования искусственного интеллекта в кибербезопасности, включая автоматизацию обнаружения угроз, поведенческий анализ пользователей и систем, ускорение реагирования на инциденты и снижение нагрузки на

специалистов по информационной безопасности. Особое внимание уделено реальным рискам и ограничениям для информационной безопасности, атакам на сами модели искусственного интеллектка и росту масштаба преступлений. Статья опирается на актуальные данные 2024–2025 годов и приводит конкретные случаи из практики, чтобы показать баланс между преимуществами и угрозами.

Ключевые слова: искусственный интеллект, уязвимости, защита, риск, информационная безопасность, автоматизация.

За последние несколько лет статус технологий искусственного интеллекта (ИИ) трансформировался из концептуальной новинки в практически применимый инструмент обработки данных, повсеместно внедряемый для решения рутинных задач. Накопленный опыт эксплуатации ИИ позволяет выделить ключевые преимущества его использования в сфере защиты от киберпреступности. К ним относятся: снижение нагрузки на специалистов, ускорение реагирования на инциденты за счет автоматизации рутинных процессов [1], реализация поведенческого анализа пользователей и систем, а также обнаружение ранее неизвестных угроз. На современном этапе развития технологий ИИ способен заменить сотрудника отдела безопасности в части мониторинга и первичного анализа данных.

Целью данной работы является анализ современных методов и применения ИИ в кибер-преступлениях, опираясь на реальные случаи 2024–2025 годов.

По данным исследовательского центра «Аналитика. Бизнес. Право», за последние четыре года число дел, в которых фигурируют правонарушения с использованием ИИ, выросло почти в полтора раза. В 2021 году число таких дел составляло 112, а к 2024 году их количество выросло до 292 [2]. В современной практике фиксируются инциденты использования технологий синтеза изображения и голоса (дипфейков) для обхода систем верификации финансовых организаций. Примером служит создание генерированного видеоконтента, в котором от лица публичной личности обосновывается необходимость получения крупного кредита с целью введения сотрудников банка в заблуждение [3].

Примером эффективного использования ИИ-технологий в 2025 году послужила имитация голоса министра обороны Италии для хищения средств у частных предпринимателей. Применение аудио-дипфейков в сочетании с методами социальной инженерии (ложные гуманитарные цели, психологическое давление) позволило мошенникам легализовать транзакции и вывести активы в офшорные юрисдикции [4].

В региональной практике зафиксированы случаи хищения крупных активов (порядка 2,5 млн долларов США) у промышленных предприятий

с использованием технологии визуальной подмены личности. Злоумышленники реализовали многоэтапную схему социальной инженерии, имитируя внешность и голос реального зарубежного контрагента в ходе видеоконференций в мессенджерах. Длительное дистанционное ведение переговоров с применением ИИ-инструментов позволило мошенникам фальсифицировать реквизиты сделки и убедить руководство предприятия в легитимности транзакции льготных заемных средств [5].

Современные методы обеспечения кибербезопасности базируются на превентивном выявлении угроз и защите персональных данных с применением интеллектуальных систем. Ключевым направлением является автоматизация мониторинга на основе ИИ, осуществляющего анализ сетевого трафика и поведения пользователей для оперативной фильтрации ложных срабатываний. В частности, технология User and Entity Behavior Analytics формирует поведенческие профили субъектов и устройств, сопоставляя текущую активность с ретроспективными данными.

Преимуществом ИИ-решений перед традиционными сигнатурными системами выступает способность распознавать сложные многовекторные атаки и прогнозировать потенциальные инциденты, обеспечивая переход к стратегии упреждающей обороны. Дополнительным инструментом защиты служит концепция цифровых двойников – виртуальных моделей физической инфраструктуры, позволяющих ИИ моделировать сценарии атак и тестировать устойчивость систем в изолированной среде без риска для реальных процессов

Таким образом, из вышеизложенного можно сделать вывод, что ИИ усиливает как защиту, так и атаки. То есть только комплексный подход – сочетание технологий, человеческий фактор и постоянное обучение – позволит сохранить контроль над информационной безопасностью.

Список использованных источников:

1. Свидетельство о государственной регистрации программы для ЭВМ № 2026616287 Российская Федерация. Программный комплекс сегментированного моделирования данных по термической деструкции генетическим алгоритмом: заявл. 03.03.2026: опубл. 05.03.2026 / Э. Р. Гиззатова, С. И. Никонова, А. А. Корнилова; заявитель федеральное государственное бюджетное образовательное учреждение высшего образования «Уфимский университет науки и технологий».

2. Количество дел об использовании ИИ в судах выросло на 40 % [Электронный ресурс] // Servicepipe: [офиц. сайт]. – 2025. – 13 марта. –

URL: https://servicepipe.ru/press-center/kolichestvo_del_ob_ispolzovanii_ii_v_sudah_vyroslo_na_40_procentov (дата обращения: 31.03.2026).

3. Штурма, Я.Голосовые связи: число дел об использовании ИИ в судах выросло почти на 40 % [Электронный ресурс] / Я. Штурма, В. Мишина // Известия: [информ. портал]. – 2025. – 10 марта. – URL: https://iz.ru/1853700/iana-shturma-valeriia-mishina/golosovie-svyazi-chislo-del-ob-ispolzovanii-ii-v-sudakh-vyroslo-pochti-na-40 (дата обращения: 31.03.2026).

4. Киберпреступность и искусственный интеллект: типы преступлений с использованием ИИ [Электронный ресурс] // Kaspersky: [портал о кибербезопасности]. – URL: https://www.kaspersky.ru/resource-center/preemptive-safety/ai-cybercrime (дата обращения: 31.03.2026).

5. Число судебных дел об ИИ в РФ выросло на 40 % [Электронный ресурс] // Коммерсантъ: [информ. портал]. – 2025. – 11 марта. – URL: https://www.kommersant.ru/doc/7604145 (дата обращения: 31.03.2026).

6. Использование ИИ для совершения преступлений в отношении компаний [Электронный ресурс] // Адвокат 24: [юр. портал]. – URL: https://www.advo24.ru/publication/ispolzovanie-ii-dlya-soversheniya-prestupleniy-v-otnoshenii-kompaniy.html (дата обращения: 31.03.2026).

Popov S.I., Donchik S.A.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Kornilova A.A.
Ufa University of Science and Technology, Ufa

ARTIFICIAL INTELLIGENCE IN CYBERCRIME: THREATS, OPPORTUNITIES, AND PROTECTIVE MEASURES

Abstract. The article examines in detail the beneficial aspects of using artificial intelligence in cybersecurity, including automated threat detection, behavioral analysis of users and systems, accelerated incident response, and reduced workload for information security specialists. Particular attention is paid to real risks and limitations for information security, attacks on the AI models themselves, and the growing scale of crimes. The study relies on current data from 2024–2025 and provides specific case studies to demonstrate the balance between advantages and threats.

Keywords: artificial intelligence, vulnerabilities, protection, risk, information security, automation.

УДК 004

Сунь Хаожань
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина), Санкт-Петербург

Научный руководитель:
Шульженко А.Д.
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина), Санкт-Петербург

АДАПТИВНЫЙ АЛГОРИТМ КЛАСТЕРИЗАЦИИ ДЛЯ БПЛА НА ОСНОВЕ ОБУЧЕНИЯ С ПОДКРЕПЛЕНИЕМ

Аннотация. Традиционные алгоритмы кластеризации с трудом адаптируются к высокодинамичной среде самоорганизующихся сетей БПЛА. В данной статье предлагается адаптивный алгоритм кластеризации на основе обучения с подкреплением (адаптивная кластеризация на основе Q-обучения, QLAC), который обучается выбору и поддержанию главы кластера в режиме реального времени, динамически балансируя внутрикластерную связность и нагрузку, тем самым увеличивая срок службы сети и скорость доставки данных.

Ключевые слова: самоорганизующаяся сеть БПЛА; адаптивная кластеризация; выбор главы кластера

Обзор литературы. В самоорганизующихся сетях БПЛА структура кластеризации имеет решающее значение для повышения масштабируемости и эффективности использования ресурсов, но традиционные алгоритмы имеют недостатки в динамических средах. Алгоритм кластеризации Least ID (LID) опирается на идентификаторы узлов, а не на метрики мобильности, что приводит к низкой скорости смены главы кластера и низкой вероятности доступности в условиях мобильной связи [1]. Хотя алгоритм взвешенной кластеризации (WCA) вводит многомерные веса, параметры основаны на статических предустановках, и скорость смены главы кластера и время жизни сети все еще недостаточны в высокоскоростных динамических сценариях [2]. Рен и др. отметили, что методы кластеризации, основанные на идентификаторах или фиксированных весах, с трудом справляются с прерываниями связи в высокодинамичных сценариях, и необходимо ввести такие метрики, как направление движения и время жизни канала связи [3]. Обучение с подкреплением предлагает новое решение этой проблемы: Абдулхае и др. разработали схему кластеризации FANET на основе обучения с подкреплением, которая обеспечивает многоплоскостное покрытие маршрутизации с помощью многоиндексных

функций вознаграждения [4]; Фэн и др. объединение нечеткой кластеризации и оптимизации политики ближнего конца для повышения скорости доставки данных и уменьшения задержки [5]; Меер и др. предложили иерархическую многоагентную структуру глубокого обучения с подкреплением для снижения частоты переконфигурации кластеров, которая подходит для высокодинамичных кластеров БПЛА [6].

Разработка алгоритма QLAC.

Для устранения недостатков WCA и LID в данной статье предлагается распределенный адаптивный алгоритм кластеризации (QLAC), основанный на Q-обучении. Каждый БПЛА выступает в роли агента, динамически корректирующего стратегии выбора главы кластера и поддержания кластера посредством онлайн-обучения.

1. Модель системы: Набор узлов N, время дискретизировано на временные интервалы t, радиус связи R, узлы получают свое положение и скорость с помощью GPS.

2. Элементы обучения с подкреплением. Состояние: $s_i(t) = \{d_i, v_i, e_i, \text{role}_i(t-1)\}$: степень узла, нормированная скорость, процент оставшейся энергии и роль в текущем временном интервале (0 – участник/1 – глава кластера/2 – шлюз). Действие A={0,1,2}: 0 – Выбор главы кластера, 1 – Присоединение к соседнему кластеру, 2 – Остаться в режиме ожидания. Вознаграждение рассчитывается как $r_i = \alpha R_{\text{stab}} + \beta R_{\text{load}} + \gamma R_{\text{energy}} - \delta C_{\text{overhead}}$, где R_{stab} способствует стабильности ролей, R_{load} способствует балансировке нагрузки, R_{energy} отдает предпочтение кластерным главам с высокой энергией, а C_{overhead} наказывает за управляющие сообщения.

3. Последовательность выполнения алгоритма: В каждом временном интервале: 1. Трансляция сообщения Hello для обновления таблицы соседей; 2. Вычисление состояния s_i; 3. Выполнение ε-greedy выбора действий; 4. Выполнение действий для формирования кластера (выбор/присоединение/простой); 5. Вычисление вознаграждения; 6. Обновление Q-таблицы: $Q(s,a) \leftarrow Q(s,a) + \eta[r + \gamma \max_{a'} Q(s',a') - Q(s,a)]$; 7. Перейдите к следующему временному интервалу.

4. Особенности: Распределенная, адаптивная, справедливая, с низкими накладными расходами, преодолевающая статические параметры WCA и неравномерное энергопотребление LID.

Анализ экспериментальных результатов и выводы.

Таблица 1

Сравнение производительности алгоритмов

Algorithm	CH Changes	Cluster Size Std
WCA	2.45	1.86
LID	0.67	1.51
QLAC	0.21	0.36

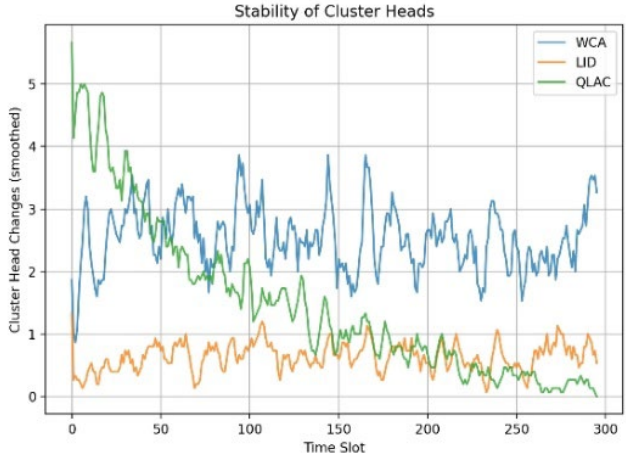


Рис. 1. Стабильность работы кластерных головок

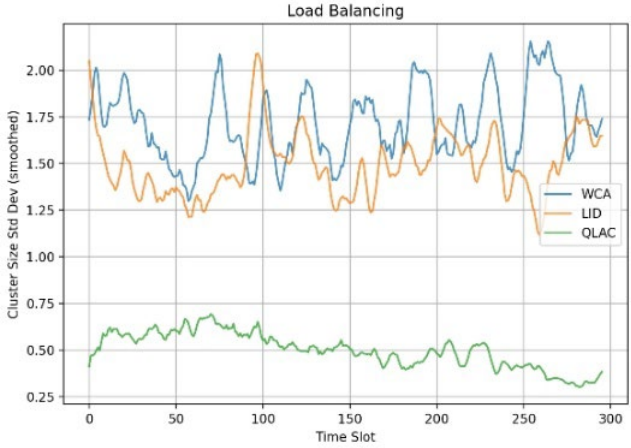


Рис. 2. Балансировка нагрузки

QLAC адаптивно выбирает меньшее количество кластерных голов, за ним следует WCA, в то время как LID приводит к наиболее изолированным кластерам из-за маргинального распределения узлов с низким ID. С точки зрения балансировки нагрузки, функция вознаграждения QLAC включает в себя член нагрузки и имеет наименьшее стандартное отклонение. В целом, QLAC демонстрирует наилучшую общую производительность, эффективно преодолевая недостатки традиционных алгоритмов.

Список использованных источников:

1. C. Tselikis, S. Mitropoulos, C. Douligeris, et al., "Empirical study of clustering algorithms for wireless ad hoc networks," in 16th International Conference on Systems, Signals and Image Processing (IWSSIP 2009), Chalkida, Greece, Jun. 2009.
2. K. Wang, X. Wang, and X. Zhang, "An Improved Weighted and Location-Based Clustering Scheme for Flying Ad Hoc Networks," Sensors, vol. 22, no. 9, p. 3236, Apr. 2022.
3. M. Ren, L. Khoukhi, H. Labiod, J. Zhang, and V. Vèque, "A new mobility-based clustering algorithm for vehicular ad hoc networks (VANETs)," Vehicular Communications, vol. 9, pp. 233-241, 2017.
4. O. T. Abdulhae, J. S. Mandeep, M. T. Islam, and M. S. Islam, "Reinforcement-Based Clustering in Flying Ad-Hoc Networks for Serving Vertical and Horizontal Routing," IEEE Access, vol. 11, pp. 143881-143895, 2023.
5. H. Feng, J. Wang, X. Hou, X. Zhang, Z. Zhang, and Z. Han, "Communication-Aware Hierarchical Routing for FANET: A Reinforcement Learning Approach," IEEE Transactions on Cognitive Communications and Networking, Oct. 2025.
6. I. A. Meer, K.-L. Besser, M. Ozger, D. A. Schupke, H. V. Poor, and C. Cavdar, "Hierarchical Multi-Agent DRL-Based Dynamic Cluster Reconfiguration for UAV Mobility Management," IEEE Transactions on Cognitive Communications and Networking, vol. 12, pp. 4957-4971, 2026.
7. Tariq Z U A, Baccour E, Erbad A, et al. RL-Based Adaptive UAV Swarm Formation and Clustering for Secure 6G Wireless Communications in Dynamic Dense Environments[J]. IEEE Access, 2024, 12: 125609-125628.
8. Swain S, Khilar P M, Senapati B R. A reinforcement learning-based cluster routing scheme with dynamic path planning for multi-UAV network[J]. Vehicular Communications, 2023, 42: 100605.

Sun Haoran
Saint Petersburg Electrotechnical University «LETI», Saint-Petersburg

Scientific supervisor:
Shulzhenko A.D.
Saint Petersburg Electrotechnical University «LETI», Saint-Petersburg

ADAPTIVE CLUSTERING ALGORITHM FOR UAVS BASED ON REINFORCEMENT LEARNING

Abstract. Traditional clustering algorithms struggle to adapt to the highly dynamic environment of self-organizing UAV networks. This paper proposes

an adaptive clustering algorithm based on reinforcement learning (Q-learning adaptive clustering, QLAC) that learns to select and maintain a cluster head in real time, dynamically balancing intra-cluster connectivity and load, thereby increasing network lifetime and data delivery speed.

Keywords: self-organizing UAV network; adaptive clustering; cluster head selection

УДК 004.8

Сысоева А.В.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Валеев С.С.
Уфимский университет науки и технологий, Уфа

ПРИМЕНЕНИЕ СВЕРТОЧНЫХ НЕЙРОННЫХ СЕТЕЙ В СИСТЕМЕ КОРПОРАТИВНОЙ ЗАЩИТЫ

Аннотация. Статья рассматривает возможности применения сверточных нейронных сетей для усиления корпоративной защиты. Анализируются два направления: использование CNN для физической безопасности и для стегоанализа. Приводятся результаты сравнения архитектур Faster R-CNN и YOLO применительно к задачам реального времени. Обсуждаются правовые аспекты обработки данных нейросетями.

Ключевые слова: сверточные нейронные сети, корпоративная защита, YOLO, стегоанализ, информационная безопасность, персональные данные.

Современные корпоративные системы защиты сталкиваются с растущим объемом угроз физического и цифрового характера. Традиционные средства безопасности – ручной мониторинг камер, сигнатурные методы обнаружения вторжений, системы контроля доступа – демонстрируют ограниченную эффективность в условиях масштабируемой инфраструктуры. Внедрение методов глубокого обучения, в частности сверточных нейронных сетей (CNN), становится необходимым элементом эшелонированной защиты предприятия [1].

Сверточные нейронные сети специализированы для обработки изображений и видео [2]. В корпоративной защите CNN позволяют автоматизировать визуальный контроль, выявлять аномалии и обнаруживать скрытые каналы передачи информации. В отличие от классических методов компьютерного зрения CNN самостоятельно

извлекают признаки из обучающей выборки, что обеспечивает высокую устойчивость к изменению ракурса и освещения. При этом архитектура сверточных слоев позволяет постепенно усложнять извлекаемые признаки: от простых границ и текстур на нижних уровнях до сложных форм и объектов на верхних [3].

Наиболее востребованным направлением применения CNN является интеллектуальное видеонаблюдение. Модели семейства YOLO зарекомендовали себя как оптимальное решение для задач реального времени. В отличие от двухэтапных Faster R-CNN, YOLO выполняет предсказание рамок и классов объектов за один проход через сеть [3]. Это обеспечивает скорость обработки, достаточную для анализа видеопотока в реальном времени [4].

Практические сценарии использования CNN включают: контроль доступа в зоны с ограниченным допуском; мониторинг соблюдения требований охраны труда; детектирование оставленных предметов; выявление подозрительного поведения [1]. Экспериментальные данные показывают, что модели YOLO (v8–v10) демонстрируют точность mAP@0.5 на уровне 0,25–0,28 при производительности 15–36 кадров в секунду [3]. Компактность моделей позволяет развертывать их на периферийных устройствах, исключая передачу видеоданных во внешние сервисы [3]. Такой подход не только снижает нагрузку на корпоративную сеть, но и минимизирует риски утечки конфиденциальной информации за пределы контролируемого периметра [1].

CNN находят применение в выявлении стеганографических каналов. Злоумышленники используют цифровые изображения как контейнеры для скрытого выноса конфиденциальной информации. Объем легитимного трафика изображений делает этот канал невидимым для традиционных средств защиты [5].

Стегоанализ на основе CNN решает задачу бинарной классификации. Нейросетевые стегоанализаторы улавливают тонкие изменения цвето-яркостных характеристик, вносимые алгоритмами встраивания. Интеграция модуля стегоанализа в почтовый шлюз обеспечивает блокировку подозрительных изображений до их отправки. ПНСТ 945-2024 позволяет распределять нагрузку между периферийными устройствами и сервером [5]. Использование предварительно обученных моделей с последующей тонкой настройкой под специфику корпоративного трафика существенно сокращает время развертывания системы стегоанализа [4].

При развертывании CNN-систем необходимо учитывать требования Федерального закона № 152-ФЗ «О персональных данных» [6]. Видеонаблюдение с идентификацией личности по биометрическим признакам требует письменного согласия субъекта [7]. Обработка данных

должна осуществляться с соблюдением принципов минимизации и конфиденциальности [6]. Компаниям рекомендуется проводить аудит соответствия требованиям регулятора [8].

Важным аспектом является робастность нейросетевых моделей. ГОСТ Р ИСО/МЭК 24029-2-2024 устанавливает методологию оценки устойчивости нейронных сетей к искажениям и атакам [8]. Система видеонаблюдения должна сохранять работоспособность при изменении условий съемки, а стегоанализатор – противостоять попыткам обхода. Регулирование искусственного интеллекта в России развивается в направлении установления требований к прозрачности алгоритмов [8]. Формальные методы верификации, описанные в стандарте, позволяют математически доказать отсутствие критических ошибок классификации в заданном диапазоне входных воздействий [8].

Сверточные нейронные сети представляют собой эффективный инструмент усиления корпоративной защиты, обеспечивающий автоматизацию визуального мониторинга и обнаружение скрытых каналов утечки информации. Выбор архитектуры должен определяться спецификой охраняемого объекта [3]. Перспективным направлением является интеграция CNN-аналитики с системами контроля доступа и SIEM-платформами [1]. Критически важным остается соблюдение правовых норм и соответствие национальным стандартам [8, 5]. Комплексный подход, объединяющий технические и организационные меры защиты, позволяет выстроить эшелонированную систему безопасности, устойчивую к актуальным киберугрозам [1].

Список использованных источников:

1. Автоматизация моделирования системы безопасности организации с использованием нейросетей // Editorum. Брянский ГТУ. 2025. С. 24-32.

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. Ванюшев А.А., Мокшин В.В., Мавлиев Л.Ф. Адаптивные сверточные нейронные сети в интеллектуальных транспортных системах // Известия КГАСУ. 2025. № 2(72). С. 277-290.

4. Дурасов Н.С., Крутов А.Н., Осипов М.Н. Разработка защищенного менеджера для анализа данных на основе нейросети Yolo. Самара: Самар. ун-т, 2025.

5. ПНСТ 945-2024. Техническая структура для разделения и совместного исполнения модели глубокой нейронной сети. М.: Росстандарт, 2024.
6. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (ред. от 24.06.2025).
7. Идрисова Р. Безопасность и приватность: этические аспекты подсчета посетителей // РБК Компании. 05.12.2025.
8. 9ГОСТ Р ИСО/МЭК 24029-2-2024. Оценка робастности нейронных сетей. М.: Росстандарт, 2024.Регулирование ИИ в России 2025: что делать бизнесу // EORA.RU. 2025.

Sysoeva A.V.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Valeev S.S.
Ufa University of Science and Technology, Ufa

APPLICATION OF CONVOLUTIONAL NEURAL NETWORKS IN THE CORPORATE SECURITY SYSTEM

Abstract. The article examines the possibilities of applying convolutional neural networks to enhance corporate security. Two areas are analyzed: the use of CNN for physical security and for steganalysis. The results of a comparison of Faster R-CNN and YOLO architectures are presented. Legal aspects of data processing by neural networks are discussed.

Keywords: convolutional neural networks, corporate security, YOLO, steganalysis, information security, personal data.

УДК 004.056:004.8

Чуркин П.Ю.
Абитуриент магистратуры НИУ ВШЭ, Москва

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В КИБЕРБЕЗОПАСНОСТИ В 2026 ГОДУ: КАК ИИ ОДНОВРЕМЕННО УСКОРЯЕТ АТАКИ И УКРЕПЛЯЕТ ОБОРОНУ

Аннотация. Рассматривается двойственная роль искусственного интеллекта в кибербезопасности к 2026 году. Цель – выявить механизмы, посредством которых ИИ одновременно повышает эффективность атак и усиливает защиту. На основе российских аналитических и нормативных материалов определены ключевые сценарии применения ИИ, их

ограничения и условия безопасной интеграции в систему информационной безопасности.

Ключевые слова: искусственный интеллект, кибербезопасность, фишинг, дипфейки, обнаружение угроз, автоматизация защиты, SOC.

К 2026 году искусственный интеллект перестал быть вспомогательной технологией в кибербезопасности и стал фактором, непосредственно определяющим динамику противостояния между атакующей и защищающейся сторонами. Его влияние проявляется в изменении скорости, масштаба и структуры киберинцидентов. Аналитические материалы российских компаний фиксируют рост сложности атак, усиление роли социальной инженерии и распространение комбинированных сценариев компрометации [3].

Ключевое изменение связано не с появлением принципиально новых угроз, а с трансформацией их операционной реализации. ИИ снижает издержки подготовки атак за счет автоматизации этапов, ранее требовавших ручной работы. Это приводит к смещению акцента с квалификации отдельного исполнителя на качество используемых инструментов и данных. В результате возрастает масштабируемость атак и сокращается время между их планированием и реализацией.

Наиболее выраженно это проявляется в фишинге. По данным BI.ZONE, в 2025 году наблюдался кратный рост количества фишинговых рассылок, а общий объем нежелательной почты увеличился на 46 %. При этом эффективность атак определяется уже не столько техническими характеристиками сообщений, сколько их содержательной достоверностью. Использование легитимных почтовых сервисов и скомпрометированных учетных записей дополнительно снижает результативность традиционных фильтров [1]. Таким образом, фишинг эволюционирует от технической к когнитивной атаке.

Именно на этом уровне проявляется влияние генеративных моделей. По оценке Positive Technologies, ИИ становится одним из ключевых катализаторов киберугроз, поскольку позволяет автоматизировать создание убедительного текстового контента, адаптированного под контекст взаимодействия с жертвой [6]. Это приводит к качественному изменению атак: вместо массовых однотипных рассылок формируются вариативные сценарии коммуникации, учитывающие особенности конкретной организации или пользователя.

Расширение возможностей социальной инженерии усиливается за счет распространения дипфейков. По данным «Лаборатории Касперского», в 2025 году на теневых площадках появились предложения по созданию аудио- и видеодипфейков в режиме реального времени [4]. Это свидетельствует о переходе технологии в стадию прикладного

использования. Практическое значение заключается в том, что атака на доверие приобретает мультимодальный характер: текстовая коммуникация дополняется поддельными голосовыми и визуальными сигналами, что усложняет идентификацию угрозы.

Технический аспект атак также претерпевает изменения. Positive Technologies отмечает развитие инструментов, использующих ИИ для автоматизации анализа защищенности и выполнения типовых задач тестирования на проникновение [5]. В наступательном контуре это означает ускорение поиска уязвимостей и адаптации атакующих сценариев. При этом важно подчеркнуть, что ИИ не устраняет необходимость в классических методах компрометации, а повышает их эффективность, сокращая время и трудозатраты.

Анализ ландшафта угроз показывает, что базовые векторы атак остаются неизменными. В материалах BI.ZONE отмечается сохранение значимости фишинга, атак через подрядчиков и использования доверенных каналов взаимодействия [2]. Однако их результативность возрастает за счет интеграции ИИ в подготовительные и вспомогательные этапы. Это позволяет рассматривать ИИ не как источник новых угроз, а как мультипликатор существующих.

В защитном контуре влияние ИИ имеет иную направленность. По данным Positive Technologies, его применение позволяет автоматизировать обработку событий, выявлять поведенческие аномалии и повышать точность обнаружения угроз [5]. В условиях роста объема телеметрии это становится необходимым условием функционирования центров мониторинга безопасности. ИИ обеспечивает предварительную фильтрацию и приоритизацию инцидентов, что снижает нагрузку на специалистов и сокращает время реагирования.

Особое значение ИИ приобретает в анализе коммуникаций. Поскольку современные атаки ориентированы на содержательные признаки, защита должна учитывать контекст и структуру сообщений. BI.ZONE указывает на необходимость выявления нетехнических признаков манипуляции, включая аномальную лексику и поведенческие отклонения [1]. Это формирует переход от сигнатурных методов к поведенческому анализу, в котором ИИ играет ключевую роль.

В кибер разведке ИИ используется для выявления скрытых связей между событиями и индикаторами компрометации. Это позволяет формировать более целостное представление об инциденте и прогнозировать его развитие. Особенно важным это становится в ситуациях, когда злоумышленники используют легитимные инструменты и инфраструктуру, что затрудняет их обнаружение традиционными средствами [2].

Несмотря на значительные преимущества, применение ИИ в защите сопряжено с рядом ограничений. Эффективность моделей зависит от качества входных данных и корректности их интерпретации. Кроме того, автоматизация не исключает необходимости экспертной оценки и может приводить к снижению критичности анализа. В нормативных материалах ФСТЭК России подчеркивается необходимость использования доверенных технологий ИИ и обеспечения безопасности их разработки и эксплуатации [7,8].

Таким образом, к 2026 году ИИ сформировал новую конфигурацию кибербезопасности, в которой он одновременно усиливает атакующие и защитные возможности. Его влияние заключается не в создании новых типов угроз, а в ускорении и усложнении уже существующих. Это требует пересмотра подходов к защите: приоритет должен смещаться от изолированных технических решений к интеграции ИИ в комплексные, управляемые и проверяемые системы безопасности. Только в этом случае использование ИИ способствует снижению рисков, а не их дополнительной эскалации.

Список использованных источников:

1. BI.ZONE. Фишинг стал главной угрозой для корпоративной почты в 2025 году [Электронный ресурс] // BI.ZONE. – 2026. – URL: https://bi.zone/news/fishing-stal-glavnoy-ugrozoy-dlya-korporativnoy-pochty-v-2025-godu/.

2. BI.ZONE. Threat Zone 2025 [Электронный ресурс] // BI.ZONE. – 2025. – URL: https://bi.zone/expertise/research/threat-zone-2025/.

3. F6. Больше атакующих и больше ущерба: F6 назвала главные киберугрозы в 2026 году [Электронный ресурс] // F6. – 2026. – URL: https://www.f6.ru/media-center/press-releases/cybercrime-trends-annual-report-2025-2026/.

4. Лаборатория Касперского. В даркнете предлагают услуги по созданию видео- и аудиодипфейков в режиме реального времени [Электронный ресурс] // Лаборатория Касперского. – 2025. – URL: https://www.kaspersky.ru/about/press-releases/laboratoriya-kasperskogo-v-darknete-predlagayut-uslugi-po-sozdaniyu-video-i-audiodipfejkov-v-rezhime-realnogo-vremeni.

5. Positive Technologies. Искусственный интеллект в киберзащите [Электронный ресурс] // Positive Technologies. – 2025. – URL: https://ptsecurity.com/research/analytics/iskusstvennyi-intellekt-v-kiberzaschite/.

6. Positive Technologies. Тренды атак в 2026 году [Электронный ресурс] // Positive Technologies. – 2026. – URL: https://ptsecurity.com/research/analytics/trendy-atak-v-2026-godu/.

7. ФСТЭК России. Решение заседания ТК 362 от 29.01.2025 г. [Электронный ресурс] // ФСТЭК России. – 2025. – URL: https://fstec.ru/tk-362/deyatelnost-tk362/resheniya-zasedaniya-tk-362-pk-tk-362/reshenie-zasedaniya-tk-362-ot-29-01-2025-g.

8. ФСТЭК России. Требования. Утверждены приказом ФСТЭК России от 11 апреля 2025 г. № 117 [Электронный ресурс] // ФСТЭК России. – 2025. – URL: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/trebovaniya-utverzhdeny-prikazom-fstek-rossii-ot-11-aprelya-2025-g-n-117.

Churkin P.Yu.
Master's program applicant, HSE University, Moscow

ARTIFICIAL INTELLIGENCE IN CYBERSECURITY IN 2026: HOW AI SIMULTANEOUSLY ACCELERATES ATTACKS AND STRENGTHENS DEFENSE

Abstract. The dual role of artificial intelligence in cybersecurity by 2026 is considered. The aim is to identify the mechanisms by which AI simultaneously increases the effectiveness of attacks and enhances defense. Based on Russian analytical and regulatory materials, the key scenarios of AI application, their limitations, and the conditions for its secure integration into the information security system are determined.

Keywords: artificial intelligence, cybersecurity, phishing, deepfakes, threat detection, security automation, SOC.

УДК 004.056.53

Шамин Т.С.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Сенцова А.Ю.
Уфимский университет науки и технологий, Уфа

МЕТОДЫ ОБНАРУЖЕНИЯ И ПОДАВЛЕНИЯ АТАК НУЛЕВОГО ДНЯ (ZERO-DAY) В КОРПОРАТИВНЫХ СЕТЯХ С ИСПОЛЬЗОВАНИЕМ ПОВЕДЕНЧЕСКОГО АНАЛИЗА

Аннотация. Рост числа кибератак с использованием уязвимостей нулевого дня создает серьезные вызовы для систем защиты информации российских корпоративных структур. Традиционные сигнатурные методы обнаружения угроз оказываются неэффективными против неизвестных

эксплойтов. В статье исследуются современные подходы к выявлению Zero-Day атак на основе поведенческого анализа сетевого трафика и активности пользователей. Рассматриваются методы машинного обучения, аномальная детекция и анализ отклонений от базовых профилей поведения. Обоснована необходимость комплексного подхода, сочетающего различные технологии детектирования угроз.

Ключевые слова: атаки нулевого дня, поведенческий анализ, кибербезопасность, аномальная детекция, машинное обучение, корпоративные сети, защита информации.

Согласно [1] уязвимости нулевого дня являются одним из наиболее опасных классов киберугроз для российских организаций.

Специфика Zero-Day атак заключается в том, что на момент эксплуатации уязвимость, которую используют при проведении этой атаки, не имеет не имеет опубликованного описания, а значит – не существует и сигнатуры для традиционных систем защиты [2]. Злоумышленник получает временное окно возможностей, которое может длиться от нескольких дней до нескольких месяцев.

Проблема усугубляется тем, что современные корпоративные сети представляют собой гетерогенную среду. Здесь сосуществуют разнородные операционные системы, сетевое оборудование различных производителей, унаследованные системы и новые облачные сервисы и технологии виртуализации. Такая инфраструктура расширяет поверхность атаки и создает множество потенциальных точек входа для эксплуатации неизвестных уязвимостей.

Классические средства защиты информации строятся на принципе сигнатурного анализа – сравнении входящего трафика и исполняемого кода с базой известных угроз. Такой подход демонстрирует высокую эффективность против распространенных вредоносных программ и типовых векторов атак.

Системы обнаружения вторжений (IDS) традиционной архитектуры оказываются бессильны перед модифицированными эксплойтами. Злоумышленник может изменить всего несколько байт в коде атаки, и сигнатура перестанет срабатывать. Песочницы (sandbox) обеспечивают несколько лучшие результаты – они способны детектировать больше неизвестных угроз путем анализа поведения в изолированной среде. Но опытные атакующие научились распознавать среду песочницы и переводить вредоносный код в «спящий режим» до выхода в реальную систему.

Практика показывает, что детектирование возможно – но только на основе косвенных признаков. Речь идет не о поиске конкретной сигнатуры атаки, а о выявлении аномального поведения в системе.

Чаще всего злоумышленники успевают закрепиться в сети, повысить привилегии и начать латеральное перемещение к критически важным активам. Большинство таких атак обнаруживается не техническими средствами, а случайно – при плановых аудитах или в результате явных сбоев в работе систем.

В основе поведенческого подхода лежит допущение о том, что любая атака – даже использующая неизвестную уязвимость – неизбежно создает аномальные комбинации активности. Эти ошибки могут проявляться на разных уровнях, сетевой трафик, системные вызовы, действия пользователей, обращения к файловой системе, изменения конфигураций.

Ключевая идея – построение базового профиля нормального поведения для каждого элемента инфраструктуры. Системы поведенческого анализа, – особенно те, что используют алгоритмы машинного обучения, – способны автоматически формировать такие профили на основе длительного наблюдения за сетью. После создания базовой модели любое отклонение от нее фиксируется как потенциальная аномалия и требует дополнительного анализа.

Практическая реализация поведенческого анализа включает несколько взаимодополняющих технологий:

- анализ сетевого трафика (Network Behavior Analysis) – выявление аномальных коммуникационных паттернов, необычных объемов передачи данных, подозрительных соединений с внешними узлами;
- анализ поведения пользователей и сущностей (User and Entity Behavior Analytics) – детектирование нетипичных действий учетных записей, таких как доступ к необычным ресурсам, активность в нерабочее время, массовое копирование файлов;
- анализ потоков данных (Data Flow Analysis) – отслеживание перемещения конфиденциальной информации внутри сети и попыток ее эксфильтрации.

Наиболее распространенными в российской практике стали три класса алгоритмов [3]. Методы обучения без учителя – кластеризация, метод главных компонент, автоэнкодеры – используются для выявления объектов, не вписывающихся в основную массу наблюдений. Такие алгоритмы не требуют предварительной разметки данных и особенно эффективны для детектирования ранее неизвестных типов атак.

Методы обучения с учителем – случайный лес, градиентный бустинг, нейронные сети – применяются для классификации событий на легитимные и вредоносные на основе размеченных примеров. Проблема в том, что для обучения таких моделей необходимы репрезентативные выборки атак, включая Zero-Day эксплойты – а их по определению мало.

Гибридная модель, комбинирующая изоляционный лес для первичного отсева явных аномалий и рекуррентную нейронную сеть для анализа временных последовательностей событий, продемонстрировала наилучшее соотношение между полнотой обнаружения (recall = 0,76) и точностью (precision = 0,68).

Модели глубокого обучения требуют значительных вычислительных ресурсов и способны обрабатывать лишь ограниченный объем сетевых событий в реальном времени. Для крупной корпоративной сети, генерирующей десятки терабайт логов ежедневно, это создает серьезные технические ограничения. По этой причине многие российские организации используют многоуровневую архитектуру, простые статистические методы для грубой фильтрации на первом этапе, а сложные модели ML – только для анализа предварительно отобранных подозрительных событий.

Другая проблема – интерпретируемость решений. Глубокие нейронные сети работают как «черный ящик», они способны с высокой точностью классифицировать события, но не объясняют, почему конкретное событие признано аномальным. Для аналитика службы безопасности это существенное ограничение – ему необходимо понимать природу угрозы, чтобы принять адекватные меры реагирования. Поэтому в критически важных системах предпочтение часто отдается более простым, но интерпретируемым алгоритмам – таким как деревья решений или логистическая регрессия.

Внедрение систем поведенческого анализа в российских корпоративных сетях сталкивается с рядом специфических вызовов. Первый из них – дефицит квалифицированных специалистов. Настройка и эксплуатация систем UEBA требует компетенций на стыке информационной безопасности, администрирования сетей и науки о данных.

Атаки нулевого дня представляют собой один из наиболее серьезных вызовов для информационной безопасности российских корпоративных сетей. Традиционные методы защиты, основанные на сигнатурном анализе, демонстрируют недостаточную эффективность против неизвестных угроз. Поведенческий анализ, использующий методы машинного обучения и статистического детектирования аномалий, обеспечивает принципиально новые возможности выявления Zero-Day атак на ранних стадиях.

Критически важным фактором успеха является наличие квалифицированных специалистов, способных настраивать сложные системы детектирования и анализировать генерируемые ими предложения.

Дальнейшее развитие технологий обнаружения Zero-Day угроз связано с совершенствованием алгоритмов машинного обучения, повышением их интерпретируемости и снижением вычислительной сложности. Перспективным направлением является использование федеративного обучения, позволяющего нескольким организациям совместно обучать модели детектирования без раскрытия конфиденциальных данных о собственной инфраструктуре.

Список использованных источников:

1. Что такое атака нулевого дня? Определение и описание URL: https://www.kaspersky.ru/resource-center/definitions/zero-day-exploit (дата обращения: 12.04.2026).

2. Уязвимость нулевого дня: что такое и как защититься URL: https://kontur.ru/aegis/blog/83380-uyazvimost_nulevogo_dnya (дата обращения 12.04.2026).

3. Comparison of Supervised, Semi-supervised and Unsupervised Learning Methods in Network Intrusion Detection System (NIDS) Application URL: https://akwi.hswlu.ch/article/view/3183 (дата обращения 15.04.2026).

Shamin T.S.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Sentsova A.Yu.
Ufa University of Science and Technology, Ufa

METHODS FOR DETECTING AND SUPPRESSING ZERO-DAY ATTACKS IN CORPORATE NETWORKS USING BEHAVIORAL ANALYSIS

Abstract. The growing number of cyberattacks using zero-day vulnerabilities poses serious challenges to the information security systems of Russian corporate structures. Traditional signature-based threat detection methods are ineffective against unknown exploits. This article explores modern approaches to detecting zero-day attacks based on behavioral analysis of network traffic and user activity. It examines machine learning techniques, anomaly detection, and deviations from baseline behavior profiles. The article emphasizes the need for a comprehensive approach that combines various threat detection technologies.

Key words: zero-day attacks, behavioral analysis, cybersecurity, anomaly detection, machine learning, corporate networks, and information protection.

УДК 004

Шигапов А.В.
Уфимский университет науки и технологий, Уфа

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

ИДЕНТИФИКАЦИЯ ФИШИНГОВЫХ РЕСУРСОВ В ИНТЕРНЕТЕ НА ОСНОВЕ ТЕХНОЛОГИЙ МАШИННОГО ОБУЧЕНИЯ

Аннотация. Фишинговые атаки остаются одной из наиболее распространенных киберугроз в российском сегменте интернета. Классические методы обнаружения вредоносных ресурсов, основанные на черных списках и сигнатурном анализе, демонстрируют снижающуюся эффективность. Статья рассматривает применение алгоритмов машинного обучения для автоматической идентификации фишинговых сайтов, анализируя актуальные подходы к извлечению признаков URL-адресов и особенности контента страниц.

Ключевые слова: фишинг, машинное обучение, кибербезопасность, классификация веб-ресурсов, нейронные сети, информационная безопасность, киберугрозы.

Фишинг как форма социальной инженерии эволюционировал от примитивных почтовых рассылок до сложных многоэтапных атак. По данным Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (ФинЦЕРТ), в 2024 году количество уникальных фишинговых ресурсов, нацеленных на российских пользователей, выросло на 48,3% по сравнению с 2023-м. Причем речь идет не просто о количественном росте – меняется качество атак [1].

Традиционные методы противодействия базируются на составлении и регулярном обновлении черных списков. Роскомнадзор и операторы связи блокируют доступ к выявленным вредоносным ресурсам. Однако скорость создания новых фишинговых доменов превышает темпы их обнаружения классическими средствами. Киберпреступники регистрируют сотни доменов ежедневно, используя автоматизированные системы генерации имен и дешевые хостинговые площадки за пределами российской юрисдикции. Здесь возникает принципиальный вопрос о времени обнаружения фишинговых сайтов. Период между появлением фишингового сайта и его внесением в черный список составляет в среднем 18–24 часа. За это время злоумышленники успевают скомпрометировать десятки, а иногда сотни учетных записей [2, 3].

Анализ URL-адресов дает первичные сигналы о потенциальной угрозе. Фишинговые домены часто содержат имена известных брендов в нестандартных позициях – например, «sberbank-secure-login.ru» вместо «sberbank.ru». Длина домена, наличие цифр, использование дефисов, применение интернационализированных доменных имен (IDN) с визуально похожими символами – все это служит индикаторами.

Однако одного анализа адреса недостаточно. Содержимое страницы несет критически важную информацию. HTML-структура, наличие форм для ввода конфиденциальных данных, количество внешних ссылок, использование JavaScript для обфускации кода – параметры, требующие детального разбора. Особое внимание уделяется анализу форм авторизации: легитимные банковские сайты используют сложные многофакторные системы аутентификации, тогда как фишинговые копии часто ограничиваются простыми полями логина и пароля.

Поведенческие признаки добавляют третий уровень защиты. Время жизни домена, география хостинга, скорость изменения DNS-записей, репутация IP-адреса сервера – все это учитывается в комплексных моделях.

Модель гибридной архитектуры, где первичная фильтрация осуществляется быстрым классификатором на базе случайного леса, а подозрительные случаи направляются на углубленный анализ нейросетью. Такой подход позволил снизить вычислительную нагрузку при сохранении высокой чувствительности системы. Такая модель была использована в исследовании 2025 года и показала результат 98,64%, этот показатель подтверждает эффективность данного подхода [4].

Система мониторинга новых доменов в зоне .ru и .рф, внедренная Координационным центром доменов RU/РФ, использует алгоритмы машинного обучения для выявления потенциально вредоносных регистраций. Анализируются паттерны массовых регистраций, лексическое сходство с известными брендами, аномалии в DNS-конфигурации [5, 6].

Несмотря на высокие показатели точности в лабораторных условиях, практическое применение сталкивается с рядом вызовов. Адаптация злоумышленников происходит быстро – появляются новые техники обхода детектирования. Например, использование легитимных облачных сервисов для размещения фишинговых страниц усложняет блокировку: нельзя просто занести в черный список весь диапазон IP-адресов Google Cloud или Amazon AWS.

Необходимость постоянного переобучения моделей на свежих данных требует организации процессов сбора разметки и валидации. Команды безопасности вынуждены ежедневно анализировать сотни потенциальных угроз, подтверждать или опровергать вердикты

автоматических систем. Здесь стоит сделать оговорку: полностью автоматизированное решение без участия экспертов пока остается не реализовано на практике в полном размере.

Исследования показывают корреляцию между уровнем автоматизации обнаружения и временем реакции на инциденты. Организации, применяющие машинное обучение, блокируют доступ за 15 часов [7].

Исследования в этой области очевидны, каждый час сокращения времени реакции напрямую влияет на снижение финансовых потерь пользователей и репутационных рисков организаций. В условиях растущей цифровизации экономики и государственных услуг, развитие интеллектуальных систем защиты становится стратегическим приоритетом обеспечения информационной безопасности.

Список использованных источников:

1. 80% создаваемых фейковых ресурсов маскируются под известные бренды // ITSec.ru. – URL: https://www.itsec.ru/news/80-sozdavayemih-feykovih-resursov-maskiruyetsia-pod-izvestniye-brendi (дата обращения: 19.04.2026).

2. Фиши прилетели: Group-IB выявила рекордное число мошеннических ресурсов в Рунете в 2022 году // Habr.com. – 2022. – 11 ноября. – URL: https://habr.com/ru/companies/F6/news/698878/ (дата обращения: 19.04.2026).

3. Исследование «Лаборатории Касперского»: жизненный цикл более трети фишинговых страниц не превышает 24 часов // Kaspersky: веб-сайт. – 2021. – 11 декабря. – URL: https://www.kaspersky.ru/about/press-releases/issledovanie-laboratorii-kasperskogo-zhiznennyj-cikl-bolee-treti-fishingovyh-stranic-ne-prevyshaet-24-chasov (дата обращения: 18.04.2026).

4. Aniyansyah N., Rina R., Puspitasari S., Erfina A. Evaluation of AI Models for Phishing Detection Using Open Datasets // Engineering Proceedings. – 2025. – Т. 107, № 1. – С. 37. – DOI: 10.3390/engproc2025107037. – URL: https://www.mdpi.com/2673-4591/107/1/37 (дата обращения: 17.04.2026).

5. Искусственный интеллект против кибersквоттинга // Координационный центр доменов .RU/.РФ. – 2025. – 26 марта. – URL: https://cctld.ru/media/news/industry/37724/ (дата обращения: 19.04.2026).

6. Проактивный подход помогает в борьбе с фишингом // Координационный центр доменов .RU/.РФ. – 2024. – 18 января. – URL: https://cctld.ru/media/news/kc/35493/ (дата обращения: 20.04.2026).

7. Фишинг в Рунете пошел на снижение // Byte/RE. – 2025. – 17 июля. – URL: https://bytemag.ru/fishing-v-runete-poshel-na-snizhenie-41876/ (дата обращения: 19.04.2026).

Shigapov A.V.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Yunusova D.S.
Ufa University of Science and Technology, Ufa

IDENTIFICATION OF PHISHING RESOURCES ON THE INTERNET BASED ON MACHINE LEARNING TECHNOLOGIES

Abstract. Phishing attacks remain one of the most common cyber threats in the Russian Internet segment. Classical methods of detecting malicious resources based on blacklists and signature analysis demonstrate decreasing effectiveness. This article explores the use of machine learning algorithms for automatic identification of phishing websites, analyzing current approaches to extracting URL features and page content characteristics.

Keywords: phishing, machine learning, cybersecurity, web resource classification, neural networks, information security, and cyber threats.

УДК 378.14:004.8

Якупов Я.Г.
Уфимский государственный нефтяной технический университет, Уфа

Научный руководитель:
Попов Д.В.
Уфимский государственный нефтяной технический университет, Уфа

ПЕРСОНАЛИЗАЦИЯ ОБУЧЕНИЯ С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА: КОНЦЕПТУАЛЬНЫЕ ОСНОВЫ И ОБРАЗОВАТЕЛЬНЫЙ ПОТЕНЦИАЛ

Аннотация. В статье рассматриваются концептуальные основы персонализации образовательного процесса с применением технологий искусственного интеллекта (ИИ). Анализируются ключевые подходы к

построению адаптивных обучающих систем, в том числе методы машинного обучения, обработки естественного языка и интеллектуального анализа данных. Обосновывается связь между концепцией «цифрового двойника студента» и персонализированными образовательными траекториями. Выявлены преимущества и ограничения ИИ-ориентированных решений, обозначены направления дальнейших исследований.

Ключевые слова: персонализация обучения, искусственный интеллект, адаптивные образовательные системы, цифровой двойник, машинное обучение, образовательная аналитика.

1. Введение

Современная система высшего образования переживает период трансформации, обусловленной стремительным развитием цифровых технологий и накоплением больших массивов данных об учебной деятельности студентов. Традиционные модели обучения, построенные на единых образовательных программах, все менее соответствуют индивидуальным потребностям обучающихся, различающихся темпом усвоения материала, когнитивным стилем и мотивационным профилем [1].

Одним из перспективных направлений является персонализация обучения – подход, предполагающий адаптацию содержания, темпа и методов преподавания к индивидуальным характеристикам каждого учащегося. Технологии искусственного интеллекта (ИИ) открывают принципиально новые возможности для реализации этого подхода в масштабе, недостижимом при опоре исключительно на педагогическую экспертизу [2].

Концептуально близкой является идея цифрового двойника студента – динамической цифровой модели, отражающей текущее состояние знаний, умений и поведенческих паттернов конкретного обучающегося, выступающей информационной основой для адаптивных педагогических решений в режиме реального времени [3].

2. Теоретические основы персонализации обучения

Идея персонализированного обучения уходит корнями в педагогические концепции XX века – от работ Л.С. Выготского о зоне ближайшего развития до теории множественного интеллекта Г. Гарднера [4]. С появлением систем управления обучением (LMS) и развитием образовательной аналитики (Learning Analytics) возможности персонализации существенно расширились: появились инструменты измерения, сбора и анализа данных об обучающихся с целью оптимизации образовательной среды [5].

В рамках технологического подхода выделяют несколько уровней адаптации: контентную (содержание), процессную (темп и последовательность), интерфейсную (формат представления) и целевую (оценочные критерии) [6]. Искусственный интеллект автоматизирует все эти уровни на основе непрерывно обновляемых данных, используя алгоритмы коллаборативной фильтрации и модели глубокого обучения для выявления латентных паттернов в образовательных данных [7].

3. Методы ИИ в адаптивных образовательных системах

Интеллектуальные обучающие системы (ITS) имитируют работу педагога-тьютора: ведут детализированную модель студента, включающую знания по предмету, типичные ошибки и историю взаимодействия, генерируя на ее основе персонализированные задания и объяснения [8].

Методы машинного обучения – логистическая регрессия, случайные леса, градиентный бустинг – применяются для прогнозирования академических рисков и раннего выявления студентов с угрозой неуспеваемости [9]. Нейросетевые языковые модели обеспечивают персонализацию на уровне педагогического взаимодействия через интеллектуальные чат-боты, способные вести диалог и адаптировать язык объяснений [10].

Цифровой двойник студента выступает интегрирующей структурой, аккумулирующей все доступные данные об обучающемся и предоставляющей унифицированный интерфейс для ИИ-алгоритмов адаптации [3].

4. Преимущества, ограничения и этические аспекты

Эффективность персонализированного ИИ-обучения подтверждена эмпирически: мета-анализ VanLehn (2011) показал, что ITS обеспечивают размер эффекта от 0,76 до 1,0 стандартного отклонения относительно традиционного обучения – результат, сопоставимый с индивидуальным репетиторством [8].

Вместе с тем внедрение ИИ сопряжено с ограничениями. Качество адаптации зависит от объема данных о студенте, что порождает проблему «холодного старта». Рекомендательные системы склонны к формированию «пузырей фильтрации», сужающих учебный опыт [11]. Наконец, построение цифрового двойника предполагает обработку чувствительных персональных данных, что ставит вопросы соответствия Федеральному закону № 152-ФЗ «О персональных данных», прозрачности алгоритмов и защиты от дискриминирующих автоматизированных решений [12].

5. Заключение

Персонализация обучения средствами ИИ представляет собой одно из наиболее перспективных направлений развития высшей школы.

Концепция цифрового двойника студента органично вписывается в данную парадигму, предоставляя информационную инфраструктуру для адаптивных педагогических систем.

Успешная реализация этого подхода требует разработки стандартов представления учебных данных, совершенствования интерпретируемых алгоритмов ИИ, формирования соответствующей правовой базы, а также подготовки педагогических кадров для работы с интеллектуальными образовательными системами. Дальнейшие исследования следует направить на изучение долгосрочных эффектов персонализации и анализ социальных последствий внедрения ИИ в образование.

Список использованных источников:

1. Bloom B.S. The 2 sigma problem: the search for methods of group instruction as effective as one-to-one tutoring // Educational Researcher. 1984. Vol. 13, № 6. P. 4-16.

2. Zawacki-Richter O., Marín V.I., Bond M., Gouverneur F. Systematic review of research on artificial intelligence applications in higher education — where are the educators? // International Journal of Educational Technology in Higher Education. 2019. Vol. 16, № 1. Art. 39.

3. Grieves M., Vickers J. Digital twin: mitigating unpredictable, undesirable emergent behavior in complex systems // Transdisciplinary Perspectives on Complex Systems. Springer, 2017. P. 85-113.

4. Выготский Л.С. Педагогическая психология. М.: Педагогика, 1991. 480 с.

5. Siemens G., Long P. Penetrating the fog: analytics in learning and education // EDUCAUSE Review. 2011. Vol. 46, № 5. P. 30-40.

6. Pane J.F., Steiner E.D., Baird M.D., Hamilton L.S. Informing Progress: Insights on Personalized Learning Implementation and Effects. RAND Corporation, 2017. 84 p.

7. Baker R.S. Stupid tutoring systems, intelligent humans // International Journal of Artificial Intelligence in Education. 2016. Vol. 26, № 2. P. 600-614.

8. VanLehn K. The relative effectiveness of human tutoring, intelligent tutoring systems, and other tutoring systems // Educational Psychologist. 2011. Vol. 46, № 4. P. 197-221.

9. Hlosta M., Zdrahal Z., Zendulka J. Ouroboros: early identification of at-risk students without models based on legacy data // Proceedings of the 7th International Learning Analytics and Knowledge Conference. ACM, 2017. P. 6-15.

10. Wollny S., Schneider J., Di Mitri D. et al. Are we there yet? A systematic literature review on chatbots in education // Frontiers in Artificial Intelligence. 2021. Vol. 4. Art. 654924.

11. Pariser E. The Filter Bubble: What the Internet Is Hiding from You. New York: Penguin Press, 2011. 294 p.
12. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» // Собрание законодательства Российской Федерации. 2006. № 31 (ч. 1). Ст. 3451.

Yakupov Y.G.
Ufa State Petroleum Technological University, Ufa

Scientific supervisor:
Popov D.V.
Ufa State Petroleum Technological University, Ufa

PERSONALIZATION OF LEARNING USING ARTIFICIAL INTELLIGENCE TECHNOLOGIES: CONCEPTUAL FOUNDATIONS AND EDUCATIONAL POTENTIAL

Abstract. The article examines the conceptual foundations of personalizing the educational process using artificial intelligence (AI) technologies. Key approaches to building adaptive learning systems are analyzed, including machine learning, natural language processing, and educational data mining. The relationship between the concept of a 'student digital twin' and personalized educational trajectories is substantiated. Advantages and limitations of AI-oriented solutions in higher education are identified, and directions for further research are outlined.

Keywords: personalized learning, artificial intelligence, adaptive educational systems, digital twin, machine learning, learning analytics.

СЕКЦИЯ 3. ОРГАНИЗАЦИОННО-ПРАВОВЫЕ АСПЕКТЫ ЗАЩИТЫ ИНФОРМАЦИИ

УДК 004.056.5:347.9

Аввакумов А.В.
Уфимский университет науки и технологий, Уфа

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

ПРОБЛЕМАТИКА ПРИМЕНЕНИЯ 152-ФЗ В СУДЕБНОЙ ВЛАСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ В АСПЕКТЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация. В статье рассматриваются особенности применения законодательства о персональных данных в судебной системе Российской Федерации. Анализируется различие подходов судов общей юрисдикции и арбитражных судов к публикации судебных актов. Выявлены основные угрозы информационной безопасности, связанные с размещением персональных данных физических лиц в открытом доступе, а также предложены меры по совершенствованию защиты информации.

Ключевые слова: персональные данные, информационная безопасность, судебная система, арбитражный суд, обезличивание, 152-ФЗ.

Цифровизация государственной власти привела к активному использованию информационных систем в судебной деятельности. Электронное правосудие обеспечивает доступность судебной защиты, ускоряет документооборот и повышает прозрачность рассмотрения дел. Вместе с тем развитие цифровых сервисов требует соблюдения требований информационной безопасности, особенно при обработке персональных данных граждан.

Основным нормативным актом в данной сфере является Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных». Его положения направлены на защиту прав граждан при обработке сведений, относящихся к определенному или определяемому физическому лицу. Для судебной системы это особенно актуально, поскольку в материалах дел содержатся паспортные данные, адреса регистрации, сведения о доходах, семейном положении, задолженностях и иная конфиденциальная информация.

В настоящее время в судебной практике наблюдается различный подход к размещению судебных актов в сети Интернет. В судах общей юрисдикции тексты решений, как правило, публикуются в обезличенном виде: исключаются фамилии участников процесса, адреса, реквизиты документов и иные идентификаторы личности. Такой подход снижает вероятность несанкционированного распространения сведений и соответствует принципам минимизации обработки данных.

Иная ситуация наблюдается в арбитражных судах. При рассмотрении дел о банкротстве граждан, корпоративных и иных экономических споров в открытом доступе часто размещаются судебные акты, содержащие фамилии, инициалы, суммы задолженности, сведения об имуществе, адресах и обязательствах физических лиц. Формально это объясняется принципом открытости правосудия и публичным характером отдельных категорий дел. Однако с позиции информационной безопасности подобная практика создает существенные риски.

Во-первых, открытая публикация персональных данных позволяет осуществлять массовый автоматизированный сбор сведений. Современные программные средства способны индексировать судебные сайты, формировать базы данных граждан, выявлять имущественное положение и финансовые проблемы конкретных лиц.

Во-вторых, полученная информация может использоваться злоумышленниками для социальной инженерии, мошенничества, фишинговых атак и вымогательства. Например, наличие сведений о банкротстве гражданина позволяет использовать психологическое давление, предлагать фиктивные юридические услуги либо направлять ложные уведомления от имени государственных органов.

В-третьих, возникает репутационный ущерб. Даже после завершения процедуры банкротства сведения о деле длительное время сохраняются в поисковых системах и агрегаторах данных, что влияет на деловую репутацию гражданина, его трудоустройство и кредитную историю.

Следовательно, в судебной системе возникает коллизия между двумя значимыми принципами: открытостью правосудия и обеспечением конфиденциальности персональных данных. С технической точки зрения проблема усугубляется отсутствием единых стандартов публикации судебных актов и недостаточной автоматизацией процессов обезличивания информации.

Для решения обозначенной проблемы целесообразно реализовать комплекс следующих мер: во-первых, необходимо унифицировать правила публикации судебных актов для всех ветвей судебной системы, во-вторых, следует внедрить программные средства автоматического выявления и сокрытия персональных данных перед размещением документов в открытом доступе, в-третьих, требуется установить

дифференцированный режим доступа к сведениям: полные тексты актов – для участников процесса и уполномоченных органов, сокращенные версии – для публичного доступа, в-четвертых, необходимо усилить контроль за соблюдением требований законодательства о защите информации в судебных информационных системах.

Таким образом, применение 152-ФЗ в судебной власти Российской Федерации требует дальнейшего совершенствования. Существующие различия между судами общей юрисдикции и арбитражными судами создают правовую и технологическую неоднородность. Приоритетной задачей становится достижение баланса между принципом гласности судопроизводства и обеспечением информационной безопасности граждан в цифровой среде.

Список использованных источников:

1. О персональных данных: Федеральный закон от 27 июля 2006 г. № 152-ФЗ // Собрание законодательства Российской Федерации. 2006. № 31. Ст. 3451.

2. Об обеспечении доступа к информации о деятельности судов в Российской Федерации: Федеральный закон от 22 декабря 2008 г. № 262-ФЗ // Собрание законодательства Российской Федерации. 2008. № 52 (ч. 1). Ст. 6217.

3. Об утверждении Доктрины информационной безопасности Российской Федерации: Указ Президента Российской Федерации от 5 декабря 2016 г. № 646 // Собрание законодательства Российской Федерации. 2016. № 50. Ст. 7074.

4. Арбитражный процессуальный кодекс Российской Федерации: Федеральный закон от 24 июля 2002 г. № 95-ФЗ // Собрание законодательства Российской Федерации. 2002. № 30. Ст. 3012.

5. Гражданский процессуальный кодекс Российской Федерации: Федеральный закон от 14 ноября 2002 г. № 138-ФЗ // Собрание законодательства Российской Федерации. 2002. № 46. Ст. 4532.

6. О несостоятельности (банкротстве): Федеральный закон от 26 октября 2002 г. № 127-ФЗ // Собрание законодательства Российской Федерации. 2002. № 43. Ст. 4190.

7. В.М. Пискайкина, А.Г. Монетов Проблема защиты персональных данных в эпоху цифровизации // https://cyberleninka.ru/article/n/problema-zaschity-personalnyh-dannyh-v-epohu-tsifrovizatsii/viewer.

8. Солдатов А.В. Организационно - правовые проблемы деятельности по размещению в сети «интернет» текстов судебных актов // https://cyberleninka.ru/article/n/organizatsionno-pravovye-problemy-deyatelnosti-po-razmescheniyu-v-seti-internet-tekstov-sudebnyh-aktov/viewer.

Avvakumov A.V.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Fatkhelislamov A.F.
Ufa University of Science and Technology, Ufa

PROBLEMS OF THE APPLICATION OF FEDERAL LAW NO. 152-FZ IN THE JUDICIAL SYSTEM OF THE RUSSIAN FEDERATION IN THE ASPECT OF INFORMATION SECURITY

Abstract. The article examines the specific features of applying personal data legislation within the judicial system of the Russian Federation. It analyzes the differences in approaches between courts of general jurisdiction and arbitration courts regarding the publication of judicial acts. The main information security threats associated with the public disclosure of personal data of individuals are identified, and measures aimed at improving information protection are proposed.

Keywords: personal data, information security, judicial system, arbitration court, depersonalization, Federal Law No. 152-FZ.

УДК 004.056

Александрова В.М.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Яппаров Р.М.
Уфимский университет науки и технологий, Уфа

СОВЕРШЕНСТВОВАНИЕ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ В ПРАВООХРАНИТЕЛЬНЫХ ОРГАНАХ: АНАЛИЗ УГРОЗ И НАПРАВЛЕНИЯ РАЗВИТИЯ

Аннотация. В статье рассмотрены актуальные проблемы обеспечения информационной безопасности в правоохранительных органах. Проведен анализ специфических угроз, возникающих при обработке информации ограниченного доступа. Выделены основные направления совершенствования организационных и технических мер защиты информации.

Ключевые слова: информационная безопасность, правоохранительные органы, защита информации, угрозы, органы внутренних дел.

В условиях повсеместного внедрения цифровых технологий в сферу государственного управления, вопросы обеспечения защиты данных в структурах правоохранительных органов приобретают первостепенное значение, играя ключевую роль в поддержании стабильности общества и государственной безопасности [1]. Основная специфика деятельности органов внутренних дел заключается в обращении с масштабными массивами служебной информации, включая персональные данные граждан, материалы расследований и оперативные сведения. Функционирование информационных систем в рамках правоохранительных органов требует баланса между скоростью обработки данных и надежностью их защиты, обеспечивая конфиденциальность, целостность и доступность. При изучении деятельности правоохранительных органов выявляются специфические угрозы, связанные с характером их профессиональных функций. Криминальные элементы часто нацелены на информационный поток, используя агентов для намеренного искажения данных с целью дезинформации [2]. Многообразие источников поступления информации, как отмечается в научных трудах, увеличивает вероятность возникновения рисков, затрудняющих выполнение служебных задач [3]:

1. Вероятность утечки закрытых сведений по каналам связи. Использование незащищенных средств передачи информации увеличивает риск перехвата служебных данных. Эта проблема особенно проявляется при трансграничном обмене информацией.

2. Риски, связанные с действиями персонала. Недостаточный уровень цифровой грамотности сотрудников, пренебрежение установленными правилами работы с данными и формальный подход к обучению часто приводят к ситуациям, способствующим компрометации защищаемой информации.

3. Угрозы, связанные с методами социальной инженерии. Целенаправленное психологическое манипулирование сотрудниками для получения их учетных данных и несанкционированного доступа к информации. Учитывая высокий уровень взаимодействия сотрудников с населением, данный вид угроз приобретает особую актуальность.

4. Риски, связанные с нарушением доступности информационных ресурсов. Технические сбои, перебои в энергоснабжении, а также атаки вредоносным ПО могут привести к блокировке доступа к информационным системам.

Информационная безопасность является фундаментальной составляющей национальной безопасности, успешное обеспечение которой достигается за счет слаженной работы множества участников [4]. Их деятельность регулируется федеральным законодательством, ведомственными нормативными актами МВД, а также руководящими

документами ФСТЭК и ФСБ. Тем не менее, существующая законодательная и нормативная база требует дальнейшего усовершенствования. В первую очередь, необходимо разработать единые стандарты для различных типов информационных систем, учитывая их уникальные особенности, для унификации требований к защите информации. Во-вторых, требуется четко определить процедуры межведомственного обмена данными, установив обязательное применение сертифицированных средств криптографической защиты. Также важно ужесточить ответственность сотрудников за несоблюдение установленных правил работы с конфиденциальными данными.

Для эффективного парирования угроз в условиях усложняющейся архитектуры информационных систем необходимо модернизировать технические средства, обеспечивающие защиту обрабатываемых данных, в том числе и в системе правоохранительных органов. К основным направлениям следует относить [5]:

1. Интеграцию систем раннего обнаружения и пресечения вторжений (IDS/IPS). Современные аналитические инструменты сетевого трафика позволяют своевременно выявлять следы атак и автоматически нейтрализовывать несанкционированные действия.

2. Применение средств криптографической защиты данных. Использование сертифицированных криптошлюзов для всех магистралей передачи информации является обязательным условием для гарантии конфиденциальности при обмене данными как между различными организациями, так и внутри самой структуры.

3. Формирование изолированного сегмента для обработки данных с ограниченным доступом. Физическое и логическое обособление информационных ресурсов от общеведомственной сети существенно снижает вероятность их компрометации.

4. Внедрение систем контроля действий пользователей. Решения класса DLP (Data Loss Prevention) отслеживают передачу конфиденциальной информации по разрешенным каналам связи, пресекая попытки несанкционированного копирования и пересылки данных.

Анализ инцидентов в сфере информационной безопасности, произошедших в правоохранительных структурах, показывает, что основная масса нарушений вызвана человеческим фактором. Следовательно, одним из ключевых аспектов в улучшении системы защиты является повышение осведомленности персонала. Программа непрерывного обучения должна включать: регулярные тренинги с акцентом на актуальные методы социальной инженерии и фишинга; практические упражнения по выявлению признаков компрометации сведений; проверку знаний правил обращения с портативными накопителями информации; отработку алгоритмов действий при

обнаружении признаков нарушений информационной безопасности. Формирование устойчивых навыков безопасного поведения и осознание личной ответственности за сохранность служебной информации представляют собой неотъемлемый компонент эффективного механизма защиты.

Обеспечение информационной безопасности в правоохранительных органах в современных условиях требует комплексного подхода, который охватывает модернизацию нормативно-правовой базы, применение передовых технических средств защиты и планомерную работу с личным составом. Основными векторами совершенствования системы защиты информации являются: стандартизация требований к безопасности, внедрение криптографических технологий и инструментов мониторинга активности пользователей, а также организация систематического обучения персонала. Реализация данных мер позволит существенно повысить уровень защиты информационных активов правоохранительных органов, минимизировать риски утечки конфиденциальных сведений и обеспечить эффективное противодействие современным информационным угрозам.

Список использованных источников:

1. Информатизация и информационная безопасность правоохранительных органов: сборник трудов Международной научно-практической конференции / под общ. ред. А. В. Бецкова. – Москва: Академия управления МВД России, 2024. – 330 с. – ISBN 978-5-907721-31-9. – Текст: электронный // Национальная электронная библиотека (НЭБ). – URL: https://rusneb.ru/catalog/ (дата обращения: 03.04.2026).

2. Николаев, О. Э. Угрозы информационной безопасности при осуществлении оперативно-розыскной деятельности и основные пути их отражения / О. Э. Николаев // Юридическая наука и практика: Вестник Нижегородской академии МВД России. – 2020. – № 4. – С. 30-35. – ISSN 2078-5356. – Текст: электронный // Научная электронная библиотека eLibrary.ru. – URL: https://www.elibrary.ru/item.asp?id=44428635 (дата обращения: 02.04.2026).

3. Страхов, А. А. Основы кибербезопасности: учебник / А. А. Страхов, Н. М. Дубинина, Н. В. Задохина [и др.]. – Москва: Московский университет МВД России им. В. Я. Кикотя, 2024. – 307 с. – ISBN 978-5-9694-1477-8. – УДК 004.056(075.8). – Текст: электронный // Электронная библиотека СибЮИ МВД России. – URL: http://lib.sibli.ru/elib/0086703.pdf (дата обращения: 01.04.2026).

4. Мильшин, Ю. Н. К вопросу об обеспечении информационной безопасности / Ю. Н. Мильшин // Теология. Философия. Право. – 2024. – № 2 (22). – С. 53-61. – ISSN 2782-4473. – Текст: электронный // Научная

электронная библиотека eLibrary.ru. – URL: https://www.elibrary.ru/item.asp?id=67314578 (дата обращения: 05.04.2026).

5. Исмагилова А.С. Алгебраические инструменты для построения криптографических систем / А.С. Исмагилова // Кибернетика и информационная безопасность "КИБ-2025": Сборник научных трудов Третьей Всероссийской научно-технической конференции. В 2-х томах, Москва, 03–04 декабря 2025 года. – Москва: Национальный исследовательский ядерный университет МИФИ, 2025. – С. 114-115. – EDN DDMYVA. – Текст: электронный // Научная электронная библиотека eLibrary.ru. – URL: https://elibrary.ru/item.asp?id=88832315 (дата обращения: 02.04.2026).

Aleksandrova V. M.
Ufa university of science
and technology, Ufa

Yapparov R.M.
Ufa university of science
and technology, Ufa

IMPROVEMENT OF THE INFORMATION SECURITY SYSTEM IN LAW ENFORCEMENT AGENCIES: THREAT ANALYSIS AND DEVELOPMENT DIRECTIONS

Abstract. The article examines current problems of ensuring information security in law enforcement agencies. The analysis of specific threats arising from the processing of restricted information is carried out. The main directions for improving organizational and technical measures for information protection are identified.

Keywords: information security, law enforcement agencies, information protection, threats, internal affairs bodies.

УДК 004.056

Аскарова Г.Ф.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Яппаров Р.М.
Уфимский университет науки и технологий, Уфа

АНАЛИЗ ПРОЦЕССА УПРАВЛЕНИЯ УЯЗВИМОСТЯМИ НА ПРИМЕРЕ ДЕЯТЕЛЬНОСТИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

Аннотация. В статье анализируется процесс управления уязвимостями на примере обеспечения информационной безопасности деятельности органов внутренних дел. Рассмотрен непрерывный цикл: выявление, оценка, приоритизация и устранение уязвимостей. Приведены данные инцидентов, связанных с персоналом, и среднем сроке их устранения и др. Предлагаются решения и новые подходы управления уязвимостями.

Ключевые слова: управление уязвимостями, информационная безопасность, ОВД, риск, уязвимость, мониторинг, защита данных

Управление уязвимостями описывается как непрерывный процесс, и это сразу задает рамку анализа. Процесс управления уязвимостями − это непрерывный цикл выявления, оценки, приоритизации, устранения и мониторинга слабых мест в IT-инфраструктуре. Он направлен на снижение ущерба от реализации угроз [1]. Управление уязвимостями – не разовое событие, а постоянная работа.

Она начинается с инвентаризации активов – это исходная стадия. Далее формируется база уязвимостей и проводится их оценка, часто с использованием шкалы риска. Ключевой момент - переход от практики устранения всех уязвимостей к их приоритизации, поскольку не все уязвимости несут одинаковый риск.

Однако существуют расхождения в подходах. Морозов В.Е. и Милославская Н.Г. рассматривают управление ИБ как циклический процесс, включающий сбор и анализ данных, оценку рисков и планирование мер [2]. Их модель шире и охватывает всю систему безопасности. Если у нас акцент на техническом цикле, то у этих авторов − на управленческом контуре. Тем не менее необходима интеграция: управление уязвимостями связано с мониторингом событий безопасности, управлением инцидентами и конфигурациями [1].

Статистика по государственным информационным системам усиливает аргумент о необходимости такого процесса. По данным

Гавдана Г.П. и соавторов, свыше 50% государственных информационных систем подвергались серьезным угрозам отказа [3]. Причем 85% инцидентов связаны с действиями сотрудников [3]. Здесь прослеживается слабое место: необходимо больше концентрироваться на технических уязвимостях, однако человеческий фактор выходит за рамки технической модели.

Это хорошо видно с точки зрения специфики работы органов внутренних дел (ОВД). Обеспечение информационной безопасности в ОВД − это система стратегических, организационных и технических мер [1]. Акцент на технической стороне − сознательное упрощение, хотя оно не бесспорно.

Дополняет картину правовой аспект. Русскевич Е.А. определяет информационную безопасность как состояние защищенности личности, общества и государства [4]. Регулирование характеризуется многоуровневостью и сложностью [4]. При этом уголовная ответственность за нарушения управления средствами защиты наступает только при третьем нарушении [4], что снижает оперативность реагирования.

В итоге складывается неоднозначная ситуация. С одной стороны, выстраивается четкий процесс управления уязвимостями как последовательность этапов. С другой − нормативная среда и организационные факторы усложняют его реализацию. Техническая модель без учета правовых и человеческих факторов остается неполной.

Для более полной картины, позволяющей уяснить суть происходящих процессов, логично перейти к анализу конкретных моделей и инструментов, позволяющих реализовать этот процесс на практике.

Практическая реализация управления уязвимостями требует формализации [5]. Якименко К.В. и Золотарев В.В. предлагают использовать гетерогенные графы, где система представляется через операции, информационные системы и данные [6]. Цифровая трансформация − это цепочка переходных состояний [6], что увеличивает поверхность атаки. Вводятся количественные показатели: количество критических путей, уровень центральности узлов, индекс распределенности данных, время восстановления, уровень автоматизации защиты [6]. Чем больше критических путей, тем выше риск; необходимо стремиться к их минимизации [6]. Однако такие модели требуют постоянного обновления, что сложно и не всегда реализуемо в условиях деятельности ОВД. Тем не менее идея количественной оценки позволяет уйти от субъективности.

Технические инструменты: Морозов В.Е. и Милославская Н.Г. предлагают минимальный набор: систему мониторинга событий,

контроля утечек и анализа доступа [2]. С 2022 года рост числа инцидентов приобрел взрывной характер [2]. Среднее время устранения уязвимостей составляет 14 дней при нормативе 24 часа [3]. Разрыв огромный - система не успевает реагировать. При этом около 85% инцидентов связаны с действиями сотрудников [3]. Это уже не только техническая проблема.

Необходима интеграция управления уязвимостями с мониторингом, управлением инцидентами и конфигурациями [1]. Это сближает нас с моделью Морозова В. Е., но у нее меньше внимания к инструментам и больше − к последовательности действий.

Система управления информационной безопасностью должна учитывать видение, стратегию, цели, политики, стандарты и процессы [7]. Хади М.А. и Абдулредхи М.Н. выводят управление безопасностью на уровень организации, рассматривая безопасность как часть корпоративного управления [7]. Вводится матрица ответственности, где определяется, кто отвечает за процессы [7]. «Эффективность системы зависит от понимания ролей всеми сотрудниками» [7]. Но на практике это работает не всегда, есть и правовые ограничения.

Русскевич Е. А. отмечает, что регулирование в сфере обеспечения ИБ характеризуется многоуровневостью и сложностью [4]. Ответственность за нарушения централизованного управления наступает только при третьем нарушении [4], что снижает эффективность контроля. Это противоречит логике непрерывного управления уязвимостями, требуещего быстрого реагирования.

Якименко К. В. предлагает учитывать время восстановления как отдельную метрику [6], что связано с устойчивостью системы. В условиях ОВД такие показатели часто не фиксируются.

В итоге, получается противоречивая картина. С одной стороны, есть математические модели и автоматизированные системы. С другой − организационные ограничения и человеческий фактор, причем последний доминирует (85% инцидентов) [3]. Технические решения предполагают автоматизацию и количественную оценку. Организационные подходы делают упор на регламенты и роли. А правовая база добавляет ограничения.

Проще говоря, управление уязвимостями оказывается на пересечении трех систем. И ни одна из них не дает полного решения. Комбинация подходов выглядит наиболее реалистичной. Без интеграции моделей, инструментов и организационных механизмов процесс управления уязвимостями остается фрагментарным.

Список использованных источников:

1. Прохоров С.А., Федосеев А.А., Иващенко А.В. Автоматизация комплексного управления безопасностью предприятия /Самара: СНЦ РАН, 2008 – 55 с.

2. Морозов В.Е., Милославская Н.Г. Комплексные решения для минимизации внутренних угроз информационной безопасности // Вопросы кибербезопасности. – 2024. – № 5 (63). – С. 67–78. – DOI: 10.21681/2311-3456-2024-5-67-78.

3. Гавдан Г.П., Голубев А.А., Голубев А.Г. и др. Обеспечение безопасности государственных информационных систем как объектов критической информационной инфраструктуры // Безопасность информационных технологий. – 2025. – Т. 32, № 3. – С. 26–43. – DOI: 10.26583/bit.2025.3.03.

4. Русскевич Е.А. Нарушение правил централизованного управления техническими средствами противодействия угрозам информационной безопасности // JournalofDigitalTechnologiesandLaw. – 2023. – Т. 1, № 3. – С. 650–672. – DOI: 10.21202/jdtl.2023.28.

5. Исмагилова А.С. Алгебраические инструменты для построения криптографических систем / А.С. Исмагилова // Кибернетика и информационная безопасность "КИБ-2025": Сборник научных трудов Третьей Всероссийской научно-технической конференции. В 2-х томах, Москва, 03–04 декабря 2025 года. – Москва: Национальный исследовательский ядерный университет МИФИ, 2025. – С. 114-115. – EDN DDMYVA. – Текст: электронный // Научная электронная библиотека eLibrary.ru. – URL: https://elibrary.ru/item.asp?id=88832315 (дата обращения: 02.04.2026).

6. Якименко К.В., Золотарев В.В. Управление информационной безопасностью в процессе цифровой трансформации: моделирование на основе гетерогенных графов и метрик риска // Известия ЮФУ. Технические науки. – 2025. – № 3 (245). – С. 246–256. – DOI: 10.18522/2311-3103-2025-3-246-256.

7. Хади М.А., Абдулредха М.Н. Универсальная система управления информационной безопасностью: организационно-правовые принципы // JournalofDigitalTechnologiesandLaw. – 2025. – Т. 3, № 1. – С. 125–142. – DOI: 10.21202/jdtl.2025.6.

Askarova G.F.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Yapparov R.M.
Ufa University of Science and Technology, Ufa

ANALYSIS OF THE VULNERABILITY MANAGEMENT PROCESS ON THE EXAMPLE OF INTERNAL AFFAIRS BODIES

Abstract. The paper examines the construction of a vulnerability management process in a regional IFA unit. It outlines a continuous cycle including identification, assessment, prioritization and remediation of vulnerabilities. Statistical data are considered: 85% of incidents relate to personnel, while average remediation time reaches 14 days versus a 24-hour target. Simply put, the approach combines technical and organizational controls, though sometimes it feels slightly overloaded.

Keywords: vulnerability management, information security, IFA, risk, vulnerabilities, monitoring, critical infrastructure, data protection.

УДК 004

Баянов К.А.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Салов И.В.
Уфимский университет науки и технологий, Уфа

ПАРАДОКС ФОРМАЛЬНОЙ ЗАЩИЩЕННОСТИ: ПРАВОВЫЕ РИСКИ РЕАЛИЗАЦИИ ТРЕБОВАНИЙ ФСТЭК РОССИИ В ГОСУДАРСТВЕННЫХ УЧРЕЖДЕНИЯХ

Аннотация. В данной статье рассмотрена проблема формального соблюдения требований ФСТЭК России в государственных учреждениях. Установлено, что наличие внедренных защитных механизмов само по себе не гарантирует реальной защищенности информационных систем. Определены основные правовые риски, возникающие в случае несоответствия между установленными законом требованиями и фактическими трудностями их реализации.

Ключевые слова: ФСТЭК России, информационная безопасность, государственные учреждения, правовые риски, формальная защищенность.

В деятельности органов государственной власти защита информации занимает все более значимое место: нарастающие потоки обрабатываемых сведений и планомерное ужесточение регуляторных стандартов придают этой сфере особую значимость. Вместе с тем на практике обеспечение информационной безопасности нередко сводится к документальному подтверждению соответствия предписаниям ФСТЭК России, а не к фактическому противодействию угрозам. Существование пакета согласованной документации, набора задекларированных мер и принятых организационных регламентов отнюдь не свидетельствует о том, что система надежно ограждена от реальных атак и инцидентов.

Особое внимание следует уделить Приказу ФСТЭК России № 117 от 11 апреля 2025 года, который вступил в силу с 1 марта 2026 года. Данный приказ значительно ужесточает требования к информационной безопасности в государственных информационных системах: расширяет перечень обязательных организационных и технических мер, а также устанавливает более строгие требования к моделированию угроз и выбору мер защиты. Важно отметить, что данный документ уделяет особое внимание не только техническим решениям, но и обязательствам по разработке локальных нормативных актов, проведению регулярных аудитов и обеспечению непрерывного управления безопасностью. Для реализации этих требований потребуются значительные ресурсы и коренной пересмотр существующих подходов к организации информационной безопасности в государственных органах.

Актуальность темы обусловлена тем, что государственные учреждения подвергаются усиленному нормативному контролю и обязаны в полной мере выполнять требования к информационной защите. В то же время реальная практика показывает, что многие меры реализуются лишь на бумаге: документы составляются без учета особенностей информационной системы, процедуры выполняются от случая к случаю, а контроль за их соблюдением носит чисто формальный характер. Это приводит к парадоксу, при котором система, на первый взгляд, соответствует требованиям, но на самом деле остается уязвимой.

Проблема заключается в том, что формальное соблюдение требований регулятора может создать видимость достаточного уровня безопасности, но при этом создавать юридические риски для организации. Если меры защиты являются неполными, реализуются с задержкой или внедряются без учета реальных условий эксплуатации информационных систем, это может привести к замечаниям со стороны надзорных органов, административной ответственности и даже необходимости корректировки уже внедренных решений. Таким образом, с юридической точки зрения формальная безопасность становится не преимуществом, а слабым местом.

В таких условиях организационные и юридические аспекты играют особенно важную роль. Государственные учреждения должны не только внедрять меры защиты, но и обеспечить наличие механизмов, контролирующих соблюдение законодательства, правил доступа, процедур реагирования на инциденты и требований. Если эти документы существуют только для целей аудита и на практике не применяются, система управления информационной безопасностью теряет свою практическую ценность.

Особое внимание следует уделить вопросу ответственности руководителей и сотрудников. Ненадлежащая организация процессов защиты данных, отсутствие внутреннего контроля, а также задержки с обновлением документации могут привести к тому, что ответственность за инциденты будет лежать не только на исполнителях, но и на руководителях, которые принимали решения о введении или несоблюдении предписанных мер. В связи с этим юридические знания и управленческая дисциплина в сфере информационной безопасности приобретают еще большее значение.

С 1 марта 2026 года Приказ ФСТЭК № 117 расширил область применения до всех информационных систем государственных органов, унитарных предприятий и учреждений, заменив устаревший Приказ № 17. Новые требования к непрерывной отчетности (КЗИ раз в полгода), кадровому составу ИБ-подразделения (30% с профильным образованием) и процессуальному подходу по циклу Деминга создают риски для организаций, формально выполняющих старые регламенты. Наиболее серьезным последствием становится приостановка эксплуатации ГИС и внеплановые проверки ФСТЭК за показатель КЗИ ниже 0,9 [1]. Правовые риски формального выполнения требований ФСТЭК № 117 закреплены в Кодексе об административных правонарушениях в ст. 13.12 КоАП РФ, несоблюдение требований влечет административные штрафы должностным лицам до 50000 рублей [2].

Таким образом, парадокс формальной безопасности заключается в несоответствии между законодательными требованиями и мерами безопасности, зафиксированными на бумаге; зачастую это создает лишь иллюзию безопасности, в то время как фактический уровень безопасности в организации остается критически низким. Это особенно опасно для государственных органов, поскольку влечет за собой не только технические, но и правовые риски. Эффективная защита информации возможна только при комплексном подходе, который, помимо соблюдения нормативных требований, включает в себя конкретные организационные меры, регулярный мониторинг и адаптацию мер безопасности к конкретным условиям той или иной информационной системы. В качестве решения этой проблемы предлагается переход от

документально-ориентированной модели обеспечения соответствия к модели управления информационной безопасностью, основанной на оценке рисков. Эта модель предполагает, во-первых, внедрение системы непрерывного внутреннего контроля с распределением ответственности между подразделениями организации, а не только в рамках отдела информационной безопасности. Во-вторых, необходима разработка типовых регламентов с образцами моделей угроз и локальных нормативных актов, актуализированных под требования Приказа ФСТЭК № 117, что снизит правовую вариативность между учреждениями. В-третьих, требуется создание механизма непрерывного профессионального обучения специалистов, ориентированного на практические навыки реагирования на инциденты, а не на формальное выполнение кадрового критерия в 30%. В-четвертых, внедрение автоматизированных инструментов мониторинга показателя КЗИ в режиме реального времени позволит своевременно выявлять отклонения от порогового значения 0,9 и оперативно устранять недостатки – до, а не после плановой полугодовой отчетности. Наконец, необходимо законодательно закрепить персональную ответственность руководителей учреждений за организацию функционирующей, а не декларативной системы информационной безопасности, подкрепленную регулярным внутренним аудитом. Только при последовательной реализации перечисленных мер возможно преодоление сложившегося парадокса и достижение фактически высокого уровня защищенности государственных информационных систем в условиях ужесточающихся требований регулятора. Следует также подчеркнуть, что описанный парадокс не является сугубо российской спецификой: аналогичные проблемы соответствия нормативным требованиям при сохранении реальных уязвимостей фиксируются в международной практике информационной безопасности. Однако в отечественном контексте они приобретают особую остроту ввиду одновременного ужесточения регуляторных требований, хронической нехватки квалифицированных кадров и недостаточного финансирования ИБ-подразделений в государственном секторе. В этой связи системное решение проблемы требует скоординированных усилий как со стороны самих учреждений, так и со стороны регулятора – прежде всего в части обеспечения методической поддержки и выработки реалистичных, верифицируемых критериев оценки фактического уровня защищенности. Принятие Приказа ФСТЭК № 117 создает для этого необходимую нормативную основу; задача теперь состоит в том, чтобы его реализация не воспроизвела те же формальные паттерны, с которыми призвана бороться. Достижение этой цели возможно лишь при условии, что требования регулятора воспринимаются не как внешнее обязательство, исполнение которого

нужно задокументировать, а как инструмент формирования подлинной культуры информационной безопасности, пронизывающей все уровни государственного управления – от технических специалистов до руководителей высшего звена.

Список использованных источников:

1. Приказ ФСТЭК России от 11.04.2025 № 117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений».

2. Кодекс об административных правонарушениях РФ Статья 13.12. Нарушение правил защиты информации. URL: https://www.consultant.ru/document/cons_doc_LAW_34661/721c5c0cd868c2438ea66f09091f3a352bd56365/.

Bayanov K.A.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Salov I.V.
Ufa University of Science and Technology, Ufa

THE PARADOX OF FORMAL PROTECTION: LEGAL RISKS ASSOCIATED WITH THE IMPLEMENTATION OF THE RUSSIAN FEDERAL SERVICE FOR ELECTRONIC COMMUNICATIONS, INFORMATION TECHNOLOGY, AND MASS MEDIA'S REQUIREMENTS IN GOVERNMENT AGENCIES

Abstract. This article examines the issue of formal compliance with the requirements of the FSTEC of Russia in government agencies. It has been established that the mere existence of implemented security mechanisms does not in itself guarantee the actual security of IT systems. The article identifies the main legal risks that arise when there is a discrepancy between statutory requirements and the practical difficulties of implementing them.

Keywords: FSTEC of Russia, information security, government agencies, legal risks, formal security.

УДК 003

Биктубаева К.С.
Уфимский университет науки и технологий, Уфа

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

ОРГАНИЗАЦИОННО-ПРАВОВЫЕ АСПЕКТЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ЦИК РЕСПУБЛИКИ БАШКОРТОСТАН С УЧЕТОМ НОВЫХ ТРЕБОВАНИЙ ФСТЭК РОССИИ

Аннотация. Обеспечение информационной безопасности избирательных процессов является ключевым элементом защиты суверенитета. В статье рассматриваются организационно-правовые механизмы обеспечения информационной безопасности на примере ЦИК РБ. Особое внимание уделено новым требованиям Приказа ФСТЭК России №117 от 11.04.2025. Проведен сравнительный анализ между текущим состоянием ИБ в ЦИК РБ и новыми требованиями, сформулированы конкретные предложения по совершенствованию существующей системы защиты информации.

Ключевые слова: информационная безопасность, ЦИК РБ, ГАС «Выборы», ФСТЭК России, анализ состояния.

Правовой статус Центральной избирательной комиссии Республики Башкортостан (далее ЦИК РБ) определен статьей 20 Кодекса Республики Башкортостан от 06.12.2006 г. №380-з «О выборах». Деятельность избирательных комиссий напрямую связана с обработкой информации, нарушения целостности, конфиденциальности или доступности которой может нанести ущерб безопасности государства. В связи с этим организационно-правовые аспекты защиты информации приобретают актуальность, поскольку именно они формируют и регламентируют нормативную, процедурную и кадровую основу всей системы ИБ. ЦИК РБ является держателем значительного числа защищаемой информации и информационных ресурсов, а также на комиссию возложены функции сбора и обработки информации, связанной с организацией и проведением выборов – от подготовки до проведения итогов.

Согласно официальным данным, Интернет-портал ЦИК России с 1 июня 2025 года подвергся 15,3 миллиона кибератак, свыше 12 млн кибератак были совершены на информационные ресурсы за время президентской избирательной кампании. Эти данные подтверждают, что

технические меры защиты неэффективны без четко определенной организационно-правовой системы, регулирующей все аспекты деятельности.

Ключевым событием стало вступление в силу Приказа ФСТЭК России №117 от 11.04.2025 г. «Требования о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений». Основными нововведениями в организационно-правовые основы в соответствии с Приказом ФСТЭК России №117 являются:

1. Расширение сферы деятельности. Приказ распространяется на все информационные системы государственных органов, унитарных предприятий и учреждений.

2. Приказ №117 устанавливает конкретные цели защиты информации, а именно: недопущение или снижение вероятности негативных последствий от нарушений конфиденциальности, целостности, доступности сведений, а также сбоев в работе информационных систем.

3. Не менее 30 процентов работников структурного подразделения по защите информации должны иметь профильное образование в данной области либо пройти профессиональную переподготовку.

4. Настоящее Требование обязывает оператора разработать и утвердить Политику информационной безопасности, внутренние стандарты и регламенты.

5. Приказ №117 вводит обязанности для сторонних организаций соблюдать внутреннюю политику информационной безопасности заказчика и подтверждать это документально.

6. Контроль: оценка защищенности не реже 2 раз в год, уведомление ФСТЭК об уязвимостях за 5 дней, устранение критических – до 24 часов, высокоопасных – до 7 дней.

7. Приказ №117 уделяет внимание вопросам безопасности при использовании ИИ. При использовании в информационных системах искусственного интеллекта или сервисов на его основе должны применяться доверенные технологии ИИ или их компоненты.

В целях выявления необходимости изменений в системе организационно-правового обеспечения ИБ ЦИК РБ был проведен сравнительный анализ действующего состояния и требований Приказа ФСТЭК России №117.

В результате анализа установлено, что:

1) действующая штатная структура подразделения ИБ ЦИК РБ не гарантирует выполнения требования о наличии профильного образования

у 30% сотрудников (требуется проверка личных дел и, при необходимости, направление на переподготовку);

2) внутренние нормативные документы ЦИК РБ не актуализированы под положения Приказа №117, что подтверждается отсутствием в них ссылок на данный документ, требований к ИИ и обязанностей для подрядных организаций;

3) регламенты ЦИК РБ не устанавливают периодичность оценки защищенности (не реже 2 раз в год) и сроки устранения уязвимостей (24 часа и 7 дней), что создает риск несвоевременного реагирования на инциденты.

Таким образом, подтверждается необходимость пересмотра всех трех компонентов организационно-правовой системы ИБ ЦИК РБ.

С учетом вышеизложенного, для ЦИК РБ необходима реализация следующих организационно-правовых мер:

1. Привести нормативную базу на соответствие Требованиям Приказа ФСТЭК России №117, а именно обновить Политику ИБ, проводить регулярное обучение всех сотрудников противодействию фишингу и социальной инженерии.

2. Необходимо провести проверку квалификации сотрудников подразделения ИБ, организовать профессиональную переподготовку (обучение) сотрудников, а также обеспечить регулярное обучение всех работников вопросам информационной безопасности.

3. Создать пакет документов, включая Регламент разграничения доступа, Модель угроз безопасности информации, Инструкцию о действиях при происшествиях в сфере информационной безопасности, Положение об обработке персональных данных, План обеспечения непрерывности деятельности и восстановление избирательного процесса.

4. Внедрить SIEM-системы, проводить оценку защищенности каждые полгода и оценку процессов ИБ раз в два года, уведомлять ФСТЭК об уязвимостях в течение 5 дней.

5. Требуется включить в договоры со сторонними организациями, обслуживающими информационные системы, положения о соблюдении внутренних правил ИБ ЦИК РБ, ограничить доступ работников привлекаемых организаций к действующей эксплуатационной среде, а также предусмотреть документальное подтверждение выполнения указанных требований.

6. Внедрить средства защиты информации с сертификацией ФСТЭК от несанкционированного доступа, межсетевые экраны, антивирусную защиту, анализ уязвимостей, DLP-систему.

7. Организовать физическую защиту, а именно контроль доступа в серверные, установка видеонаблюдения, охранной сигнализации, бесперебойного питания.

Вступление в силу Приказа ФСТЭК России №117 от 11.04.2025 г. требует от ЦИК РБ пересмотра и обновления организационно-правовой системы обеспечения информационной безопасности. Ключевыми являются: приведение нормативной базы в соответствии с новыми требованиями, обеспечение кадрового состава подразделений ИБ квалифицированными специалистами, внедрение регулярного мониторинга и отчетности, усиление контроля за подрядными организациями, а также регламентация использования новых технологий в избирательном процессе. Выполнение указанных требований вместе с внедрением сертифицированных средств защиты информации повысит устойчивость информационной инфраструктуры к современным угрозам. Без строго выстроенной организационно-правовой основы любая защита становится неэффективной.

Список использованных источников:

1. Приказ ФСТЭК России от 11.04.2025 № 117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений» [Электронный ресурс]. URL: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/trebovaniya-utverzhdeny-prikazom-fstek-rossii-ot-11-aprelya-2025-g-n-117.

2. Федеральный закон от 10.01.2003 № 20-ФЗ «О Государственной автоматизированной системе Российской Федерации «Выборы» [Электронный ресурс] // КонсультантПлюс: справочно-правовая система / Режим доступа: URL: http://base.www.consultant.ru/.

3. Кодекс Республики Башкортостан «О выборах» [Электронный ресурс]. URL: https://docs.cntd.ru/document/450366898?ysclid=mhd9i6ipov190019

4. Официальный сайт Центральной Избирательной комиссии Российской Федерации. URL: http://www.cikrf.ru/?]A?1. – [Электронный ресурс].

5. Организационное и правовое обеспечение информационной безопасности: учебник для вузов / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов; под редакцией Т. А. Поляковой, А. А. Стрельцова. – 2-е изд., перераб. и доп. – Москва: Издательство Юрайт, 2026. – 357 с. – Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/583236.

Biktubaeva K.S.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Shagapov I.A.
Ufa University of Science and Technology, Ufa

ORGANIZATIONAL AND LEGAL ASPECTS OF INFORMATION SECURITY IN THE CEC OF THE REPUBLIC OF BASHKORTOSTAN, TAKING INTO ACCOUNT THE NEW REQUIREMENTS OF THE FSTEC OF RUSSIA

Abstract. Ensuring the information security of electoral processes is a key element in protecting sovereignty. This article examines the organizational and legal mechanisms for ensuring information security using the example of the Central Election Commission of the Republic of Bashkortostan. Special attention is given to the new requirements of Order No. 117 of the Federal Service for Technical and Export Control of Russia dated April 11, 2025. A comparative analysis is conducted between the current state of information security in the Central Election Commission of the Republic of Bashkortostan and the new requirements, and specific information protection measures are proposed.

Keywords: information security, Central Election Commission of the Republic of Bashkortostan, GAS «Vybory», Federal Service for Technical and Export Control of Russia, status analysis.

УДК 004.056

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

Научный руководитель:
Яппаров Р.М.
Уфимский университет науки и технологий, Уфа

К ВОПРОСУ О СОВЕРШЕНСТВОВАНИИ МЕХАНИЗМОВ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Аннотация. В статье анализируются судебные решения за 2025 год, в которых граждане оспаривали договоры займа, оформленные с использованием их персональных данных без согласия. Исследуются источники получения персональных данных мошенниками, способы обхода идентификации и правовые позиции судов. Рассматривается

механизм самозапрета на кредиты. Предложены меры по защите прав субъектов обработки персональных данных.

Ключевые слова: персональные данные, незаконная обработка, договор займа, судебная практика, 152-ФЗ.

В 2024-2025 гг. законодательство о персональных данных (далее - ПДн) было ужесточено: введена уголовная ответственность по ст. 272.1 Уголовного кодекса Российской Федерации (далее – УК РФ) [1], а также увеличены штрафы по ст. 13.11 Кодекса Российской Федерации об административных правонарушениях (далее – КоАП) [2]. Однако граждане продолжают «узнавать о своих кредитах» только после возбуждения в отношении них исполнительных производств. На наш взгляд, ключевая проблема в данном случае заключается в ненадлежащей идентификации заемщика микрофинансовыми организациями (далее - МФО) и банками при дистанционном заключении договоров.

Согласно Федеральному закону «О персональных данных» от 27.07.2006 № 152-ФЗ обработка ПДн допускается только с согласия субъекта (ст. 6, 9) [3] и при дистанционном заключении договора простая электронная подпись (СМС-код) не доказывает волю заемщика – она лишь подтверждает доступ к телефону. Таким образом, сделка, совершенная мошенниками указанным способом, ничтожна в соответствии с п. 2 ст. 168 Гражданского кодекса Российской Федерации (далее - ГК РФ) [4]. Анализ судебных решений, приведенных в таблице 1, доказывает это.

Так, в Ивановской области (Дело № 1) согласно фабуле дела мошенники через вредоносное программное обеспечение (далее - ПО) получили доступ к телефону истца, извлекли оттуда паспортные данные и использовали его номер для получения СМС-кода [9], затем оформили покупку с рассрочкой на 224 тыс. руб. в АО «Плайт». Суд признал договор незаключенным, так как ответчик не проверил принадлежность номера телефона истцу. ПДн обрабатывались без согласия, а это нарушение статьи 6, 9 федерального закона № 152-ФЗ [3].

Аналогичный случай произошел в г. Санкт-Петербург (Дело № 2) [10]. Там мошенники использовали паспортные данные истца, номер телефона и банковскую карту, которые ему не принадлежали, и оформили микрозаем на 5 820 руб. в ООО МКК «Твои Плюс». Суд признал договор недействительным, потому что МФО не проверила принадлежность телефона и карты.

Подобная махинация имела место быть и в Республике Башкортостан (Дело № 3) [5]. Мошенники использовали паспортные данные истца из похищенной базы данных и полученный из сети Интернет телефон, также как и в предыдущем случае оформили

микрозаем на 6 350 руб. в ООО МКК «Финлаб». Суд признал договор недействительным, обязал исключить запись из кредитной истории, взыскал компенсацию морального вреда (5 000 руб.) и штраф (2 500 руб.), сославшись на отсутствие согласия на обработку ПДн [3].

В Республике Татарстан (Дело № 4) мошенники, используя паспортные данные истца и чужой номер телефона [6], оформили кредит на 286 600 руб. в АО «Альфа-Банк». Суд признал договор незаключенным и отменил нотариальную надпись, так как банк не проверил принадлежность телефона.

В Самарской области (Дело № 5) мошенники использовали паспортные данные истца и номер телефона, который перестал принадлежать ему три года назад, и оформили микрозаем на 8 200 руб. в ООО МКК «Срочноденьги» [7]. Суд признал договор незаключенным: МФО не проверила актуальность номера.

Таблица 1

Анализ судебных решений

№	Действия злоумышленника	Источник получения ПДн	Полученные ПДн	Нарушения МФО/банка	Решение суда
1	Взлом телефона, рассрочка 224 тыс. руб.	Вредоносное ПО на телефоне жертвы	Паспорт, номер телефона	Принадлежность телефона жертве (телефон ее, но оформлял не она)	Незаключенный договор
2	Микрозаем 5 820 руб.	Утечка базы данных	Паспорт, номер телефона и карты	Принадлежность телефона и карты жертве (они были чужие)	Недействительный договор
3	Микрозаем 6 350 руб.	Утечка базы данных	Паспорт, номер телефона	Личность заемщика (что заявку подает именно владелец паспорта)	Недействительный договор, компенсация 5 000 руб., штраф 2 500 руб
4	Кредит 286 600 руб.	Утечка базы данных	Паспорт, не актуальный номер телефона	Принадлежность телефона жертве (номер был чужой)	Незаключенный договор, отмена нотариальной надписи
5	Микрозаем 8 200 руб.	Утечка базы данных	Паспорт жертвы, номер, ранее принадлежавший жертве	Актуальность телефона (номер уже не принадлежит жертве)	Незаключенный договор

Таким образом, в четырех делах из пяти мошенники использовали паспортные данные жертвы, указывая свой номер телефона (в деле №2 – также свою банковскую карту). МФО и банки не проверяли принадлежность этих реквизитов, ограничиваясь совпадением паспортных данных. В деле №1 данные были получены через вредоносное ПО на телефоне жертвы. Наиболее распространенными нарушениями МФО/банками является отсутствие проверки принадлежности номера телефона (дела №1, №2, №4, №5). В деле №3 МФО не осуществила еще и идентификацию личности заемщика. Компенсация морального вреда взыскана только в деле №3, поскольку истица представила медицинские документы. Во всех случаях с МФО/банка были взысканы штрафы за отказ добровольно удовлетворить требования потребителя. Также во всех делах суд встал на сторону граждан: договоры признаны незаключенными (№1, №4, №5) или недействительными (№2, №3). В деле №4 дополнительно была отменена нотариально заверенная исполнительная надпись.

В итоге, с 1 марта 2025 года был введен механизм запрета на заключение договоров потребительского займа (кредита) (Федеральный закон от 26.02.2024 № 31-ФЗ) [8]. Гражданин может установить запрет через многофункциональный центр (далее – МФЦ) или единый портал государственных услуг (далее – ЕПГУ), после чего кредитор обязан проверить его наличие и отказать в выдаче кредита. Во всех пяти делах, если бы истцы заранее установили запрет, мошеннические сделки не состоялись бы, поскольку кредиторы обязаны проверять его наличие.

На основании проведенного анализа можно сформулировать следующие рекомендации для граждан: установить запрет на кредиты через МФЦ или ЕПГУ, проверять кредитную историю, а при обнаружении «чужого» кредита обращаться в полицию или в суд. Для законодателя: дополнить часть 18 статьи 5 Федерального закона от 21 декабря 2013 года № 353-ФЗ «О потребительском кредите (займе)» требованиями об обязательной проверке принадлежности номера телефона заемщику через оператора связи и об идентификации заемщика с использованием страхового номера индивидуального лицевого счета или идентификационного номера налогоплательщика в дополнение к паспортным данным; дополнить статью 8 Федерального закона от 30 декабря 2004 года № 218-ФЗ «О кредитных историях» упрощенным порядком аннулирования кредитной записи при возбуждении уголовного дела о мошенничестве (статьи 159, 159.3, 159.6, 272.1 УК РФ [1]); а также увеличить размер штрафов по статье 13.11 КоАП [2] за незаконную обработку ПДн.

Список использованных источников:

1. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ. URL: https://base.garant.ru/10108000/ (дата обращения: 07.04.2026).
2. Кодекс РФ об административных правонарушениях от 30.12.2001 № 195-ФЗ. URL: https://base.garant.ru/12125267/ (дата обращения: 07.04.2026).
3. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных». URL: https://base.garant.ru/12148567/ (дата обращения: 07.04.2026).
4. Гражданский кодекс Российской Федерации (часть первая) от 30.11.1994 № 51-ФЗ. URL: https://base.garant.ru/10164072/ (дата обращения: 07.04.2026).
5. Решение Бирского межрайонного суда Республики Башкортостан от 28.10.2025 по делу № 2-1288/2025. URL: https://sudact.ru/regular/doc/b7CAncKoC1rI/ (дата обращения: 07.04.2026).
6. Решение Апастовского районного суда Республики Татарстан от 24.10.2025 по делу № 2-399/2025. URL: https://sudact.ru/regular/doc/HSkRbNlNP6Ud/ (дата обращения: 07.04.2026).
7. Решение Автозаводского районного суда г. Тольятти Самарской области от 29.09.2025 по делу № 2-9416/2025. URL: https://sudact.ru/regular/doc/If7Xw6TU1RUJ/ (дата обращения: 07.04.2026).
8. Федеральный закон от 26.02.2024 № 31-ФЗ «О внесении изменений в Федеральный закон «О потребительском кредите (займе)». URL: https://base.garant.ru/408603209/ (дата обращения: 07.04.2026).

Gavrilova A.A.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Yapparov R.M.
Ufa University of Science and Technology, Ufa

ON THE ISSUE OF IMPROVING PERSONAL DATA PROTECTION MECHANISMS

Abstract. The article analyzes five 2025 court rulings on loan agreements made without consent using stolen personal data. It examines data sources, identification bypass methods, legal positions, and loan self-prohibition, and proposes measures to protect the rights of personal data processing subjects.

Keywords: personal data, illegal processing, loan agreement, judicial practice, Federal Law No. 152-FZ.

УДК 004.056

Еремина Л.А.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Яппаров Р.М.
Уфимский университет науки и технологий, Уфа

СОВЕРШЕНСТВОВАНИЕ НОРМАТИВНО-ПРАВОВОГО РЕГУЛИРОВАНИЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СЕТИ ИНТЕРНЕТ

Аннотация. В данной статье проведен анализ нормативно-правового регулирования защиты информации в сети Интернет в РФ. Рассмотрены ключевые федеральные законы (№ 149-ФЗ, № 187-ФЗ, № 152-ФЗ, № 126-ФЗ) и выявлены проблемы правоприменения в условиях развития современных технологий, включая искусственный интеллект, машинное обучение. Обоснована необходимость совершенствования отечественного законодательства для повышения эффективности обеспечения информационной безопасности в сети Интернет.

Ключевые слова: информационная безопасность, нормативно-правовая база, Интернет, ФСТЭК России, ФСБ России, КИИ, персональные данные, киберпреступность, искусственный интеллект.

Цифровизация превратила Интернет в критически важную среду для государства и экономики. При этом общее количество преступлений, совершенных с использованием информационно-телекоммуникационных технологий, остается по-прежнему высоким. Так, по данным Центробанка РФ (далее – ЦБ РФ) российские банки в 2025 году только с помощью антифрод-систем предотвратили 134,2 млн. мошеннических операций, что почти вдвое больше, чем в 2024 году. При этом размер похищенных злоумышленниками средств вырос на 6,4%, до 29,3 млрд. рублей [1]. Продолжаются и фиксируются инциденты с компьютерными атаками на финансовую сферу, включая DDoS-атаки и использование вирусов-шифровальщиков. Рост киберпреступлений актуализирует вопросы совершенствования законодательства, поскольку эффективность расследования зависит от четкости разграничения полномочий и правового статуса информации.

Нормативно-правовая база РФ представляет собой иерархическую систему:

- Конституция РФ;
- федеральные законы;

- указы Президента, постановления Правительства РФ;
- ведомственные акты (ФСТЭК, ФСБ, Минцифры).

Если проанализировать содержание основных федеральных законов в Российской Федерации, то мы видим, что:

1. Федеральный закон от 27.07.2006 № 149-ФЗ устанавливает принципы регулирования, понятийный аппарат, требования к защите информации и порядок ограничения доступа (включая Единый реестр запрещенной информации). Практическая реализация осложняется проблемами идентификации владельцев ресурсов с зарубежными серверами.

2. Федеральный закон от 27.07.2006 № 152-ФЗ регулирует обработку персональных данных: принцип локализации (ч. 5 ст. 18), требование согласия, категории данных, полномочия Роскомнадзора. Рост утечек персональных данных подтверждает необходимость усиления контроля.

3. Федеральный закон от 26.07.2017 № 187-ФЗ вводит понятие критической информационной инфраструктуры и значимых объектов, устанавливает категорирование, обязанности субъектов критической информационной инфраструктуры, полномочия ФСТЭК. Нарушения квалифицируются по ст. 13.12–13.13 КоАП РФ или ст. 274.1 УК РФ.

4. Федеральный закон от 07.07.2003 № 126-ФЗ обязывает операторов связи соблюдать тайну переписки и сообщений [2].

Детализация положений законов закреплена в подзаконных актах соответствующих регуляторов: ФСТЭК России (защита КИИ и ПДн, приказы № 239, 31, 21), ФСБ России (криптографическая защита) и Роскомнадзора (контроль связи и ведение реестров).

Несмотря на созданную систему нормативно-правового регулирования обеспечения информационной безопасности в настоящее время не урегулированными в сети Интернет остаются вопросы связанные с:

1. Технологическим отставанием: нормы УК РФ (ст. 159.6, 272–274) не позволяют квалифицировать новые виды преступлений (дипфейки, криптовалюты, децентрализованные сети и др.).

2. Трансграничностью преступлений: отсутствие эффективных механизмов международного сотрудничества создает «юридические лакуны» при расследовании преступлений с участием иностранных юрисдикций.

3. Слабой доказательственной базой: ошибки при изъятии цифровых носителей могут привести к признанию доказательств недопустимыми (ст. 75 УПК РФ).

Кроме того, вызовы и риски связанные с искусственным интеллектом (далее – ИИ) тоже необходимо учитывать. Технологии ИИ

создают двойственные риски: используются злоумышленниками (дипфейки, автофишинг), но могут быть и инструментом расследования (анализ аномалий). Несмотря на принятую Национальную стратегию развития ИИ до 2030 года и внесенные в нее изменения и дополнения [3], на уровне федеральных законов отсутствует регулирование:

- правового статуса доказательств, полученных с помощью ИИ;
- ответственности за создание дипфейков и использование ИИ в кибератаках;
- оборота данных, используемых для обучения нейросетей.

Подзаконные нормативные правовые акты (требования ФСТЭК к системам с ИИ, регулирование постквантовой криптографии ФСБ) носят технический характер и не решают фундаментальных правовых проблем.

Таким образом, в Российской Федерации сформирована системная нормативно-правовая база защиты информации (законы № 149-ФЗ, № 152-ФЗ, № 187-ФЗ, № 126-ФЗ и др.), однако не определены приоритетные направления совершенствования:

- актуализация законодательства с учетом ИИ и новых технологий;
- унификация подходов к сбору цифровых доказательств;
- развитие международного сотрудничества;
- введение ответственности за использование ИИ в преступных целях;
- регулирование оборота данных для обучения нейросетей.

На наш взгляд, только комплексный подход, сочетающий правовые нормы и технические средства, обеспечит устойчивость информационного пространства РФ.

Для реализации указанных приоритетных направлений мы предлагаем внести следующие изменения в нормативные правовые акты:

1. В области ответственности за использование ИИ в преступных целях:

- дополнить УК РФ статьей 273.1 «Неправомерное использование технологий искусственного интеллекта» (установив ответственность за создание дипфейков без согласия лица и использование ИИ для совершения кибератак).
- внести изменение в ст. 272 УК РФ (неправомерный доступ к компьютерной информации), добавив квалифицирующий признак «… с использованием технологий искусственного интеллекта».

2. В области регулирования оборота данных для обучения нейросетей:

- дополнить Федеральный закон № 149-ФЗ статьей 15.6 «Оборот данных для обучения систем искусственного интеллекта» (установив требования к маркировке датасетов и запрет на использование данных, полученных с нарушением законодательства о персональных данных).

– внести изменение в ст. 6 Федерального закона № 152-ФЗ, дополнив ее пунктом 11, допускающим обработку персональных данных для обучения ИИ только при условии их обезличивания и получения отдельного согласия субъекта.

3. В области правового статуса доказательств, полученных с помощью ИИ:

– дополнить ст. 74 УПК РФ пунктом 7, включив «результаты обработки данных с использованием систем искусственного интеллекта» в перечень допустимых доказательств.

– дополнить ст. 75 УПК РФ примечанием, устанавливающим критерии допустимости таких доказательств (сертификация программного обеспечения, воспроизводимость результата).

– внести изменения в приказ ФСТЭК России № 21 «Об утверждении требований к защите персональных данных», добавив раздел о требованиях к системам ИИ, используемым в оперативно-розыскной деятельности.

4. В области усиления контроля за утечкой персональных данных:

– дополнить ст. 18.1 Федерального закона № 152-ФЗ требованием об обязательном внедрении операторами персональных данных систем обнаружения утечек информации, сертифицированных ФСТЭК России.

– дополнить ст. 13.11 КоАП РФ соответствующими положениями, увеличив размер административного штрафа за утечку персональных данных для юридических лиц до 15 миллионов рублей.

Список использованных источников:

1. Информационная безопасность // Официальный сайт ЦБ РФ. – URL: https://cbr.ru/information_security/ (дата обращения: 12.04.2026).

2. Письмо ФНС России от 27.04.2022 № СД-4-2/5153@ «О запрете истребования сведений, относящихся к тайне связи» // Доступ из СПС «КонсультантПлюс» (дата обращения: 12.04.2026).

3. Указ Президента РФ от 15.02.2024 N 124 "О внесении изменений в Указ Президента Российской Федерации от 10 октября 2019 г. N 490 "О развитии искусственного интеллекта в Российской Федерации" и в Национальную стратегию, утвержденную этим Указом" // КонтурНорматив. – URL: https://normativ.kontur.ru/document?moduleId=1&documentId=465635 (дата обращения: 12.04.2026).

Eremina L.A.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Yapparov R.M.
Ufa University of Science and Technology, Ufa

IMPROVING THE LEGAL AND REGULATORY FRAMEWORK FOR ENSURING INFORMATION SECURITY ON THE INTERNET

Abstract. This article analyzes the legal and regulatory framework for information protection on the Internet in the Russian Federation. Key federal laws (No. 149-FZ, No. 187-FZ, No. 152-FZ, No. 126-FZ) are examined, and problems of law enforcement in the context of technological development, including artificial intelligence, are identified. The necessity of improving domestic legislation to enhance the effectiveness of ensuring information security on the Internet is substantiated.

Keywords: information security, legal and regulatory framework, Internet, FSTEC of Russia, FSB of Russia, critical information infrastructure, personal data, cybercrime, artificial intelligence.

УДК 004.056

Журавлева Ю.О., Шамсутдинова А.А.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Байрушин Ф.Т
Уфимский университет науки и технологий, Уфа

РОЛЬ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОБЕСПЕЧЕНИИ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Аннотация. В статье рассматривается роль информационной безопасности в обеспечении национальной безопасности Российской Федерации. Отмечаются основные направления государственной политики в данной сфере, анализируются современные вызовы и угрозы, а также предлагаются пути совершенствования системы защиты информационного суверенитета страны.

Ключевые слова: информационная безопасность, национальная безопасность, киберугрозы, цифровой суверенитет, критическая информационная инфраструктура.

В Концепции информационной безопасности Российской Федерации, принятой в 2016 году, отмечается, что информационная безопасность играет ключевую роль в обеспечении национальной безопасности. Противодействие манипуляциям общественным сознанием, защита критической информационной инфраструктуры и обеспечение технологической независимости стали приоритетными задачами государства в условиях цифровой трансформации и роста геополитической напряженности [1].

Современное российское государство сталкивается со значительным уровнем внешней агрессии в информационном пространстве. Количество киберугроз за последние годы выросло в разы.

Особую тревогу вызывает рост атак на объекты критической информационной инфраструктуры (КИИ). По данным Совета Безопасности Российской Федерации, количество преступлений в отношении объектов КИИ увеличилось почти в четыре раза. На эти объекты пришлось около 64% от общего числа инцидентов за 2024 год. Стратегические отрасли, включая госсектор и промышленность, стали главными целями злоумышленников, при этом 72% всех успешных кибератак, зафиксированных в СНГ, пришлось на Россию [2].

При этом по некоторым оценкам, лишь 20% субъектов КИИ выполнили все установленные требования по защите своей информационной инфраструктуры [2], что создает серьезные риски для национальной безопасности.

В Российской Федерации применяются системные меры по укреплению информационной безопасности. С 1 января 2025 года органам государственной власти, госкомпаниям и стратегическим предприятиям запрещено использовать средства защиты информации из недружественных стран, а также пользоваться их сервисами по обеспечению информационной безопасности [3]. Эта мера направлена на достижение технологического суверенитета, который является основой экономической и политической независимости страны.

В 2025 году была сформирована и начала реализацию новая национальная программа «Экономика данных и цифровая трансформация государства», пришедшая на смену программе «Цифровая экономика». Расходы на кибербезопасность по итогам 2024 года выросли на 23%, достигнув 299 миллиардов рублей [4], что вывело Россию в топ-10 стран по этому показателю.

Важным шагом стала работа над новой редакцией Доктрины информационной безопасности Российской Федерации [5], которая призвана учесть современные вызовы и угрозы в цифровой сфере, а также изменения в международной обстановке и развитии технологий.

Обновленная версия должна определить стратегические направления защиты национальных интересов России.

Анализ текущей ситуации показывает ряд направлений, требующих развития. Для достижения целей обеспечения информационной безопасности РФ необходимо усилить контроль за защитой объектов КИИ и стимулировать их своевременное категорирование; продолжить развитие отечественных технологических решений и ускорить импортозамещение; решить проблему дефицита кадров через развитие профильного образования; внедрить механизмы стимулирования бизнеса (например, налоговые льготы) для использования надежных средств киберзащиты.

Информационная безопасность является неотъемлемой составляющей национальной безопасности Российской Федерации. В условиях нарастающей геополитической напряженности и беспрецедентного уровня киберугроз обеспечение защиты информационного пространства страны становится важнейшим стратегическим приоритетом. Только комплексный подход, объединяющий усилия государства, бизнеса и научного сообщества, позволит создать надежную систему противодействия современным вызовам и угрозам в информационной сфере, обеспечив тем самым суверенитет и безопасность России в цифровую эпоху.

Список использованных источников:

1. Указ Президента Российской Федерации от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // Официальный сайт Кремля. – URL: http://www.kremlin.ru/acts/bank/41460 [Электронный ресурс] (дата обращения 15.04.2026).

2. На критическую инфраструктуру России было совершено 208 тыс. кибератак // Anti-Malware.ru, 19.06.2025. – URL: https://www.anti-malware.ru/news/2025-06-19-121598/46387 [Электронный ресурс] (дата обращения 15.04.2026).

3. Указ Президента Российской Федерации от 13.06.2024 № 500 «О внесении изменений в Указ Президента Российской Федерации от 1 мая 2022 г. № 250» // Официальный сайт Кремля. [Электронный ресурс] (дата обращения 15.04.2026).

4. Расходы на кибербезопасность в России по итогам 2024 г. выросли до 299 млрд рублей // Компьютерра, 09.06.2025. – URL: https://www.computerra.ru/316195/ [Электронный ресурс] (дата обращения 15.04.2026).

5. Совбез начал готовить новую Доктрину информбезопасности Российской Федерации // KP.RU, 09.09.2025. – URL: https://www.kp.ru/online/news/6561650/ [Электронный ресурс] (дата обращения 15.04.2026).

Zhuravleva Yu.O., Shamsutdinova A.A.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Bayrushin F.T
Ufa University of Science and Technology, Ufa

THE ROLE OF INFORMATION SECURITY IN ENSURING THE NATIONAL SECURITY OF THE RUSSIAN FEDERATION

Abstract. The article discusses the role of information security in ensuring the national security of the Russian Federation. The main directions of state policy in this area are noted, modern challenges and threats are analyzed, and ways of improving the system of protection of the country's information sovereignty are proposed.

Keywords: information security, national security, cyber threats, digital sovereignty, critical information infrastructure.

УДК 004.056.53

Зайнуллин Б.З.
Казанский национальный исследовательский технический университет им. А.Н. Туполева-КАИ, Казань

Научный руководитель:
Медведева С.Н.
Казанский национальный исследовательский технический университет им. А.Н. Туполева-КАИ, г. Казань

АВТОМАТИЗИРОВАННАЯ СИСТЕМА ОЦЕНКИ КРИТИЧНОСТИ УЯЗВИМОСТЕЙ В СООТВЕТСТВИИ С МЕТОДИКОЙ ФСТЭК РОССИИ ОТ 30 ИЮНЯ 2025 ГОДА

Аннотация. Рассмотрена методика оценки уровня критичности уязвимостей, утвержденная Федеральной службой по техническому и экспортному контролю (далее – ФСТЭК) России 30 июня 2025 г. Проанализированы публикации 2020–2026 гг. по Common Vulnerability Scoring System (далее – CVSS) и системам Vulnerability Management. Сформулированы функциональные, нефункциональные к автоматизированной системе, реализующей расчет показателя V (значение оценки уровня критичности уязвимости). Показано, что отечественные VM-решения пока не поддерживают новую формулу в полном объеме.

Ключевые слова: ФСТЭК, уязвимости, CVSS, Vulnerability Management, критичность, автоматизация, информационная безопасность.

30 июня 2025 г. ФСТЭК России утвердила методический документ «Методика оценки уровня критичности уязвимостей программных, программно-аппаратных средств», заменивший документ от 28 октября 2022 г. [1]. Новая методика вводит формулу:

$$V = Icvss \times Iinfr \times (Iat + Iimp)$$

и четыре уровня критичности: низкий ($V < 2{,}0$), средний ($2{,}0 \le V < 5{,}0$), высокий ($5{,}0 \le V \le 8{,}0$), критический ($V > 8{,}0$) [1].

Документ обязателен к применению операторами ГИС и значимых объектов КИИ в силу приказа ФСТЭК России от 11 апреля 2025 г. № 117 [1]. По оценке Anti-Malware.ru, к апрелю 2025 г. лишь часть отечественных VM-платформ перестроили алгоритмы приоритезации под требования регулятора [9]. Опрос пользователей VM-систем 2025 г. показал: 62% специалистов считают соответствие методикам ФСТЭК ключевым критерием выбора продукта [2].

Цель работы – обосновать архитектурные и функциональные требования к автоматизированной системе, реализующей новую методику. Обратимся к данным существующих публикаций и нормативной базе, чтобы зафиксировать исходные ограничения.

Анализ современных публикаций

Сравнительный обзор сканеров RedCheck и MaxPatrol 8, выполненный С.А.Макиенко, Д.С.Преподобным и А.Е.Козловым (ТюмГУ, 2023), показал разброс покрытия идентификаторов БДУ от 71% до 94% [8]. В работе С.Б.Вепрева, С.А.Нестеровича и А.В.Макарова (Вестник РГГУ, 2025) доказано, что ручной анализ уязвимостей ОС без учета инфраструктурных коэффициентов занижает приоритет до 28% уязвимостей периметра [4]. Ю.В.Косолапов (МАИС, 2020) обосновал автоматизированный пересчет критичности при появлении новых сведений в БДУ [6].

И.В.Котенко, И.Б.Саенко, О.С.Лаута и соавторы (2024) предложили методику оценки устойчивости программно-конфигурируемых сетей при атаках, применимую к расчету показателя Iinfr [7]. А.А.Балябин и С.А.Петренко (2025) описали модель облачной платформы КИИ с кибериммунитетом, где предусмотрен автоматический пересчет критичности [5]. Л.А.Грищенко и В.А.Левицкая (БЦТ, 2025) разобрали процесс управления уязвимостями в финансовом секторе – среднее время устранения критической уязвимости 19 дней против 24 ч норматива [3]. И.В.Никрошкин и А.В.Савенкова (БЦТ, 2025) указали на расхождение между CVSS-оценкой и реальной актуальностью угрозы в 34 % случаев [2]. По данным отчета «Солар» (2024), внешние атаки на российские

компании выросли на 64 % [10]. Проведенный анализ показал: существующие решения частично закрывают задачу, но расчет V и контроль сроков устранения остаются «белыми пятнами».

Основная часть

Формула ФСТЭК агрегирует четыре показателя. Icvss берется из БДУ (bdu.fstec.ru) либо рассчитывается по базовым метрикам CVSS 3.1 [1]. Iinfr = k·K + l·L + p·P учитывает тип уязвимого компонента (K ∈ [0,1; 1,1]), долю уязвимых компонентов (L ∈ [0,5; 1,0]) и доступность из сети «Интернет» (P ∈ {0,6; 1,1}) [1]. Iat = e·E отражает эксплуатацию в реальных атаках (E = 0,6) либо наличие эксплойта (E = 0,3) [1]. Iimp = h·H привязан к последствиям: выполнение произвольного кода и повышение привилегий дают H = 0,5, XSS – H = 0,1 [1].

Рассмотрим пример из приложения к методике: для уязвимости BDU:2025-03219 (ingress-nginx, CVSS 9,8) при K = 0,55, L = 0,2, P = 0,33, Iat = 0,3, Iimp = 0,5 итоговое значение V ≈ 8,47 – критический уровень [1]. Ручной расчет для большого количества уязвимостей практически невозможен; по данным опроса 2025 г., 74 % специалистов тратят на приоритезацию более 8 часов в неделю [2]. Автоматизация снимает этот барьер.

Предлагаемая архитектура включает 6 модулей. Первый – импорт и парсинг отчетов из сканеров уязвимостей. Второй – автоматическое обогащение уязвимостей метриками и информацией из баз данных уязвимостей. Третий – ручное обогащение. Четвертый – расчет критичности уязвимостей. Пятый – управление уязвимостями и принятие решения. Шестой – импорт результатов повторного анализа и выдача итогового заключения по результатам анализа защищенности.

Требования, предъявляемые к системе

Функциональные требования: поддержка импорта отчетов различных сертифицированных сканеров уязвимостей с возможностью добавления новых; расчет V с точностью до сотых; хранение истории значений V для ретроспективного анализа [3]; формирование отчетов.

Нефункциональные требования: обработка до 10 000 уязвимостей в рамках одного проекта с приемлемым временем отклика (ориентир – не более 5 секунд на массовые операции); разграничение доступа по ролям согласно ГОСТ Р 56545-2015 [1]. Система должна поддерживать сертифицированные ОС (Astra Linux SE, РЕД ОС) и СУБД PostgreSQL Pro [10].

Заключение

Проведенный анализ показал, что методика ФСТЭК от 30 июня 2025 г. вводит более строгую многофакторную модель оценки критичности по сравнению с документом 2022 года [1]. Рынок VM-систем отстает от нормативных изменений: по состоянию на начало 2026 г. полная

поддержка формулы V реализована менее чем в половине продуктов [9]. Разработка автоматизированной системы является обоснованной и практически значимой задачей.

Список использованных источников:

1. Методика оценки уровня критичности уязвимостей программных, программно-аппаратных средств: методический документ / ФСТЭК России. Утв. 30.06.2025. URL: https://pravo.ppt.ru/metodika/316218 (дата обращения: 19.04.2026).

2. Никрошкин И.В., Савенкова А.В. Проблемы оценки актуальности угроз безопасности информации // Безопасность цифровых технологий. 2025. № 2 (117). С. 9–24. ISSN 2782-2230. DOI: 10.17212/2782-2230-2025-2-9-24.

3. Грищенко Л.А., Левицкая В.А. Организация процесса управления уязвимостями предприятий финансового сектора // Безопасность цифровых технологий. 2025. № 2 (117). С. 76–102. ISSN 2782-2230. DOI: 10.17212/2782-2230-2025-2-76-102.

4. Вепрев С.Б., Нестерович С.А., Макаров А.В. Анализ уязвимостей в операционных системах и прикладных программных продуктах // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2025. № 1. С. 95–105. ISSN 2686-679X. DOI: 10.28995/2686-679X-2025-1-95-105.

5. Балябин А.А., Петренко С.А. Модель облачной платформы критической информационной инфраструктуры с кибериммунитетом // Информатика и автоматизация. 2025. Т. 24, № 5. С. 1471–1505. DOI: 10.15622/ia.24.5.8.

6. Косолапов Ю.В. Об обнаружении эксплуатации уязвимостей, приводящей к запуску вредоносного кода // Моделирование и анализ информационных систем. 2020. Т. 27, № 2. С. 138–151. ISSN 1818-1015. DOI: 10.18255/1818-1015-2020-2-138-151.

7. Котенко И.В., Саенко И.Б., Лаута О.С., Скоробогатов С.Ю., Кочин В.П. Методика оценки устойчивости программно-конфигурируемых сетей в условиях компьютерных атак // Журнал Белорусского государственного университета. Математика. Информатика. 2024. № 3. С. 90–102.

8. Макиенко С.А., Преподобный Д.С., Козлов А.Е. Сравнительный анализ сканеров уязвимостей RedCheck и MaxPatrol 8 // Математическое и информационное моделирование: материалы Всерос. конф. молодых ученых. Тюмень: ТюмГУ-Press, 2023. Вып. 21. С. 281–285. ISBN 978-5-400-01722-3.

9. Как эффективно выстроить процесс управления уязвимостями: аналитический обзор AM Live // Anti-Malware.ru. 2025. 15 апреля. URL:

https://www.anti-malware.ru/analytics/Technology_Analysis/Vulnerability-Management-AM-Live-2025 (дата обращения: 19.04.2026).

10. Ключевые внешние цифровые угрозы для российских компаний: аналитический отчет ГК «Солар». М., 2024. URL: https://rt-solar.ru/analytics/reports/6452/ (дата обращения: 19.04.2026).

Zaynullin B.Z.
Kazan National Research Technical University
named after A.N. Tupolev–KAI, Kazan

Scientific supervisor:
Medvedeva S.N.
Kazan National Research Technical University
named after A.N. Tupolev–KAI, Kazan

AUTOMATED SYSTEM FOR VULNERABILITY CRITICALITY ASSESSMENT ACCORDING TO THE FSTEC RUSSIA METHODOLOGY OF JUNE 30, 2025

Abstract. The methodology for assessing the vulnerability severity level, approved by the Federal Service for Technical and Export Control (FSTEC) of Russia on June 30, 2025, is considered. Publications from 2020 to 2026 on the Common Vulnerability Scoring System (CVSS) and Vulnerability Management systems are analyzed. Functional and non-functional requirements for an automated system that implements the calculation of the V metric (vulnerability severity level value) are formulated. It is shown that domestic VM solutions do not yet fully support the new formula.

Keywords: FSTEC, vulnerabilities, CVSS, Vulnerability Management, severity, automation, information security.

УДК 003

Ижболдина Т.К.
Уфимский университет науки и технологий, Уфа

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

ОРГАНИЗАЦИОННО-ПРАВОВЫЕ АСПЕКТЫ ЗАЩИТЫ ИНФОРМАЦИИ ГИС ОТДЕЛА ЗАГС РЕСПУБЛИКИ БАШКОРТОСТАН ПО ДЕЛАМ ЮСТИЦИИ

Аннотация. В статье рассматриваются организационно-правовые проблемы защиты информации в государственной информационной системе органов ЗАГС на примере Республики Башкортостан. Анализируется нормативная база, включая требования ФСТЭК и ФСБ России, выявляются основные угрозы персональным данным. Предлагаются меры по совершенствованию системы защиты с учетом региональной специфики и динамики законодательства.

Ключевые слова: защита информации, ГИС ЗАГС, персональные данные, Республика Башкортостан, ФСТЭК, ФСБ.

В условиях цифровой трансформации государственного управления эффективное функционирование государства невозможно без надежных государственных информационных систем (ГИС). Особое место среди них занимают системы органов записи актов гражданского состояния (ЗАГС), поскольку они обрабатывают данные, определяющие правовой статус личности на протяжении всей жизни: рождение, брак, установление отцовства, усыновление, перемена имени, смерть. Эти сведения являются фундаментом для реализации конституционных прав граждан – от получения паспорта до оформления пенсии и наследства. В связи с этим обеспечение сохранности, целостности и конфиденциальности информации в системах ЗАГС является задачей первостепенной государственной важности.

Республика Башкортостан, как один из крупнейших и наиболее развитых регионов РФ (население свыше 4 млн человек), сталкивается с повышенными рисками в сфере защиты информации. Через отделы ЗАГС республики ежегодно проходят сотни тысяч обращений, масштаб обрабатываемых персональных данных огромен. Структурно отделы подчиняются Госкомитету РБ по делам юстиции, который обеспечивает общее руководство, однако единообразие мер защиты информации на всех объектах (районные и городские подразделения) не всегда

достижимо из-за территориальной распределенности и различий в технической оснащенности.

В соответствии с Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», государственная информационная система – это совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств. ГИС отдела ЗАГС относится к региональному уровню, так как вопросы регистрации актов гражданского состояния находятся в совместном ведении РФ и субъектов. С введением в эксплуатацию ФГИС «ЕГР ЗАГС» произошло объединение всех записей актов, составленных на территории России с 1926 года. Эта система взаимодействует с МВД, Судебным департаментом, ФНС России через систему межведомственного электронного взаимодействия (СМЭВ). Правовую основу функционирования ГИС ЗАГС составляют: Федеральный закон от 15.11.1997 № 143-ФЗ «Об актах гражданского состояния», Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных», Постановление Правительства РФ от 06.07.2015 № 676 «О требованиях к порядку создания, развития, ввода в эксплуатацию… государственных информационных систем». А также согласно Приказу № 117, требования к защите информации предъявляются в зависимости от класса защищенности информационной системы, который определяется на основе уровня значимости информации и масштаба системы. В органах ЗАГС обрабатываются персональные данные специальных категорий: фамилия, имя, дата и место рождения, гражданство, сведения о родителях, супруге(е), детях, усыновлении, перемене имени, смерти. Особенностью работы ЗАГС является юридическая значимость каждой записи: исправление или аннулирование данных возможно только по решению суда или органа ЗАГС. Это предъявляет повышенные требования к целостности информации и системе защиты информации (СрЗИ). При этом для подтверждения достаточности принятых мер до начала обработки информации должна быть проведена аттестация информационной системы на соответствие требованиям Приказа № 117.

Высокая востребованность персональных данных, обрабатываемых в органах ЗАГС, обусловливает повышенный интерес к ним со стороны злоумышленников. Типичные угрозы включают мошеннические схемы с использованием персональных данных (оформление кредитов на умерших или несуществующих лиц), подделку документов для получения наследства, несанкционированный доступ к базам данных со стороны инсайдеров, а также атаки на программное обеспечение с целью модификации актовых записей. Особую сложность представляет необходимость одновременного выполнения требований двух

регуляторов: ФСТЭК России (в части технической защиты информации, антивирусной защиты, контроля доступа, регистрации событий безопасности) и ФСБ России (в части использования криптографических средств защиты информации при передаче данных по каналам связи, в том числе при взаимодействии через СМЭВ).

Анализ текущего состояния системы защиты информации в ЗАГС ГК РБ выявляет следующие проблемные зоны: нерегулярное обновление моделей угроз в связи с динамикой нормативно-правовой базы; недостаточная автоматизация контроля за действиями пользователей с персональными данными; человеческий фактор – низкая осведомленность сотрудников о современных методах социальной инженерии. В связи с этим совершенствование системы защиты информации ГИС отдела ЗАГС должно носить комплексный характер, объединяя организационно-правовые и технические меры.

Организационно-правовые меры неразрывно связаны с техническими. Для ГИС отдела ЗАГС Республики Башкортостан приоритетными техническими направлениями являются: внедрение средств криптографической защиты информации (СКЗИ), сертифицированных ФСБ России, для всех каналов передачи данных; усиление мер идентификации и аутентификации – переход на двухфакторную аутентификацию для пользователей, имеющих право на внесение изменений в актовые записи; обеспечение целостности информации с использованием электронной подписи для каждой актовой записи; регистрация событий безопасности в соответствии с требованиями

Таким образом, проведенный анализ показал, что система защиты информации ГИС отдела ЗАГС Республики Башкортостан требует постоянного совершенствования в условиях динамичного изменения законодательства и роста внешних угроз. Основные направления развития включают актуализацию организационно-распорядительной документации в соответствии с требованиями ФСТЭК России и ФСБ России; регулярную аттестацию объектов информатизации и пересмотр модели угроз, обязательное обучение персонала и повышение его ответственности, внедрение сертифицированных российских средств защиты информации, включая криптографические. Только комплексное применение организационно-правовых и технических мер позволит обеспечить сохранность, целостность и конфиденциальность записей актов гражданского состояния – основы правового статуса миллионов граждан Республики Башкортостан и всей Российской Федерации.

Список использованных источников:

1. Федеральный закон от 27.07.2012 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [Электронный ресурс] // КонсультантПлюс: справочно-правовая система / Режим доступа: URL: http://base.www.consultant.ru/.

2. Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 24.06.2025) «О персональных данных» [Электронный ресурс] // КонсультантПлюс: справочно-правовая система / Режим доступа: URL: http://base.www.consultant.ru/.

3. Постановление Правительства РФ от 06.07.2015 № 676 «О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации» [Электронный ресурс] // КонсультантПлюс: справочно-правовая система / Режим доступа: URL: http://base.www.consultant.ru/.

4. Приказ ФСТЭК России от 11.04.2025 № 117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений» [Электронный ресурс]. URL: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/trebovaniya-utverzhdeny-prikazom-fstek-rossii-ot-11-aprelya-2025-g-n-117.

5. ГОСТ Р ИСО/МЭК 27001-2021. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. – М.: Стандартинформ, 2021.

6. Даниленко А.О. Правовое регулирование государственных информационных систем субъектов Российской Федерации и гарантии конституционных прав граждан // Журнал российского права. – 2025. – № 10. – С. 45–58.

7. Комаров А.А. Ответственность за нарушение требований в области обработки персональных данных в государственных информационных системах // Информационное право. – 2024. – № 3. – С. 22–28.

8. Цветкова И.А. Государственные информационные системы России: история, современное состояние и перспективы развития. – М.: Наука, 2021. – 248 с.

Izhboldina T.K.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Shagapov I.A.
Ufa University of Science and Technology, Ufa

ORGANIZATIONAL AND LEGAL ASPECTS OF INFORMATION PROTECTION IN THE REGISTRY OFFICE OF THE REPUBLIC OF BASHKORTOSTAN IN THE FIELD OF JUSTICE

Abstract. This article examines organizational and legal issues related to information security in the state registry office information system (SIS) in the Republic of Bashkortostan. The regulatory framework, including the requirements of the Federal Service for Technical and Export Control (FSTEC) and the Federal Security Service (FSB), is analyzed, and the main threats to personal data are identified. Measures are proposed to improve the security system, taking into account regional specifics and legislative developments.

Keywords: information security, SIS SIS, personal data, Republic of Bashkortostan, FSTEC, FSB.

УДК 004

Иркина Ю.Р.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Салов И.В.
Уфимский университет науки и технологий, Уфа

СИСТЕМЫ ОПОВЕЩЕНИЯ НАСЕЛЕНИЯ КАК ОБЪЕКТ ИНФОРМАЦИОННОЙ ЗАЩИТЫ

Аннотация. Статья рассматривает системы оповещения населения в контексте информационной безопасности как элемент государственной системы защиты от чрезвычайных ситуаций. На основе анализа ключевых нормативных актов рассматриваются нормативно-правовые основы их создания и функционирования, уровни и виды систем, а также требования к защите информации

Ключевые слова: системы оповещения населения, информационная безопасность, гражданская оборона, защита информации, ФСТЭК России, региональная система оповещения, локальная система оповещения, КСЭОН.

Системы оповещения населения занимают особое место в структуре единой государственной системы предупреждения и ликвидации чрезвычайных ситуаций (РСЧС) и гражданской обороны. Они обеспечивают оперативное доведение сигналов и экстренной информации до граждан в условиях угроз природного, техногенного или военного характера. Актуальность темы обусловлена ростом рисков различных угроз и необходимостью поддержания постоянной готовности этих систем к использованию, так как она прямо влияет на безопасность миллионов людей.

Правовую основу составляют Федеральный закон от 21.12.1994 № 68-ФЗ «О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера», Федеральный закон от 12.02.1998 № 28-ФЗ «О гражданской обороне», а также постановления Правительства РФ. Одним из главных актов является совместный приказ МЧС России и Министерства цифрового развития, связи и массовых коммуникаций РФ от 31.07.2020 № 578/365 «Об утверждении Положения о системах оповещения населения» (далее Приказ № 578/365). Этот документ определяет назначение, задачи, порядок задействования и поддержания готовности систем [1]. А методические рекомендации 2024 года дополнительно конкретизируют меры по поддержанию постоянной готовности, включая вопросы защиты информации [2].

Системы создаются на трех уровнях: региональном – региональная автоматизированная система централизованного оповещения муниципальном (муниципальная система) и объектовом (локальная система). Отдельным элементом выступает комплексная система экстренного оповещения населения (КСЭОН), действующая в автоматическом или автоматизированном режиме в зонах экстренного оповещения. Кроме того, используется общероссийская комплексная система информирования и оповещения населения в местах массового пребывания людей (ОКСИОН) [1].

Локальные системы создаются организациями, эксплуатирующими опасные объекты, 1 и 2 классов опасности, радиационно и ядерно опасные объекты, а также гидротехнические сооружения высокой опасности. Границы зон действия определяются административными границами субъектов и муниципалитетов или зонами воздействия поражающих факторов. Все эти системы представляют собой объект информационной безопасности, поскольку включают программно-технические средства, каналы связи и сети передачи данных единой сети электросвязи РФ [1].

Нарушение работы систем оповещения напрямую угрожает жизни и здоровью миллионов граждан, поскольку именно через них доводятся сигналы оповещения и экстренная информация об опасностях. В случае

сбоя или несанкционированного вмешательства население может не получить вовремя предупреждение о ЧС, что приведет к росту жертв и ущерба. Кроме того, такие системы обладают высоким потенциалом для дестабилизации общественного порядка: ложные или искаженные сигналы способны вызвать панику. Массовые беспорядки или парализовать работу органов управления. Локальные системы на опасных объектах тесно связаны с автоматизированными системами управления технологическими процессами (АСУ ТП), поэтом их защита приобретает особую значимость для предотвращения техногенных катастроф.

Приказ № 578/365 устанавливает, что системы оповещения включаются в систему управления гражданской обороной и РСЧС и состоят из взаимодействующих элементов: специальных программно-технических средств, КСЭОН, ОКСИОН, громкоговорящих средств и каналов связи. Документ подчеркивает необходимость защиты информации при ее обработке и передаче. Пункт 6 Приложения № 1 к Положению приказа связывает функционирование систем с общими требованиями к защите государственных информационных систем с общими требованиями к защите государственных информационных систем и АСУ ТП на критически важных объектах [1].

Региональные системы и КСЭОН относятся к государственным информационным системам (ГИС) и должны соответствовать Требованиям о защите информации, содержащейся в государственных информационных системах, утвержденным приказом ФСТЭК России от 11.04.2025 № 117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных государственных органов, государственных унитарных предприятий, государственных учреждений». Этот документ устанавливает класс защищенности не ниже второго для систем, обрабатывающих информацию ограниченного доступа. Оператор обязан определять цели защиты выявлять угрозы из банка данных ФСТЭК и применять программно-аппаратные средства защиты на всех стадиях жизненного цикла системы [3].

Локальные системы оповещения на опасных объектах попадают под действие приказа ФСТЭК России от 14.03.2014 № 31 [4]. Он регулирует защиту информации в автоматизированных системах управления производственными и технологическими процессами на критически важных потенциально опасных объектах. Требования данного приказа предусматривают многоуровневую структуру защиты (операторский, автоматический и полевой уровни), меры по предотвращению неправомерного доступа, уничтожения или модификации информации, а также согласование с мерами промышленной и физической безопасности.

Приказ № 578/365 в Приложении № 1 (пункты 1-10) конкретизирует функции защиты информации. Они включают:

- недопущение нарушения конфиденциальности, целостности и доступности данных;
- обеспечение непрерывности функционирования систем в условиях угроз;
- применение сертифицированных средств защиты;
- организацию контроля доступа;
- регулярное обновление политик безопасности;
- обучение персонала;
- мониторинг событий безопасности;
- резервное копирование и восстановление;
- документирование всех мероприятий.

Эти требования совпадают с приказом ФСТЭК № 117 и № 31. В результате достигается комплексная защита, исключающая негативные последствия от реализации угроз.

Системы оповещения населения являются не только техническим инструментом доведения информации, но и стратегическим объектом информационной безопасности, требующим строгого соблюдения нормативных требований ФСТЭК России. Комплексное применение приказов № 578/365 № 117 и № 31 позволяет обеспечить надежную защиту на всех уровнях и минимизировать риски для жизни и здоровья граждан.

Список использованных источников:

1. «Об утверждении Положения о системах оповещения населения» Приказ МЧС России и Министерства цифрового развития, связи и массовых коммуникаций РФ от 31 июля 2020г. № 78/365 «Об утверждении Положения о системах оповещения населения» [Электронный ресурс]. – URL: https://www.garant.ru/products/ipo/prime/doc/74723317/.

2. Методические рекомендации по поддержанию в состоянии постоянной готовности к использованию систем оповещения населения (утв. Протоколом заседания по предупреждению и ликвидации чрезвычайных ситуаций и обеспечению пожарной безопасности по координации создания и поддержания в постоянной готовности систем оповещения населения от 26 июня 2024г. № 2) [Электронный ресурс]. – URL: https://www.garant.ru/products/ipo/prime/doc/409441511/.

3. «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных государственных органов, государственных унитарных предприятий, государственных учреждений»: Приказ ФСТЭК России от

11.04.2025 № 117 [Электронный ресурс]. – URL: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/trebovaniya-utverzhdeny-prikazom-fstek-rossii-ot-11-aprelya-2025-g-n-117.

4. «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды»: Приказ ФСТЭК России от 14.03.2014 № 31 [Электронный ресурс]. – URL: https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-14-marta-2014-g-n-31?ysclid=mnobir1tpk174672526.

Irkina Y.R.
Ufa University of Science and Tecnology, Ufa

Scientific supervisor:
Salov I.V.
Ufa University of Science and Tecnology, Ufa

POPULATION WARNING SYSTEMS AS AN OBJECT OF INFORMATION PROTECTION

Abstract. The article examines population warning systems in the context of information security as an element of the state system of protection against emergencies. Based on the analysis of key regulatory acts, the legal and regulatory framework for their creation and operation, levels and types of systems, as well as requirements for information protection are considered.

Keywords: population warning systems, information security, civil defense, information protection, FSTEC of Russia, regional warning system, local warning system, CSED (Comprehensive System for Emergency Alerting of the Population)

УДК 004

Кунавина О.А.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Сенцова А.Ю.
Уфимский университет науки и технологий, Уфа

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ БИОМЕТРИЧЕСКИХ ПЕРСОНАЛЬНЫХ ДАННЫХ

Аннотация. В статье раскрыты особенности защиты персональных данных. Описаны вопросы обеспечения безопасности биометрических персональных данных, а также методы и средства их защиты. Особое внимание уделено практике функционирования Единой биометрической системы и выявленным в ее работе уязвимостям.

Ключевые слова: биометрические данные, персональные данные, информационная безопасность, Единая биометрическая система, защита информации.

Биометрические персональные данные занимают особое место в системе информационной безопасности. В отличие от паролей или PIN-кодов, которые можно изменить, отпечатки пальцев или рисунок радужной оболочки глаза остаются неизменными на протяжении всей жизни человека.

Российское законодательство определяет биометрические персональные данные как сведения, характеризующие физиологические и биологические особенности человека, на основании которых можно установить его личность [1]. Речь идет о дактилоскопических данных, изображении лица, голосе, радужной оболочке глаза, ДНК-профиле.

Постановление Правительства РФ №883 от 2023 года устанавливает обязательное шифрование данных при передаче и хранении, требует многофакторной аутентификации для доступа к базам, регламентирует процедуры аудита и мониторинга инцидентов.

Все биометрические шаблоны должны храниться в зашифрованном виде с использованием сертифицированных ФСБ России средств криптографической защиты информации (СКЗИ), а также быть зашифрованы с помощью отечественных стандартов шифрования. Требование применения отечественных СКЗИ закреплено для государственных информационных систем и критической информационной инфраструктуры [2].

Многофакторная аутентификация для доступа к биометрическим данным стала обязательной нормой для государственных систем. Администраторы и операторы должны использовать не только логин и пароль, но и дополнительные факторы – токены, смарт-карты, биометрию самих администраторов.

Системы обнаружения аномалий и мониторинга действий пользователей (User Behavior Analytics, UBA) позволяют выявлять подозрительную активность в режиме реального времени. Если сотрудник, обычно работающий с биометрическими данными в дневное время с корпоративного компьютера, внезапно авторизуется ночью с неизвестного устройства и начинает массовую выгрузку записей – система должна заблокировать доступ и оповестить службу безопасности.

Международное сотрудничество в области обмена информацией об угрозах биометрическим системам затруднено геополитической ситуацией. Российские специалисты ограничены в доступе к ряду зарубежных баз данных об уязвимостях и методах атак. Это стимулирует развитие отечественных экспертных центров и систем обмена информацией об инцидентах – например, на базе ФинЦЕРТ Банка России и ГосСОПКА.

Единая биометрическая система (ЕБС) представляет собой государственную информационную систему, созданную для обеспечения идентификации и аутентификации граждан при получении государственных и коммерческих услуг.

Архитектура ЕБС предполагает распределенное хранение данных. Биометрические шаблоны граждан размещаются на серверах оператора – ПАО «Ростелеком», доступ к ним осуществляется через защищенные каналы связи. Организации, оказывающие услуги с использованием биометрии, направляют запросы в систему, которая сравнивает предоставленный биометрический образ с хранящимися шаблонами и возвращает результат – подтверждение или отказ в идентификации.

Процесс регистрации в ЕБС требует личного присутствия гражданина в одной из точек сбора биометрии – отделениях банков, МФЦ, почтовых отделениях. Сотрудник проверяет документ, удостоверяющий личность, и осуществляет захват биометрических данных – фотографирование лица и запись голоса [3]. ЕБС использует механизмы проверки живости, призванные отличить реальное лицо от фотографии или видеозаписи. Пользователю предлагается выполнить определенные действия – повернуть голову, моргнуть, произнести случайную последовательность цифр. Алгоритмы анализируют естественность движений и характеристики голоса.

Прозрачность работы алгоритмов ЕБС вызывает вопросы у части экспертного сообщества. Детальная информация о применяемых методах

распознавания и механизмах защиты не раскрывается публично, что объясняется соображениями безопасности – злоумышленники не должны знать подробностей работы системы. С другой стороны, отсутствие независимого аудита алгоритмов порождает недоверие. Можно ли утверждать, что система достаточно защищена, если ее оценивают только разработчики и заказчик?

Международный опыт показывает разные подходы к этой дилемме. Некоторые страны проводят открытые тестирования биометрических систем с участием независимых исследователей, публикуют технические характеристики точности распознавания, частоты ложных срабатываний [2]. Другие, напротив, предпочитают режим закрытости, считая его необходимым условием безопасности. Россия пока выбрала второй путь.

Количество зарегистрированных в ЕБС граждан по состоянию на начало 2026 года превысило 15 миллионов человек. Это значительный рост по сравнению с первым годом функционирования системы, когда число пользователей измерялось сотнями тысяч. Одновременно растет и привлекательность ЕБС как цели для кибератак. База данных с биометрией 15 миллионов россиян – это желаемая цель злоумышленника.

Реализованные меры защиты включают многоуровневую архитектуру с разделением функций обработки и хранения данных, применение сертифицированных СКЗИ, постоянный мониторинг состояния системы, регулярные испытания на проникновение силами специализированных команд. Оператор отчитывается об отсутствии успешных атак, приведших к утечке данных. Однако попытки атак фиксируются регулярно.

Таким образом, биометрические персональные данные представляют собой уникальный объект правовой охраны и технической защиты, требующий особого внимания в условиях стремительной цифровизации государственных и коммерческих услуг. Анализ российской практики показывает неоднородность подходов к защите биометрических данных.

Действующая нормативная база обеспечивает базовые требования к защите биометрических данных, однако не всегда успевает за технологическими изменениями. Необходима детализация требований для различных сценариев использования биометрии, введение обязательной сертификации критичных систем, усиление ответственности операторов за утечки данных.

Перспективные направления развития системы защиты включают внедрение технологий Privacy by Design, применение блокчейн для обеспечения прозрачности обработки данных, развитие отечественных систем обнаружения аномалий и поведенческой аналитики, создание единых образовательных стандартов для специалистов.

Практическая значимость исследования состоит в формировании комплексного представления о проблемах безопасности биометрических данных в российском контексте и выработке рекомендаций для операторов, регуляторов, разработчиков технологий. Дальнейшие исследования целесообразно сосредоточить на оценке эффективности различных методов защиты биометрии, анализе экономических аспектов инвестиций в безопасность, изучении социальных факторов восприятия биометрических технологий гражданами.

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 05.04.2026).

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: 01.04.2026).

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.

Kunavina O.A.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Sentsova A.Yu.
Ufa University of Science and Technology, Ufa

SECURITY OF BIOMETRIC PERSONAL DATA

Abstract. The article reveals the features of personal data protection. It describes the issues of ensuring the security of biometric personal data, as well as the methods and means of protecting them. Special attention is paid to the practice of the Unified Biometric System and the vulnerabilities identified in its operation.

Keywords: biometric data, personal data, information security, Unified Biometric System, information protection.

УДК 004

Лаптева Е.А.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Исмагилова А.С.
Уфимский университет науки и технологий, Уфа

АДАПТАЦИЯ ПРОЦЕССНОГО ПОДХОДА К ИБ МЕДИЦИНСКИХ ИНФОРМАЦИОННЫХ СИСТЕМ

Аннотация. Региональные медицинские информационно-аналитические системы (РМИАС), обрабатывающие специальные категории персональных данных, требуют соответствия обновленным требованиям Приказа ФСТЭК России № 117. В статье проанализированы нормативные изменения, выявлены ограничения их прямого применения в медицинских организациях и разработана модель адаптации процессного управления ИБ к архитектуре РМИАС. Предложенные организационно-технические механизмы обеспечивают соответствие приказу без нарушения клинических и административных процессов.

Ключевые слова: информационная безопасность, РМИАС, специальные категории персональных данных.

Региональные медицинские информационно-аналитические системы (РМИАС) давно стали основным инструментом сбора, хранения и анализа данных о здоровье населения. Данные системы интегрированы в Единую государственную информационную систему здравоохранения (ЕГИСЗ), в следствие чего ежедневно обрабатывают сведения, от которых напрямую зависят жизнь и здоровье граждан. Однако рост объема данных неизбежно усилил угрозы несанкционированного доступа, что ставит под вопрос как выполнение требований законодательства, так и сохранение доверия пациентов к сервисам здравоохранения.

Вступление в силу Приказа ФСТЭК России от 11.04.2025 № 117 было необходимым шагом для развития нормативного регулирования Российской Федерации. Документ заменил статичную модель Приказа № 17 процессным подходом, где защита информации рассматривается уже как непрерывно действующая система управления рисками [1].

Цель настоящей статьи состоит в проверке практических механизмов реализации требований применительно к РМИАС. Для достижения цели последовательно анализируются нормативные изменения и существующие угрозы в медицинской сфере, а также

предлагаются организационно-технические решения, учитывающие условия работы региональных сегментов ЕГИСЗ.

Правовую базу защиты информации в информационных системах составляют Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» и Федеральный закон от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации», которые подчеркивают статус медицинских сведений как специальной категории персональных данных [2,3]. Приказ № 117 развивает приведенные в Федеральных законах положения, вводя обязательную эшелонированную систему защиты, охватывающую уровни от периметра сети до конечных устройств и организационных процессов. Главным элементом становится трехуровневая иерархия внутренних документов Оператора: политика защиты информации на стратегическом уровне, стандарты по управлению уязвимостями и доступом на тактическом и регламенты рутинных процедур на операционном. Кроме того, вводятся количественные показатели – коэффициент защищенности (Кзи), рассчитываемый не реже одного раза в шесть месяцев, и показатель уровня зрелости процессов защиты (Пзи), оцениваемый раз в два года. Данный подход позволяет перейти информационной безопасности от периодической аттестации к непрерывному мониторингу состояния защищенности, что приобретает важность для региональных систем, где интеграция с ЕГИСЗ сопровождается разнородностью программного обеспечения и различным уровнем технической зрелости медицинских организаций и учреждений.

Особенности применения Приказа № 117 в сфере здравоохранения определяются чувствительностью и ценностью обрабатываемых данных и характерными угрозами. Децентрализованный характер разработки региональных систем создает дополнительные уязвимости при интеграции с федеральными подсистемами, а специфика медицинских данных усиливает последствия любых инцидентов [4]. Приказ учитывает актуальные угрозы, включая облачные технологии и автоматизированные атаки, и устанавливает требования к срокам устранения уязвимостей и контролю привилегированного доступа. В условиях РМИАС эти нормы требуют внимания к сегментации сети и разграничению доступа, поскольку система обслуживает организации с разным уровнем готовности. Утечка медицинских сведений влечет не только административную ответственность, но и моральный вред и материальный ущерб пациентам, подрывая доверие к системе здравоохранения в целом [5].

Для успешной адаптации РМИАС к новым требованиям предлагается комплексная модель, построенная на процессном подходе. Прежде всего необходимо сформировать трехуровневую систему

внутренних документов Оператора, которая обеспечит точное распределение ответственности и полную прослеживаемость всех операций с данными. Далее целесообразно внедрить эшелонированную защиту: на сетевом уровне – средства обнаружения и предотвращения вторжений, на прикладном – контроль привилегированного доступа и защиту конечных устройств, на организационном – автоматизированный расчет показателей Кзи и Пзи. Автоматизация сбора данных для оценки значительно снижает трудозатраты и повышает объективность результатов. Наконец, рекомендуется провести сегментацию системы по уровням доступа с обязательным применением многофакторной аутентификации и шифрования данных при хранении и передаче. Данные меры рекомендованы с учетом необходимости оперативного доступа к информации, важной для оказания своевременной медицинской помощи.

Реализация требований Приказа ФСТЭК России от 11.04.2025 № 117 открывает возможности на путти к совершенствованию обеспечения информационной безопасности в РМИАС. Переход к процессному управлению и эшелонированной модели позволяет оперативно реагировать на угрозы и укреплять доверие граждан к цифровому здравоохранению. Полученные результаты могут послужить основой для дальнейших исследований, по количественной оценке, эффективности мер защиты и стать практическим ориентиром для модернизации региональных сегментов ЕГИСЗ.

Список использованных источников:

1. Приказ Федеральной службы по техническому и экспортному контролю от 11 апреля 2025 г. № 117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений» // Официальный интернет-портал правовой информации. URL: http://publication.pravo.gov.ru/document/0001202506170011 (дата обращения: 10.04.2026).

2. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (в ред. от 24.06.2025) // Официальный интернет-портал правовой информации. URL: http://publication.pravo.gov.ru (дата обращения: 10.04.2026).

3. Федеральный закон от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации» (в ред. от 29.12.2025) // Официальный интернет-портал правовой информации. URL: http://publication.pravo.gov.ru (дата обращения: 10.04.2026).

4. Горбунов Н. А. Персональные данные, обрабатываемые в медицинских информационных системах // КиберЛенинка. 2023. URL:

https://cyberleninka.ru/article/n/personalnye-dannye-obrabatyvaemye-v-meditsinskih-informatsionnyh-sistemah (дата обращения: 10.04.2026).

5. Аверьянов В. С. Цифровая трансформация государственных учреждений // КиберЛенинка. 2024. URL: https://cyberleninka.ru/article/n/tsifrovaya-transformatsiya-gosudarstvennyh-uchrezhdeniy (дата обращения: 10.04.2026).

Lapteva E.A.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Ismagilova A.S.
Ufa University of Science and Technology, Ufa

ADAPTING A PROCESS-BASED APPROACH TO THE SECURITY OF MEDICAL INFORMATION SYSTEMS

Annotation. Regional medical information and analytical systems (RMIS) that process special categories of personal data require compliance with the updated requirements of FSTEC Russia Order No. 117. The article analyzes the regulatory changes, identifies the limitations of their direct application in medical organizations, and develops a model for adapting process-based information security management to the architecture of RMIS. The proposed organizational and technical mechanisms ensure compliance with the order without disrupting clinical and administrative processes.

Keywords: information security, RMIAS, and special categories of personal data.

УДК 004.056:34

Максютов Т.М.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Салов И.В.
Уфимский университет науки и технологий, Уфа

АНАЛИЗ АКТУАЛЬНЫХ НОРМАТИВНО-ПРАВОВЫХ АКТОВ В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ НА ОБЪЕКТАХ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

Аннотация. Рассматриваются действующие нормативно-правовые акты, регулирующие защиту информации на объектах критической

информационной инфраструктуры Российской Федерации. Основное внимание уделяется Федеральному закону № 187-ФЗ, а также подзаконным актам Президента Российской Федерации, ФСТЭК России и ФСБ России. Отдельно анализируются изменения 2025-2026 годов, затронувшие использование российского программного обеспечения на значимых объектах КИИ, порядок категорирования, ведение реестра значимых объектов, а также правила информирования и обмена данными о компьютерных атаках и инцидентах.

Ключевые слова: критическая информационная инфраструктура, защита информации, информационная безопасность, нормативно-правовое регулирование, значимые объекты КИИ, категорирование объектов КИИ, компьютерные инциденты, ФСТЭК России, ФСБ России.

В условиях цифровой трансформации государства особое значение приобретает обеспечение информационной безопасности на объектах критической информационной инфраструктуры (КИИ). Критическая информационная инфраструктура включает в себя информационные системы, информационно-телекоммуникационные сети и автоматизированные системы управления, функционирующие в значимых для государства и общества сферах. Нарушение стабильной работы таких объектов может привести к негативным последствиям для национальной безопасности, экономики и общественной стабильности, что определяет важность правового регулирования в данной области.

Основу правового регулирования составляет Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» [1]. Он определяет основные понятия, круг субъектов КИИ, состав объектов КИИ, порядок их категорирования и полномочия государственных органов в данной сфере.

В 2025 году в Федеральный закон № 187-ФЗ были внесены изменения Федеральным законом от 7 апреля 2025 г. № 58-ФЗ [2]. Поправки закрепили обязанность субъектов КИИ, которым принадлежат значимы объекты, использовать на таких объектах российское программное обеспечение. Кроме того, Правительство Российской Федерации получило полномочия устанавливать требования к программно-аппаратным средствам, а также порядок и сроки перехода на российское ПО. Эти изменения показывают то, что законодательство развивается не только в сторону усиления мер защиты информации, но и в сторону технологической независимости.

Кроме того, продолжает действовать Указ Президента РФ от 1 мая 2022 г. № 250, который усиливает организационную ответственность за состояние информационной безопасности на объектах КИИ. Это

свидетельствует о том, что вопросы связанные с ИБ на объектах КИИ рассматриваются не только как задача профильных специалистов, но и как обязанность руководства организаций.

Важное значение имеет Постановление Правительства РФ от 8 февраля 2018 г. № 127 [3], которым утверждены правила категорирования объектов КИИ. Именно процедура категорирования позволяет определить, является ли объект значимым и подлежат ли применению к нему специальные требования по защите информации. В 2025 году данный порядок был обновлен Постановление правительства РФ от 7 ноября 2025 г. № 1762 [4]. Изменения затронули сам подход к категорированию: теперь он опирается на понятие «типовой отраслевой объект КИИ», были уточнены исходные данные для категорирования, полномочия комиссии и состав сведений, направляемых во ФСТЭК России. Перечень типовых отраслевых объектов позволяет учитывать специфику сферы деятельности, но требует более точного оформления сведений.

Положения о категорировании дополняются ведомственными актами ФСТЭК России. В этой части важное значение имеют приказы ФСТЭК России от 7 декабря 2017 г. № 227 [5], регулирующий порядок ведения реестра значимых объектов КИИ, и приказ ФСТЭК России от 22 декабря 2017 г. № 236, которым утверждена форма направления сведений о результатах категорирования. В 2025 году оба акта были обновлены. Приказ ФСТЭК России от 11 июля 2025 г. № 247 изменил форму направления сведений о результатах присвоения категории значимости, а приказ ФСТЭК России от 17 июля 2025 г. № 254 внес изменения в порядок ведения реестра значимых объектов КИИ. В результате в документации появились более детализированные сведения, в том числе данные о типовом отраслевом объекте, доменном имени и сетевом адресе.

Особое место в регулировании защиты информации на значимых объектах КИИ занимают приказы ФСТЭК России от 21 декабря 2017 г. № 235 [6] и от 25 декабря 2017 г. № 239 [7]. Приказ № 235 устанавливает требования к созданию систем безопасности значимых объектов КИИ, а приказ № 239 – требования по обеспечению их безопасности. Эти акты сохраняют ключевое значение, поскольку именно они определяют, как должна быть организована система защиты информации на практике.

Серьезные изменения в 2025–2026 годах произошли и в части реагирования на компьютерные инциденты. С 30 января 2026 года начал действовать приказ ФСБ России от 25 декабря 2025 г. № 547. Он установил новый порядок информирования ФСБ России о компьютерных атаках и компьютерных инцидентах, реагирования на них и принятия мер по ликвидации их последствий. Одновременно вступил в силу приказ ФСБ России от 25 декабря 2025 г. № 546, который регулирует порядок

обмена информацией о компьютерных атаках и компьютерных инцидентах между субъектами КИИ. Эти изменения усилили требования к оперативности и координации действий при возникновении угроз.

Проведенный анализ показывает, что действующие нормативно-правовые акты в области защиты информации на объектах КИИ образуют целостную систему регулирования, включающую федеральные законы и подзаконные акты в области защиты информации на объектах КИИ образуют целостную систему регулирования, включающую федеральные законы и подзаконные акты. В 2025–2026 годах данная система была существенно обновлена: изменения затронули использование российского программного обеспечения на значимых объектах КИИ, порядок категорирования, ведение реестра значимых объектов, а также правила информирования и обмена данными о компьютерных атаках и инцидентах. Это свидетельствует о том, что законодательство в данной сфере развивается в сторону большей точности требований, усиления контроля и повышения ответственности субъектов КИИ. В будущем можно ожидать дальнейшего развития отраслевого регулирования и совершенствования действующей нормативной базы.

Список использованных источников:

1. Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 N 187-ФЗ (последняя редакция). – URL: https://www.consultant.ru/document/cons_doc_LAW_220885/ (дата обращения: 10.04.2026).

2. Федеральный закон от 07.04.2025 N 58-ФЗ (ред. от 31.07.2025) «О внесении изменений в Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации». – URL: https://www.consultant.ru/document/cons_doc_LAW_502581 (дата обращения: 10.04.2026).

3. Постановление Правительства РФ от 08.02.2018 N 127 (ред. от 07.11.2025) «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». – URL: https://www.consultant.ru/document/cons_doc_LAW_290595/ (дата обращения: 09.04.2026).

4. Постановление Правительства РФ от 7 ноября 2025 г. № 1762 «О внесении изменений в некоторые акты Правительства Российской Федерации». – URL: https://www.consultant.ru/document/cons_doc_LAW_518358/ (дата обращения: 10.04.2026).

5. Приказ ФСТЭК России от 06.12.2017 N 227 (ред. от 17.07.2025) «Об утверждении Порядка ведения реестра значимых объектов

критической информационной инфраструктуры Российской Федерации». – URL: https://www.consultant.ru/document/cons_doc_LAW_290538/2ff7a8c72de3994f30496a0ccbb1ddafdaddf518/ (дата обращения: 10.04.2026).

6. Приказ ФСТЭК России от 21.12.2017 N 235 (ред. от 20.04.2023) «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования». – URL: https://www.consultant.ru/document/cons_doc_LAW_291501/ (дата обращения: 10.04.2026).

7. Приказ ФСТЭК России от 25.12.2017 N 239 (ред. от 28.08.2024) «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации». – URL: https://www.consultant.ru/document/cons_doc_LAW_294287/ (дата обращения: 11.04.2026).

Maksyutov T.M.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Salov I.V.
Ufa University of Science and Technology, Ufa

ANALYSIS OF CURRENT LEGAL AND REGULATORY ACTS IN THE FIELD OF INFORMATION PROTECTION AT CRITICAL INFORMATION INFRASTRUCTURE FACILITIES

Abstract. This article examines the current legal acts regulating information protection at critical information infrastructure facilities in the Russian Federation. Special attention is paid to Federal Law No. 187-FZ and subordinate acts of the President, the Government, FSTEC of Russia, and the FSB of Russia. The paper also analyzes the 2025–2026 amendments concerning Russian software, categorization, the register of significant facilities, and incident reporting.

Keywords: critical information infrastructure, information protection, information security, legal regulation, significant CII facilities, CII categorization, computer incidents, FSTEC of Russia, FSB of Russia.

УДК 004

Моисеева К.А.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Валеев С.С.
Уфимский университет науки и технологий, Уфа

АНАЛИЗ НОРМАТИВНЫХ ИЗМЕНЕНИЙ В СФЕРЕ БЕЗОПАСНОСТИ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

Аннотация. Рассматривается анализ нормативных изменений в сфере безопасности критической информационной инфраструктуры и их влияние на деятельность субъектов. Обсуждаются последствия внедрения типовых отраслевых объектов, усиления цифровой прозрачности и требований импортозамещения, роль аудита как механизма обеспечения соответствия субъектов критической информационной инфраструктуры актуализированным нормативным требованиям.

Ключевые слова: критическая информационная инфраструктура, нормативные изменения, типовые отраслевые объекты, цифровая прозрачность, импортозамещение, аудит.

Субъектам критической информационной инфраструктуры (КИИ) из разных отраслей требуется постоянное совершенствование системы защиты своих объектов. Изменения в законодательстве актуализируют требования к категорированию и контролю объектов КИИ, в частности, вводя обязательное использование типовых отраслевых перечней [1]. Такое обновление правил переносит внимание с формального соблюдения требований на реальную безопасность, где главным способом становится аудит безопасности КИИ.

Анализ текущих изменений в регулировании показывает переход от субъективного подхода к унифицированному отраслевому. Постановление Правительства РФ от 07.11.2025 № 1762 закрепило обязательное использование Перечней типовых отраслевых объектов КИИ при категорировании [2]. Ранее субъекты КИИ самостоятельно выявляли значимые объекты на основе внутренних оценок, что, в ряде случаев, приводило к пропускам критических частей инфраструктуры. С учетом изменений процесс категорирования основывается на обязательном сопоставлении имеющихся информационных систем, сетей и автоматизированных систем управления с утвержденными типовыми

отраслевыми перечнями, что существенно снижает субъективность и обеспечивает единый подход к контролю [1, 3].

Внесенные изменения позволяют снизить риски неучтенных уязвимостей в критической информационной инфраструктуре. Одновременно новая редакция формы направления сведений, утвержденная Приказом ФСТЭК России от 22.12.2025 № 236 (в редакции Приказа ФСТЭК России от 11.07.2025 № 247), предусматривает предоставление дополнительных сведений об объекте, включая доменные имена и внешние сетевые адреса информационных ресурсов при их подключении к сети «Интернет» [4]. Такие данные повышают прозрачность сведений, направляемых субъектами КИИ в ФСТЭК России, и создают основу для более эффективного государственного контроля защищенности объектов.

Параллельно усиливаются требования к технологической независимости. Федеральный закон от 31.07.2025 № 325 предусматривает создание перечня доверенных российских программ для электронных вычислительных машин и баз данных [5]. Для объектов критической информационной инфраструктуры, включенных в типовые отраслевые перечни, вводятся дополнительные требования по использованию такого программного обеспечения. Такие меры направлены на снижение рисков, связанных с применением зарубежных компонентов, и создают правовую основу для последовательного их импортозамещения.

Таблица 1

Сравнение подходов к категорированию объектов КИИ

Аспект	До изменений	После изменений
Выявление объектов КИИ	Самостоятельная оценка	Обязательное использование типовых отраслевых перечней
Оценка значимости	Субъективный анализ	Отраслевые особенности и наихудшие сценарии
Прозрачность сведений	Базовый объем	Расширенные сведения
Технологическая независимость	Общие требования	Перечень доверенных российских программ

В практическом плане принятые изменения обязывают субъектов КИИ провести выявление объектов критической информационной инфраструктуры путем сопоставления имеющихся информационных систем, сетей и автоматизированных систем управления с перечнями типовых отраслевых объектов КИИ [3]. Ранее присвоенные категории значимости подлежат приведению в соответствии с новыми правилами [2]. Кроме того, устанавливается обязанность представлять в ФСТЭК России расширенный состав сведений об объектах и обеспечивать их актуальность [4].

Переход на отечественное программное обеспечение и аппаратные средства сопровождается необходимостью решения вопросов совместимости с существующими системами, а также проведения дополнительной сертификации средств защиты информации. Обновленные требования ФСТЭК усиливают риск-ориентированный подход при оценке значимости объектов КИИ. Это требует учитывать возможные последствия компьютерных инцидентов и отражается на внутренних процедурах оценки и оформлении документации [6].

В этих условиях аудит информационной безопасности выступает частью практической реализации нормативных требований. Согласно требованиям ФСТЭК, субъекты КИИ обязаны проводить регулярный контроль состояния защищенности значимых объектов, включающий комплаенс-аудит и инструментальный анализ защищенности [7]. Систематическое проведение аудита позволяет выявить несоответствия между представляемыми сведениями и фактическим состоянием объектов.

Аудит непосредственно связан с процедурой категорирования объектов по типовым отраслевым перечням: он проверяет полноту и доверенность отнесения систем к перечням, а также соответствие реализованных мер защиты обновленным критериям значимости [2, 3]. Также аудит обеспечивает выявление различных уязвимостей на уровне архитектуры, конфигурации и программного обеспечения в процессе импортозамещения. В результате формируется объективная оценка состояния системы защиты, включая процессы мониторинга и реагирования на инциденты.

Изменения заметно повлияли на порядок обеспечения безопасности КИИ. Для организаций это означает необходимость пересмотра уже выстроенных процессов и приведения их в соответствие с новыми требованиями. Сейчас аудит информационной безопасности используется как практический способ проверки выполнений мероприятий и оценки текущего состояния защищенности. Его проведение позволяет выявить проблемные участки и скорректировать систему защиты с учетом действующих требований.

Список использованных источников:

1. Правительство РФ утвердило перечень типовых объектов КИИ [Электронный ресурс] // РБК Компании. – 27 февраля 2026. – URL: https://companies.rbc.ru/news/3W11TNmuF9/pravitelstvo-rf-utverdilo-perechen-tipovyih-obektov-kii/ (дата обращения 11.03.2026).

2. Постановление Правительства Российской Федерации 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» (в ред. от 07.11.2025 № 1762) [Электронный ресурс] // КонсультантПлюс: справочно-правовая система / URL: https://www.consultant.ru/document/cons_doc_LAW_290595/1b445ea2ca2e30b9350044e3133a1aced3b23a6c/ (дата обращения 13.03.2026).

3. Распоряжение Правительства Российской Федерации от 26.02.2026 № 360-р «Об утверждении перечня типовых отраслевых объектов критической информационной инфраструктуры Российской Федерации» [Электронный ресурс] // КонсультантПлюс: справочно-правовая система / URL: https://www.consultant.ru/document/cons_doc_LAW_527541/ (дата обращения 13.03.2026).

4. Приказ ФСТЭК России от 22.12.2017 N 236 (ред. от 11.07.2025) "Об утверждении формы направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий" [Электронный ресурс] // КонсультантПлюс: справочно-правовая система / URL: https://www.consultant.ru/document/cons_doc_LAW_295855/ / (дата обращения 13.03.2026).

5. Федеральный закон от 31.07.2025 N 325-ФЗ "О внесении изменений в отдельные законодательные акты Российской Федерации".

6. Федеральный закон от 26 июля 2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (в ред. от 07.04.2025 №58-ФЗ) [Электронный ресурс] // КонсультантПлюс: справочно-правовая система / URL: https://www.consultant.ru/document/cons_doc_LAW_220885/ (дата обращения 13.03.2026).

7. Аудит безопасности критической информационной инфраструктуры. Учебное пособие. – СПб.: Наукоемкие технологии, 2023. – 122 с. - ISBN 978-5-907618-78-7.

Moiseeva K. A.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Valeev S. S.
Ufa University of Science and Technology, Ufa

THE IMPACT OF REGULATORY CHANGES GOVERNING CRITICAL INFORMATION INFRASTRUCTURE ON AUDIT PRACTICES

Abstract. This analyzes regulatory changes in the field of critical information infrastructure security and their impact on the activities of subject entities. The consequences of implementing typical industry objects, enhancing digital transparency, and import substitution requirements are discussed, as well as the role of audit as a mechanism for ensuring CII subjects' compliance with updated regulatory requirements.

Keywords: critical information infrastructure, regulatory changes, typical industry objects, digital transparency, import substitution, audit.

УДК 003

Набиева А.И.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Яппаров Р.М.
Уфимский университет науки и технологий, Уфа

СОВЕРШЕНСТВОВАНИЕ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ В ОРГАНЕ МЕСТНОГО САМОУПРАВЛЕНИЯ

Аннотация. В статье анализируются организационные и правовые основы защиты информации в органе местного самоуправления. Рассмотрены федеральная и региональная нормативно-правовая база, виды защищаемой информации, модель угроз и распределение ответственности. Обосновано утверждением о том, что эффективная система защиты информации требует не только технических, но и организационно-правовых мер, включающих локальные акты и обучение персонала.

Ключевые слова: защита информации, орган местного самоуправления, организационные меры, модель угроз.

За последние годы количество целенаправленных кибератак на муниципальные структуры резко возросло. Городские администрации, сельские поселения и другие территориальные органы подвергаются атакам чаще, чем исполнительные органы государственной власти в силу своей меньшей защищенности периметров, территориальной удаленности и активного внедрения цифровых платформ (портал «Госуслуги», муниципальные сервисы). В этих условиях организационно-правовые аспекты системы защиты информации (далее – СЗИ) приобретают стратегическое значение, так как именно правовая база и правильная организация процессов определяют эффективность применяемых технических средств защиты [1].

Правовое обеспечение защиты информации в органах местного самоуправления базируется на иерархической системе актов:

1. Конституция РФ (ст. 23, 24) – гарантирует право на неприкосновенность частной жизни, личную и семейную тайну, а также обязывает органы местного самоуправления (далее - МСУ) обеспечивать доступ граждан к информации о своей деятельности.

2. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» – регулирует отношения при поиске, получении, передаче информации и устанавливает обязанность обеспечения доступа к информации о деятельности органов МСУ.

3. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» – задает правовой режим обработки и защиты персональных данных (далее - ПДн).

4. Федеральный закон от 28.12.2010 №3 90-ФЗ «О безопасности» – определяет принципы (законность, системность, приоритет предупредительных мер) и полномочия органов МСУ в области безопасности.

5. Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи» – важен для юридической значимости документооборота.

6. Указ Президента от 06.03.19997 № 188 «Об утверждении Перечня сведений конфиденциального характера».

7. Постановление Правительства от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» – требования к защите ПДн в информационных системах.

8. Приказ ФСТЭК от 11.04.2025 № 117 «Об утверждении Требований о защите информации в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений»

– требования к защите информации в информационных системах органов местного самоуправления.

Кроме того, на региональном уровне система может дополняться соответствующим актом. Так, в Республике Башкортостан введен в действие Указ Главы Республики Башкортостан от 21.09.2012 № УП-365 «Об утверждении основ организации защиты информации в Республике Башкортостан». Данный акт непосредственно определяет:

1) структурные элементы СЗИ (госорганы, органы МСУ, подведомственные организации, лицензиаты ФСТЭК/ФСБ);

2) что руководители органов МСУ лично возглавляют систему защиты информации;

3) порядок согласования технических заданий на создание информационных систем с уполномоченным республиканским органом.

Так, в Администрации ГО г. Уфа, как крупном, территориально распределенном органе местного самоуправления, СЗИ построена по следующему принципу:

1. Руководитель Администрации ГО г. Уфа несет персональную ответственность за организацию защиты информации (в том числе составляющей государственную тайну, если таковая имеется).

2. Непосредственное руководство деятельностью СЗИ возлагается на одного из заместителей руководителя.

3. Подразделения (штатные специалисты) по защите информации реализуют организационные и технические меры.

4. Подведомственные учреждения обязаны согласовывать с Администрацией ГО г. Уфа технические задания на создание или модернизацию информационных систем в части соблюдения требований информационной безопасности.

Ключевая организационная проблема, отмеченная в исходном материале, – сложность построения единой централизованной СЗИ из-за множества структурных подразделений и удаленных объектов. Данное обстоятельство требует не только технических, но и четких организационно-распорядительных мер (локальных актов, регламентов, назначения ответственных на местах).

Так, например, в Администрации ГО г. Уфа защите подлежат персональные данные сотрудников и граждан, служебная информация ограниченного распространения, сведения, обрабатываемые в муниципальных информационных системах (включая систему электронного документооборота), речевая информация в защищаемых помещениях, а также данные, передаваемые по каналам связи за пределы контролируемой зоны. Организационно-правовые меры включают разработку локальной нормативной базы (инструкции по делопроизводству, положения об организации контроля исполнения

документов, соглашения о неразглашении), категорирование информации для концентрации ресурсов на критически важных активах, регулярное обучение персонала правилам цифровой гигиены и распознаванию фишинга, контроль доступа и учет носителей, а также уведомление Роскомнадзора о начале обработки персональных данных.

Согласно Приказу ФСТЭК №117, Администрация ГО г. Уфа обязана разработать актуальную модель угроз, учитывающую как внешние (DDoS, вредоносное ПО), так и внутренние угрозы (инсайдеры, халатность). На практике наиболее критичны компрометация учетных данных через фишинг, утечка персональных данных через инсайдеров и нарушение доступности сервисов [2].

Администрация ГО г. Уфа использует систему автоматизированного электронного документооборота (далее – СЭД), которая обеспечивает полный цикл работы с документами (от поступления до списания в дело). Организационно-правовыми основами здесь выступают: Федеральный закон № 63-ФЗ «Об электронной подписи», Правила делопроизводства в федеральных органах исполнительной власти (распространяются и на органы МСУ как единая нормативная основа), ГОСТ Р 7.0.97-2016 (ранее ГОСТ Р 630-2003) – требования к оформлению организационно-распорядительных документов [3].

Отметим, что использование СЭД само по себе не гарантирует защиту информации, нужны еще и организационные меры [4]:

1) разграничить права доступа сотрудников;

2) обеспечить регистрацию всех действий с документами (журнал аудита);

3) применять усиленную квалифицированную электронную подпись при обмене юридически значимыми документами с внешними контрагентами.

Таким образом, организационно-правовые аспекты защиты информации в органах местного самоуправления образуют фундамент для применения технических мер. Сформированная правовая база на федеральном и региональном уровне сталкивается с проблемами территориальной удаленности и человеческим фактором.

На наш взгляд, ключевыми направлениями совершенствования защиты информации в органе местного самоуправления являются усиление контроля за инсайдерами, регулярное обучение персонала, приведение модели угроз в соответствие с требованиями ФСТЭК и согласование проектов информационных систем с республиканскими органами. Эффективная система защиты информации – это непрерывный процесс аудита, корректировки локальных актов и обучения кадров.

Список использованных источников:

1. Аверченков, В. И. и др. Аудит информационной безопасности органов исполнительной власти. – М.: ФЛИНТА, 2021.
2. Гродзенский, Я. С. Информационная безопасность. – М.: Проспект, 2022.
3. Ищейнов, В. Я. Информационная безопасность и защита информации: теория и практика. – М.: Директ-Медиа, 2021.
4. Шагапов, И. А. К вопросу построения системы защиты информации / И. А. Шагапов // 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. 51-54.

Nabieva A. I.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Yapparov R.M.
Ufa University of Science and Technology, Ufa

IMPROVING THE INFORMATION PROTECTION SYSTEM IN LOCAL GOVERNMENT BODIES

Abstract. The article analyzes the organizational and legal foundations of information protection in a local government body. It examines the federal and regional regulatory framework, the types of protected information, the threat model, and the distribution of responsibilities. The article argues that an effective information protection system requires not only technical measures but also organizational and legal measures, including local regulations and staff training.

Keywords: information protection, local government body, legal support, threat model.

УДК 349.2:004.056

Резбаева В.М.
Стерлитамакский филиал
Уфимского университета, Стерлитамак

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

ПРАВОВЫЕ АСПЕКТЫ ВНЕДРЕНИЯ DLP-СИСТЕМ: БАЛАНС МЕЖДУ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ И ТАЙНОЙ СВЯЗИ

Аннотация. В статье исследуется актуальная правовая коллизия между внедрением систем предотвращения утечек информации (DLP) и конституционным правом работников на тайну связи в условиях цифровизации трудовых отношений. Проведен анализ рисков, возникающих при использовании корпоративных устройств в личных целях, обоснована необходимость перехода от скрытого мониторинга к легитимному алгоритму контроля. В работе предложен пошаговый юридический механизм внедрения систем информационной безопасности, позволяющий работодателю минимизировать уголовные и административные риски.

Ключевые слова: информационная безопасность, DLP-системы, тайна переписки, персональные данные, коммерческая тайна, трудовое право, защита информации, цифровой комплаенс.

Актуальность темы исследования обусловлена масштабной трансформацией трудовых отношений и массовым переходом бизнеса на дистанционный формат работы. Оптимизация операционных расходов (аренда помещений, содержание инфраструктуры) и цифровизация секторов экономики привели к размытию границ между рабочим и личным цифровым пространством сотрудника.

Смешение личного и рабочего цифрового пространства при использовании корпоративных устройств существенно повышает вероятность утечек данных и заражения систем вирусным ПО, создавая прямую угрозу охраняемым законом тайнам. Для организаций подобные инциденты оборачиваются не только существенными репутационными издержками, но и серьезными финансовыми санкциями со стороны регуляторов. Таким образом, поиск баланса между внедрением систем мониторинга (DLP-систем, Data Loss Prevention) и обеспечением

конституционного права граждан на тайну переписки [1] приобретает особую значимость.

Центральным правовым конфликтом при внедрении DLP-систем является коллизия между конституционным правом работника на тайну связи [1] и правомочиями работодателя по контролю над использованием корпоративных ресурсов, закрепленными в ст. 209 ГК РФ и трудовом законодательстве [2, 3].

С учетом отсутствия прямого законодательного регулирования, легитимация использования DLP-систем переносится в плоскость локального нормотворчества организации. Легитимность мониторинга служебной деятельности обеспечивается через соблюдение формализованного юридического протокола, ключевыми элементами которого выступают информационная прозрачность и заблаговременное уведомление работников о применении технических средств защиты данных [4].

Процедура внедрения включает в себя следующие этапы:

1. Правовое закрепление целей: В локальных актах (ПВТР, Положение об ИТ-ресурсах) необходимо прямо указать, что корпоративная сеть и техника предоставлены сотруднику исключительно для выполнения трудовой функции. Это лишает сотрудника законных оснований ожидать «приватности» при их использовании.

2. Деконструкция «тайны связи» через уведомление: Юридический парадокс заключается в том, что тайна связи защищена законом, пока она остается «тайной». Если сотрудник под роспись уведомлен о том, что все каналы связи будут отслеживаться, он теряет право ссылаться на скрытый характер вмешательства в частную жизнь.

3. Документальный пакет (Legal Checklist): Приказ о внедрении системы, в котором прописано обоснование необходимости внедрения DLP-системы.

4. Лист ознакомления.

5. Положение о коммерческой тайне. Таким образом, введения режима DLP становится способом защиты активов, без данного документа, внедрение DLP можно расценить как слежку.

6. Технико-правовой барьер: рекомендуется упомянуть использование информационных окон, которые всплывают при включении компьютера. Это служит неоспоримым доказательством того, что работник осознавал факт контроля в конкретный момент времени.

Соблюдение вышеуказанного алгоритма позволяет минимизировать правовые риски, которые в современной юридической доктрине и практике традиционно классифицируются по трем уровням ответственности:

Уголовно-правовой уровень (ст. 137, 138 УК РФ) [5], это риск квалификации действий работодателя как нарушения конституционных прав на неприкосновенность частной жизни и тайну переписки в случае скрытого мониторинга.

Административно-трудовой уровень (ст. 5.27, 13.11 КоАП РФ) [6] риски, связанные с нарушением процедур обработки персональных данных работников и требований трудового законодательства (ст. 86 ТК РФ) [3], что влечет наложение штрафных санкций со стороны ГИТ и Роскомнадзора.

Гражданско-правовой уровень, представляют собой риски признания судом полученных цифровых доказательств недопустимыми, что делает невозможным привлечение работника к материальной ответственности или обоснование законности его увольнения.

Подводя итог исследованию, можно сделать вывод, что внедрение DLP-систем в современных реалиях дистанционной работы является не просто технической опцией, а критической необходимостью для обеспечения информационной безопасности и финансовой устойчивости бизнеса. Только методом объединения технических средств защиты и правовым алгоритмом позволяет создать безопасную цифровую среду.

Список использованных источников:

1. Конституция Российской Федерации: принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020. – Текст: электронный // КонсультантПлюс: [сайт]. – URL: https://www.consultant.ru/document/cons_doc_LAW_28399/ (дата обращения: 08.04.2026).

2. Гражданский кодекс Российской Федерации (часть первая): от 30.11.1994 № 51-ФЗ: (ред. от 31.07.2025, с изм. от 25.03.2026). – Текст: электронный // КонсультантПлюс: [сайт]. – URL: https://www.consultant.ru/document/cons_doc_LAW_5142/ (дата обращения: 08.04.2026).

3. Уголовный кодекс Российской Федерации: от 13.06.1996 № 63-ФЗ: (ред. от 20.02.2026). – Текст: электронный // КонсультантПлюс: [сайт]. – URL: https://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения: 08.04.2026).

4. Кодекс Российской Федерации об административных правонарушениях: от 30.12.2001 № 195-ФЗ: (ред. от 23.03.2026). – Текст: электронный // КонсультантПлюс: [сайт]. – URL: https://www.consultant.ru/document/cons_doc_LAW_34661/ (дата обращения: 08.04.2026).

5. Трудовой кодекс Российской Федерации: от 30.12.2001 № 197-ФЗ: (ред. от 29.12.2025, с изм. от 06.02.2026). – Текст: электронный //

КонсультантПлюс: [сайт]. – URL: https://www.consultant.ru/document/cons_doc_LAW_34683/ (дата обращения: 08.04.2026).

6. КоАП РФ Статья 5.27. Нарушение трудового законодательства и иных нормативных правовых актов... (Ответы на вопросы). – Текст: электронный // КонсультантПлюс: [сайт]. – URL: https://www.consultant.ru/document/cons_doc_LAW_34661/7ff50b874c8cbce814266fd45eb5fff8b30449b6/ (дата обращения: 08.04.2026).

7. Регламент обеспечения информационной безопасности: основные положения и правила разработки. – Текст: электронный // Smart-Soft: [сайт]. – URL: https://www.smart-soft.ru/blog/reglament_obespechenija_informatsionnoj_bezopasnosti/ (дата обращения: 08.04.2026).

Rezbaeva V.M.
Sterlitamak Branch of Ufa University, Sterlitamak

Scientific supervisor:
Kornilova A.A.
Ufa University of Science and Technology, Ufa

LEGAL ASPECTS OF DLP SYSTEMS IMPLEMENTATION: BALANCING INFORMATION SECURITY AND PRIVACY OF COMMUNICATIONS

Abstract. The article examines the current legal conflict between the implementation of Data Loss Prevention (DLP) systems and the constitutional right of employees to the privacy of communications in the context of the digitalization of labor relations. An analysis of the risks arising from the use of corporate devices for personal purposes is conducted, and the necessity of transitioning from covert monitoring to a legitimate control algorithm is justified. The paper proposes a step-by-step legal mechanism for implementing information security systems, allowing the employer to minimize criminal and administrative risks.

Keywords: information security, DLP systems, privacy of correspondence, personal data, commercial secret, labor law, information protection, digital compliance.

УДК 004.056

Рябова К.А.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Яппаров Р.М.
Уфимский университет науки и технологий, Уфа

ВОЗМОЖНОСТИ ПРИМЕНЕНИЯ KASPERSKY UNIFIED MONITORING AND ANALYSIS PLATFORM (KUMA) В ПРАВООХРАНИТЕЛЬНЫХ ОРГАНАХ

Аннотация. В статье анализируются возможности применения Kaspersky Unified Monitoring and Analysis Platform (KUMA) при решении задач обеспечения информационной безопасности (ИБ) в правоохранительной сфере. Предлагаются решения, связанные с созданием единого центра сбора, анализа и корреляций событий ИБ.

Ключевые слова: защита информации, информационная безопасность, SIEM-система, мониторинг событий, события информационной безопасности, инциденты безопасности.

В инфраструктуре любой организации, которая работает с массивами данных, осуществляется множество событий, которые могут быть связаны с инцидентами информационной безопасности. К таким относятся, например, неисполнение политик ИБ пользователями или проникновение злоумышленников в локальную сеть. Для результативного обнаружения, исследования и принятия мер в отношении инцидентов такого рода необходима унифицированная система сбора и обработки данных. В этих целях используются платформы SIEM (Security Information and Event Management), которые позволяют объединять, сопоставлять и анализировать события информационной безопасности из множества источников в рамках единого интерфейса.

Ключевая функция SIEM-системы заключается не только в агрегации данных о событиях из разнообразных источников, таких как сетевое оборудование, программное обеспечение (ПО), системные журналы и средства защиты, но и в автоматизации процесса выявления инцидентов безопасности. Система также обеспечивает своевременное оповещение специалистов по ИБ, тем самым освобождая службу от выполнения большого количества рутинных задач и сокращая в разы время их реагирования. Весь процесс сбора и представления информации

происходит автоматически в унифицированном интерфейсе программы, который понятен интуитивно.

SIEM-системы изначально создавались для того, чтобы собирать и быстро анализировать информацию о происшествиях, связанных с ИБ. Поэтому на начальном этапе внедрения SIEM важно фокусироваться на том, чтобы наладить сбор, хранение и обработку этих данных. Но возможности SIEM не заканчиваются на этом. Данные системы также помогают находить и разбираться в инцидентах безопасности, вести учет всех устройств и ресурсов, а также проверять, насколько хорошо защищена определенная информация в организации.

В настоящее время правоохранительные органы сталкиваются с ростом киберпреступности и острой необходимостью быстрой обработки больших массивов информации [5]. В этих условиях особую роль играют SIEM-системы, к которым относится Kaspersky Unified Monitoring and Analysis Platform (KUMA), разработанная компанией «Лаборатория Касперского». KUMA обеспечивает централизованный мониторинг, анализ и реагирование на инциденты информационной безопасности, что делает ее перспективным инструментом для правоохранительных органов. Это единая платформа для комплексного управления кибербезопасностью, включающая в себя функции мониторинга, анализа угроз и оперативного реагирования в пределах корпоративной экосистемы.

Мы предлагаем распространить данное решение для обеспечения ИБ в правоохранительных органах. Для этого на каждом компьютере в корпоративной сети правоохранительного органа разворачивается ПО Kaspersky Endpoint Security. Оно непрерывно осуществляет мониторинг активности системы, включая запущенные процессы, активные сетевые подключения и модификации файлов. Собранная информация о происходящем на устройствах передается на сервер KUMA. В интерфейсе эти события отображаются в виде простого списка, аналогично стандартным журналам событий операционных систем Windows или Linux.

К основным направлением применения KUMA относятся:

1. Выявление и расследование киберпреступлений.
2. Мониторинг критической информационной инфраструктуры (КИИ).
3. Аналитическая поддержка оперативно-розыскной деятельности.
4. Автоматизация реагирования на инциденты.
5. Централизация управления безопасностью.
6. Использование технологий искусственного интеллекта (ИИ).

Стоит отметить, что в ПО в новых версиях платформы внедряются технологии машинного обучения для приоритизации инцидентов,

выявления аномалий и повышения точности анализа. Одной из наиболее важных функций является применение алгоритмов машинного обучения для построения базовых моделей поведения пользователей и систем. Например, если сотрудник внезапно начинает активно скачивать данные или подключаться к нетипичным ресурсам, система автоматически пометит это как потенциальную угрозу.

Одной из проблем традиционных SIEM-систем является большое количество ложных тревог. В свою очередь применение ИИ в KUMA позволит этого избежать. KUMA анализирует события, учитывает историю и обучается на предыдущих инцидентах ИБ.

KUMA представляет собой интегрированную платформу, объединяющую следующие компоненты: технологии защиты конечных точек (EPP) и обнаружения/реагирования (EDR), шлюзы для защиты электронной почты и веб-трафика, изолированную среду выполнения (песочницу), инструменты для анализа сетевой активности, платформу для повышения уровня киберграмотности сотрудников, аналитические данные о текущих киберугрозах, а также систему управления событиями безопасности и их корреляции (SIEM). Все эти элементы тесно связаны, взаимно усиливают друг друга и распространяются под единой лицензией.

Правоохранительные органы на постоянной основе выполняют широкий спектр задач, связанных с обеспечением безопасности. Среди которых: борьба с киберпреступностью, расследование цифровых инцидентов, защита государственных информационных систем, противодействие терроризму и экстремизму в сети и др. Для эффективного выполнения этих задач требуется инструмент, способный быстро и качественно обрабатывать большие массивы данных и выявлять скрытые взаимосвязи между событиями - именно такие возможности предоставляет KUMA. В связи с этим внедрение этой системы в деятельность правоохранительных органов является своевременным.

Список использованных источников:

1. Зырянова, Т. Ю. Управление информационной безопасностью: учебное пособие / Т. Ю. Зырянова. – Екатеринбург: АВ, 2023. – С. 96.

2. Окороков, В. А. Безопасность операционных систем / В. А. Окороков. – Санкт-Петербург: Лань, 2024. – С. 228.

3. Парфенов, Ю. П. Средства управления и защиты информационных ресурсов автоматизированных систем: учебное пособие / Ю. П. Парфенов. – Москва: ФЛИНТА, 2022. – С.120.

4. Тумбинская, М. В. Защита информации на предприятии: учебное пособие для вузов / М. В. Тумбинская, М. В. Петровский. – 2-е изд., стер. – Санкт-Петербург: Лань, 2025. – С.184.

5. Шагапов, И. А. К вопросу построения системы защиты информации / И. А. Шагапов // 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. 51-54.

Ryabova K.A.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Yapparov R.M.
Ufa University of Science and Technology, Ufa

APPLICATION OF KASPERSKY UNIFIED MONITORING AND ANALYSIS PLATFORM (KUMA) IN LAW ENFORCEMENT

Abstract. This article describes the specifics of using Kaspersky Unified Monitoring and Analysis Platform (KUMA). It examines and analyzes information security (IS) issues in law enforcement, as well as how to address them by creating a unified center for collecting, analyzing, and correlating information security events.

Keywords: information protection, information security, SIEM system, event monitoring, information security events, security incidents.

УДК 004.056

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

Научный руководитель:
Яппаров Р.М.
Уфимский университет науки и технологий, Уфа

РАССЛЕДОВАНИЕ КОМПЬЮТЕРНЫХ ИНЦИДЕНТОВ: ПОДХОДЫ, РЕШЕНИЯ, ПРАКТИКА

Аннотация. В данной статье анализируется современная методика расследования компьютерных инцидентов с учетом требований российского законодательства и регуляторов. Особое внимание уделено этапам реагирования и применению отечественного программного обеспечения. Обосновывается необходимость использования единой

таксономии угроз. Предлагаются новые подходы к решению проблемы на основе действующей практики.

Ключевые слова: расследование компьютерных инцидентов, реагирование на инциденты ИБ, форензика, SIEM-системы.

В современных условиях организации нуждаются в построении эффективных процессов расследования компьютерных инцидентов с использованием отечественных методик и программных решений. Многоэтапный характер целенаправленных атак включает: рекогносцировку, проникновение, закрепление, распространение и целевое воздействие. Результат реализации компьютерной атаки представляет собой компьютерный инцидент, если он выражается в нарушении или прекращении функционирования информационных ресурсов, сетей их взаимодействия, и (или) нарушении безопасности, обрабатываемой в данных ресурсах информации, согласно национальному стандарту ГОСТ Р 59709-2022 [1]. Его расследование требует квалификации специалистов ИБ, сертифицированных средств защиты, имеющих соответствующие функциональные возможности и формализованной методической базы. В этой статье мы попытаемся проанализировать отечественную практику расследования компьютерных инцидентов на основе обзора российского инструментария для его реализации.

Существующая методика в настоящее время основывается на процессной модели, включающей следующие ее этапы:

1. Подготовительный этап. Включает создание политики реагирования на инциденты ИБ и расследований компьютерных инцидентов, распределение ролей и ответственности сотрудников, поддержание актуальной информации о инфраструктуре и активах, настройку средств ЗИ и средств регистрации событий ИБ, обучение персонала и мониторинг состояния ИБ в организации.
2. Обнаружение и идентификация. Выявление факта компьютерного инцидента из информации от систем управления событиями информационной безопасности (SIEM), журналов аудита ОС и прикладного ПО, сотрудников, пользователей, сработавших средств защиты информации (антивирусов, межсетевых экранов), систем анализа сетевого трафика (NTA). Проведение первичного анализа: исключение ложного срабатывания, определение категории инцидента, местоположения, уровня критичности и влияния на функционирование информационной инфраструктуры.
3. Сдерживание (локализация). Изоляция сегмента сети, в котором произошел инцидент, отключение сервисов, блокирование скомпрометированных учетных записей, приостановление

подозрительных процессов. Важным аспектом, помимо оперативности, является сохранение значимых для дальнейшего расследования данных, поэтому необходимо сначала создать образы дисков и накопителей. В случае, когда любое воздействие ведет к уничтожению артефактов и данных об инциденте, лучшим решением, при отсутствии критического воздействия на работу инфраструктуры, является изоляция сегмента без дальнейшего вмешательства.

4. Форензика. Извлечение и анализ данных с скомпрометированных устройств, включая оперативную память и жесткие диски, исследование журналов серверов, рабочих станций и сетевых устройств для фиксации следов вторжения, проверка сетевого трафика для выявления подозрительных подключений и каналов управления, обнаружение и анализ вредоносного кода, построение хронологии и вектора действий злоумышленника с определением точки входа.

5. Устранение и восстановление. Удаление вредоносного кода, окончательное исключение зараженного сегмента, устранение уязвимостей, используемых для проникновения, восстановление данных с помощью резервных копий, приведение в стабильное функционирование систем, сервисов и приложений, усиление мониторинга событий ИБ.

6. Расследование инцидента, пост-анализ. Документирование события, включая причины возникновения, хронологию, вектор, затронутые активы, факторы развития. Переоценка уязвимостей и угроз, системы защиты информации, корректировка мер ЗИ, обучение персонала.

На российском рынке аппаратного и программного обеспечения представлено большое количество инструментов для качественной реализации представленной методики [2]:

«KOMRAD Enterprise SIEM», сертифицированный продукт, позволяющий получать события из различных источников, приводить их к единому формату, фильтровать критические события и выявлять потенциальные инциденты;

«R-Vision SIEM», обеспечивающий интеграцию с Kubernetes, поддержку распределенных инсталляций и режима высокой доступности, контейнеризации, а также централизованное управление событиями ИБ, их анализ;

«MaxPatrol SIEM» – централизованный сбор событий безопасности, их корреляция в реальном времени, автоматизированное выявление инцидентов, управление жизненным циклом инцидентов, интеграцию с внешними системами, а также наличие инструментов для расследования инцидентов; SOAR-платформы («R-Vision SOAR», «Security Vision SOAR», «ePlat4m Orchestra») [3];

«Гарда Монитор» осуществляющий анализ трафика и выявления угроз;

«MK Enterprise» – DFIR-инструмент, предназначенный для криминалистического анализа данных с скомпрометированных устройств.

Мы предлагаем дополнить существующую методику обязательным применением таксономии, в частности таксономии ФСТЭК России. Таксономия ФСТЭК России представляет собой структурированную классификацию действий злоумышленников, включающую 10 целевых этапов компьютерной атаки [4]: сбор информации, получение первоначального доступа, внедрение и исполнение вредоносного ПО, закрепление доступа, управление вредоносным ПО, повышение привилегий, сокрытие действий, распространение доступа, сбор и вывод информации, целевое воздействие. Ее использование в методике необходимо, поскольку она позволяет структурировать описание инцидента и восстанавливать полную хронологию событий, планировать расследование в соответствии с этапами атаки, оценивать работу средств защиты информации и правил корреляции SIEM-систем, а также обеспечивать единообразие подхода при взаимодействии с регуляторами.

Таким образом, предложенная нами методика расследования компьютерных инцидентов основывается на требованиях нормативных правовых актов, национальных стандартов (в первую очередь ГОСТ Р 59709-2022) и методических документов ФСТЭК России, но главным в ней является использование специализированного отечественного программного обеспечения.

Список использованных источников:

1. ГОСТ Р 59709-2022 «Защита информации. Управление компьютерными инцидентами. Термины и определения» (Введен 01.02.2023) – URL: https://docs.cntd.ru/document/1200194355 (дата обращения: 24.03.2026). – Текст: электронный.

2. Шагапов, И. А. К вопросу построения системы защиты информации / И. А. Шагапов // 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. 51-54.

3. Киргизбаев, С. П. Применение SOAR-решений для автоматизации процессов выявления, анализа и реагирования на инциденты в корпоративной сети / С. П. Киргизбаев, В. П. Киргизбаев, А. А. Бутин // Информационные технологии и математическое моделирование в управлении сложными системами. – 2024. – № 3(23). – С. 29-44.

4. Дорофеев, А. В. Мониторинг событий информационной безопасности: технологии и методы контроля эффективности / А. В. Дорофеев, А. С. Марков // Вестник Военного инновационного технополиса "Эра". – 2022. – Т. 3, № 4. – С. 392-400. – DOI 10.56304/S2782375X22040052.

Fayzullina A.S.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Yapparov R.M.
Ufa university of science and technology, Ufa

INVESTIGATION OF COMPUTER INCIDENTS: APPROACHES, SOLUTIONS, AND PRACTICE

Abstract. This article analyzes the current methodology for investigating computer incidents, taking into account the requirements of Russian legislation and regulators. Special attention is paid to the stages of response and the use of domestic software. The necessity of using a unified threat taxonomy is substantiated. New approaches to solving the problem are proposed based on current practice.

Keywords: computer incident investigation, incident response, forensics, SIEM systems.

УДК 004.056.5

Чернов Р.А.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Салов И.В.
Уфимский университет науки и технологий, Уфа

ИСПОЛЬЗОВАНИЕ НОВЫХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ В РАБОТЕ С ПЕРСОНАЛОМ, ДОПУЩЕННЫМ К КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ: ОПЫТ ВНЕДРЕНИЯ ПК «СТАХАНОВЕЦ»

Аннотация. Рассматривается ПК «Стахановец» для контроля сотрудников с доступом к конфиденциальной информации. Описаны технические возможности: запись экрана, отслеживание съемных носителей, блокировка опасных действий, анализ аномалий. Без

закрепления мониторинга в трудовом договоре эффективность снижается. Предложен подход на основе профилактики, разделения персонала по группам риска и прозрачности. Смена карательной логики на профилактическую повышает защищенность информации и снижает сопротивление персонала.

Ключевые слова: защита информации, конфиденциальные данные, персонал, ПК «Стахановец», мониторинг, профилактика утечек, трудовой договор, группы риска, прозрачность.

Большинство утечек информации происходит по вине сотрудников. Человек может скопировать файл на флешку, отправить его в личный мессенджер или сфотографировать экран на телефон. Обычные DLP-системы и инструктажи такие случаи отслеживают не всегда. Для контроля за действиями людей, которые имеют доступ к конфиденциальной информации, были созданы специальные программы. Одна из них программный комплекс «Стахановец» (далее – ПК «Стахановец»). Он не просто записывает события, а может блокировать опасные действия в реальном времени. Однако одной установки программы недостаточно, нужны правильные настройки и юридическое оформление.

ПК «Стахановец» следит за действиями пользователя за компьютером. Система фиксирует подключение флешек и внешних дисков, копирование через буфер обмена, нажатия клавиш, запуск запрещенных программ, отправку файлов через мессенджеры и вывод документов на печать. Также ведется запись видео с экрана.

Программа работает в двух режимах. Первый режим запись всех действий для последующей проверки. Второй режим автоматическая блокировка подозрительных операций. Например, если сотрудник вставляет флешку и пытается скопировать на нее файл с пометкой «конфиденциально», система останавливает это действие до того, как данные будут записаны.

Система также выявляет аномальное поведение. Она замечает работу в нерабочее время (ночью или в выходные), массовое копирование большого количества файлов за короткое время, попытки доступа к папкам, к которым у сотрудника нет разрешения, а также запуск портабельных версий программ, которые могут использоваться для обхода контроля. При обнаружении таких аномалий система отправляет уведомление в службу безопасности.

ПК «Стахановец» отличается от классических DLP-систем тем [1], что ориентирован на человеческий фактор внутри периметра. DLP-системы в основном следят за тем, что уходит по сети: куда пересылаются файлы и какие письма отправляются. ПК «Стахановец»

делает другое, он следит за самим сотрудником за его компьютером, даже без интернета или при работе через VPN.

Без юридического закрепления в документах использовать ПК «Стахановец» нельзя. Программа фиксирует нажатия клавиш, записывает видео экрана, отслеживает буфер обмена и пересылку файлов. Это обработка данных, связанных как с частной жизнью сотрудника, так и его рабочими действиями. Если сотрудник не подписал письменное согласие, работодатель нарушает статью 23 Конституции Российской Федерации [2], а также Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» [3].

Статья 22 Трудового кодекса Российской Федерации дает работодателю право контролировать выполнение трудовых функций, но не определяет конкретные формы и методы этого контроля. Поэтому ключевое требование – зафиксировать согласие работника на мониторинг в письменной форме. Наиболее надежный способ: включить соответствующий пункт в трудовой договор или оформить отдельное дополнительное соглашение.

В договоре или соглашении должны быть четко перечислены контролируемые действия: запись экрана, фиксация нажатий клавиш, отслеживание подключения внешних носителей и анализ буфера обмена. Также необходимо указать цели мониторинга – защита конфиденциальной информации, предотвращение утечек и обеспечение производственной дисциплины. Также в договоре фиксируется обязанность работодателя не использовать данные мониторинга в целях, не предусмотренных договором, и ответственность работника за попытки обхода системы контроля или умышленное повреждение программного комплекса. Если какого-то из этих пунктов нет, сотрудник получает основание оспорить правомерность контроля.

Когда такие системы внедряют, обычно главной целью ставят найти нарушителя и наказать его. Это порождает у сотрудников страх и желание обойти контроль. Предлагается иной подход: использовать ПК «Стахановец» для профилактики нарушений.

Если система видит попытку скопировать конфиденциальный файл на флешку, она не просто блокирует действие, а выводит на экран краткое предупреждение: «Копирование на внешний носитель запрещено». Сотрудник видит, что нарушает правила, и сам останавливается. Ему не нужно придумывать способы обхода блокировки.

Еще один элемент подхода – это разделение сотрудников по степени риска. Новые сотрудники, которые работают меньше трех месяцев, попадают под полный мониторинг с блокировкой всех подозрительных действий. Такой подход помогает быстро заметить, как тех, кто еще не освоил правила, так и тех, кто их нарушает специально. Для опытных

сотрудников, которые раньше не попадались на нарушениях, достаточно простой записи действий без автоматической блокировки. При обнаружении аномалий приходит уведомление ответственному лицу. Сотрудники, которые уже попадались на нарушениях (даже случайных), получают усиленный контроль с блокировкой и обязательный ежемесячный разбор зафиксированных инцидентов.

Следующий элемент – интеграция с обучением персонала. Обезличенные данные о массовых однотипных нарушениях могут быть переданы в подразделение, отвечающее за обучение. Например, если система фиксирует, что несколько сотрудников регулярно пытаются отправить конфиденциальные файлы через незащищенный мессенджер, это сигнал не для наказания, а для проведения дополнительного инструктажа или корректировки внутренних реглапgmментов.

И последнее – прозрачность системы для сотрудников. Во внутренних документах имеет смысл закрепить за сотрудником право раз в квартал получать отчет о своих действиях, отслеженных ПК «Стахановец». Это повышает доверие к системе и заставляет самого сотрудника более ответственно относиться к своим действиям.

Предложенный в статье подход, включающий разделение сотрудников по группам риска, интеграцию с обучением и элементы прозрачности, позволяет превратить систему контроля из инструмента слежки в инструмент повышения ответственности.

Список использованных источников:

1. Программный комплекс «Стахановец»: описание функциональных возможностей [Электронный ресурс]. — URL: https://stakhanovets.ru/dlp/ (дата обращения: 07.04.2026).

2. Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ [Электронный ресурс]. — URL: https://www.consultant.ru/document/cons_doc_LAW_34683/ (дата обращения: 06.04.2026).

3. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» [Электронный ресурс]. — URL: https://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения: 11.04.2026).

Chernov R.A.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Salov I.V.
Ufa University of Science and Technology, Ufa

USE OF NEW INFORMATION PROTECTION MEANS IN WORK WITH PERSONNEL AUTHORIZED TO ACCESS CONFIDENTIAL INFORMATION: EXPERIENCE OF IMPLEMENTING THE STAKHANOVETS SOFTWARE

Abstract. The Stakhanovets software for controlling employees with access to confidential information is considered. Technical capabilities are described: screen recording, removable media tracking, dangerous actions blocking, anomaly analysis. Without monitoring formalization in the employment contract, effectiveness decreases. An approach based on prevention, personnel risk grouping and transparency is proposed. Replacing punitive logic with preventive one increases information security and reduces staff resistance.

Keywords: information security, confidential data, personnel, Stakhanovets, monitoring, leak prevention, employment contract, risk groups, transparency.

СЕКЦИЯ 4. КОНЦЕПЦИЯ И МЕТОДЫ ИНЖЕНЕРНО-ТЕХНИЧЕСКОГО ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

УДК 004.7

Вафин А.Р.
Уфимский университет науки и технологий, Уфа

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

ИНСТРУМЕНТЫ ЯЗЫКА ПРОГРАММИРОВАНИЯ PYTHON ДЛЯ АНАЛИЗА И МОДЕЛИРОВАНИЯ СЕТЕВЫХ ПРОЦЕССОВ

Аннотация. В статье исследуется и систематизируется набор библиотек языка Python для работы с сетевыми технологиями. Дана характеристика программных инструментов, а также пример использования для моделирования сетевых процессов и атак. Показано, как можно применить данные библиотеки на практике, в том числе в задачах информационной безопасности.

Ключевые слова: сетевые технологии, Python, Scapy, библиотека, сетевой трафик, DDoS-атака

Исследования в области сетевых технологий являются актуальными на сегодня по многим причинам. Среди них можно выделить выявление оптимальных путей решения логистических трудностей, выявление уязвимых мест информационной безопасности и т.д. Все это направлено на улучшение технологий, вследствие чего можно получить многие выгоды, такие, например, как уменьшение затрат на передачу и соответственно понизить риски от хакерских атак.

В работе рассмотрены инструменты для анализа, моделирования, а также автоматизации сетевых процессов, такие как библиотеки высокоуровневого языка программирования Python. Выбор пал именно на этот язык, так как он является весьма простым и гибким, и одно из его прямых назначений – написание скриптов для автоматизации и анализа различных процессов. А именно: Scapy, NetworkX и NFStream. Предметом исследования выступят функциональные возможности этих библиотек, а также их сравнительный анализ. Главной целью работы будет выявление оптимальных задач для каждого инструмента в работе с компьютерными сетями.

При передаче по сети информация проходит множество узлов, и на каждом этапе может возникнуть угроза безопасности: от перехвата

пакетов до внедрения вредоносного кода. Сетевой трафик представляет собой совокупность пакетов данных, передаваемых по сети. Каждый пакет содержит служебную информацию (заголовки протоколов) и полезную нагрузку (данные).

Scapy – это библиотека Python для низкоуровневой работы с сетевыми пакетами [1]. В отличие от традиционных инструментов вроде Wireshark, Scapy ориентирована на автоматизацию: она позволяет не только перехватывать и анализировать трафик в реальном времени, но и создавать, модифицировать и отправлять любые пакеты (Ethernet, IP, TCP, UDP и др.). Ее главное преимущество – возможность гибкой фильтрации и встраивания анализа в собственные программы, что делает Scapy незаменимым для тестирования сетей и протоколов [2].

NFStream – это фреймворк (используемый как библиотека) для потокового анализа сетевых данных. В отличие от Scapy, он не обрабатывает каждый пакет по отдельности, а группирует их в потоки (flows), что позволяет эффективно работать с большими объемами трафика. NFStream поддерживает чтение pcap-файлов, live-захват, экспорт статистик и расширение через плагины, что делает его удобным инструментом для мониторинга и исследований в области сетевой аналитики [3].

NetworkX – это библиотека для моделирования сетевых топологий на основе теории графов [4]. Она позволяет создавать различные типы графов (звезда, кольцо, случайные сети), задавать атрибуты узлам и ребрам, а также применять встроенные алгоритмы анализа – расчет центральностей, кластеризации, поиск кратчайших путей. Интеграция с Matplotlib дает возможность визуализировать структуру сети, что особенно полезно при проектировании и исследовании сетевых архитектур [5].

Рассмотрим на примере работы каждую из выбранных библиотек.

Для наглядности смоделируем SYN-флуд атаку, при котором злоумышленник отправляет большое количество TCP-пакетов с флагом SYN на целевой сервер, но не завершает рукопожатие (не отправляет ACK). Это истощает ресурсы сервера, так как он вынужден держать открытыми соединения.

Создадим скрипт для генерации пакетов для атаки и дальнейшего ее анализа. При помощи двух циклов for сгенерируем 250 пакетов для нашего эксперимента (см.рис.1).

```
packets = []
for i in range(100):
    packets.append(IP(src="10.0.0.1", dst="192.168.1.100") / TCP(sport=10000 + i, dport=80, flags="S"))
for i in range(150):
    packets.append(IP(src="10.0.0.2", dst="192.168.1.100") / TCP(sport=20000 + i, dport=80, flags="S"))
wrpcap( filename: "attack.pcap", packets)
print(f"Создано {len(packets)} пакетов в attack.pcap\n")
```

Рис. 1. Генерация SYN-пакетов

На рис. 2 показан процесс считывания и группировки пакетов по отправителям. Флаг 0x02 – это двоичное 00000010, что соответствует SYN-флагу в TCP-заголовке.

```
pcap = rdpcap("attack.pcap")
attack_counts = defaultdict(int)
for pkt in pcap:
    if IP in pkt and TCP in pkt and pkt[TCP].flags == 0x02:
        attack_counts[pkt[IP].src] += 1
```

Рис. 2. Распределение пакетов по отправителям

На рис. 3 показано, что NFStream позволяет заниматься задачей распределения пакетов по 5 ключам – src_ip, dst_ip, src_port, dst_port, protocol.

```
streamer = NFStreamer(source="attack.pcap")
for flow in streamer:
    print(f"{flow.src_ip}:{flow.src_port} → {flow.dst_ip}:{flow.dst_port}")
    print(f"  Пакетов: {flow.bidirectional_packets}, Байт: {flow.bidirectional_bytes}\n")
```

Рис. 3. Группировка пакетов при помощи методов NFStream

Во втором скрипте создана визуальная модель процесса атаки. В собираны потоки и ориентированный граф. Также при помощи методов библиотеки matplotlib вывели рисунок на экран. Программный код конфигурации графа представлен на рис. 4.

```
flows = list(NFStreamer(source="attack.pcap"))
G = nx.DiGraph()
for flow in flows:
    G.add_node(flow.src_ip, role='attacker')
    G.add_node(flow.dst_ip, role='target')
    G.add_edge(flow.src_ip, flow.dst_ip, weight=flow.bidirectional_packets)
pos = nx.spring_layout(G, seed=42, k=0.3)
colors = ['red' if G.nodes[n].get('role') == 'attacker' else 'blue' for n in G.nodes]
plt.figure(figsize=(8, 5))
nx.draw(G, pos, node_color=colors, with_labels=True, node_size=800,
        arrows=True, arrowstyle='->', arrowsize=15)
plt.title("Граф SYN-флуд атаки (красный → синий)")
plt.show()
```

Рис. 4. Реализация графа атаки при помощи методов библиотеки Networkx

На рис.5 представлен ориентированный граф их трех вершин – визуальное представление атаки, где по стандарту красная вершина олицетворяет атакующую сторону, синяя – оборону.

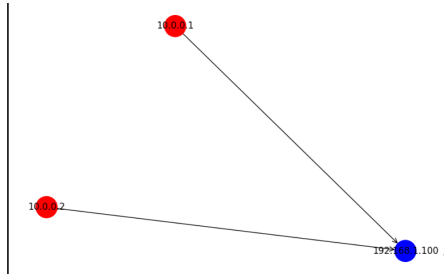


Рис. 5. Граф DDoS-атаки

Подводя итоги, можно заключить, что Scapy используется для генерации множества пакетов сетевой атаки, а используя методы NFStream проводится потоковый анализ и сгруппированы пакеты. Также на основе полученных данных граф.

Подключая библиотеки по отдельности, нельзя написать программу, которая унифицирует все использованные и не только пакеты в этой работе. Каждый инструмент выполняет свою часть работы, и они взаимно дополняют друг друга, поэтому необходимо обладать знаниями в каждой из библиотек, чтобы успешно выполнять подобные задачи. Это особенно актуально для задач информационной безопасности, где важен образ инцидента с разных уровней и ракурсов.

Список использованных источников:

1. Бражук А. Основы конструирования сетевых пакетов. // Системный администратор. 2011. № 10. С. 66-69.

2. Scapy documentation. // Scapy. URL: https://scapy.readthedocs.io.

3. NFStream documentation. // NFStream. URL: https://www.nfstream.org.

5. Русаков А. М., Юшкова Н. А., Селиванова Е. А. Современные средства визуализации графов и графовых моделей для Python. //Наукосфера. №11-2. 2022. С. 258-267.

6. NetworkX documentation. // NetworkX. URL: https://networkx.org.

Vafin A.R.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Fatkhelislamov A.F.
Ufa University of Science and Technology, Ufa

PYTHON PROGRAMMING LANGUAGE TOOLS FOR ANALYSIS AND MODELING OF NETWORK PROCESSES

Abstract. The article examines and systematizes a set of Python libraries for working with network technologies. It provides a description of software tools, as well as an example of using them for modeling network processes and attacks. It demonstrates how these libraries can be applied in practice, including in information security tasks.

Keywords: network technologies, Python, Scapy, library, network traffic, DDoS attack

УДК 004.451.042.3

Гизатова Е.А.
Уфимский университет науки и технологии, Уфа

Научный руководитель:
Исмагилова А.С.
Уфимский университет науки и технологии, Уфа

ПОДХОД К ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ВИРТУАЛИЗИРОВАННЫХ АРМ НА БАЗЕ РЕД ОС

Аннотация. В статье представлена разработка защищенного АРМ специалиста техподдержки на основе РЕД ОС в среде VMware Workstation. Обоснована реализация мер защиты штатными средствами гостевой ОС (SELinux, sudo, fapolicyd, firewalld, auditd) в условиях недоверенного гипервизора второго типа. Экспериментально подтверждено соответствие настроек требованиям ФСТЭК и их работоспособность.

Ключевые слова: РЕД ОС, VMware Workstation, защищенное АРМ, мандатный контроль доступа, sudo, fapolicyd, firewalld, импортозамещение, ФСТЭК.

Согласно политики импортозамещения и Указа Президента РФ №166 особое внимание уделяется внедрению отечественных ОС в государственные информационные инфраструктуры [1]. Лидирующие позиции занимает РЕД ОС – сертифицированная ФСТЭК России ОС на базе ядра Linux.

Наиболее безопасным способом изучения новой ОС без вмешательства в основную рабочую среду является виртуализация. Поэтому построение защищенного автоматизированного рабочего места (АРМ) специалиста технической поддержки будет осуществляться именно в среде виртуализации. Цель работы – разработка защищенной конфигурации АРМ специалиста технической поддержки на основе ОС РЕД ОС и экспериментальная проверка ее работоспособности в виртуальной среде.

В качестве среды исполнения был выбран гипервизор 2 типа – VMware Workstation, что расширяет доверенную вычислительную базу за счет хостовой ОС и самого гипервизора. Компрометация хост-системы грозит нарушением конфиденциальности и целостности гостевой ОС, использование общих буфера обмена и папок повышает риски. Все это требует дополнительной защиты внутри гостевой ОС, в отличие от автономных гипервизоров 1 типа, например, KVM/QEMU, где поверхность атаки хостовой компоненты минимизирована.

Сертификация ФСТЭК для виртуализированных сред 2 типа затруднена ввиду отсутствия у хостовой ОС достаточного класса защиты, однако в рамках лабораторного анализа VMware Workstation позволяет апробировать логику защиты, компенсируя отсутствие сертификации максимальным уровнем защиты внутри самой гостевой ОС. Именно поэтому все ключевые рубежи обороны спроектированы и реализованы исключительно штатными средствами гостевой ОС – без расчета на изолирующие свойства гипервизора. Каждая мера защиты была отображена на требования нормативной базы [2-4], что позволило оценить достаточность встроенных механизмов ОС для выполнения регуляторных предписаний даже в недоверенной среде исполнения. Результаты этого сопоставления систематизированы в таблице 1.

Таблица 1

Отображение мер защиты и их соответствие требованиям регуляторов

Мера защиты	Назначение	Соответствие НПА / ГОСТ Р
SELinux (Enforcing)	Принудительный контроль доступа (MAC)	ФСТЭК №21 (УПД.3), №239 (УЗ.2), ГОСТ Р 57580.1 (МДЗ-3)
Политика sudo (ограниченная)	Разграничение прав и минимизация привилегий	ФСТЭК №117 (УПД.1), №21 (УПД.2), ГОСТ Р 57580.1 (МДЗ-4)
fapolicyd (белый список)	Контроль запуска исполняемых файлов, целостность ПО	ФСТЭК №239 (ЦЛД.1, УЗ.3), №21 (ЗИС.3)
Парольная политика (pwquality)	Усиление аутентификации	ФСТЭК №21 (ИАФ.1), №239 (ИАФ.2)
firewalld (default deny)	Межсетевое экранирование и зонирование	ФСТЭК №21 (ЗИС.9), №239 (УПД.4)
Журналирование и запрет оболочки	Регистрация событий, блокировка повышения привилегий	ФСТЭК №21 (РЕГ.3), №239 (УЗ.4)

Анализируя таблицу 1, можно увидеть, что штатные средства защиты РЕД ОС обеспечивают закрытие всего спектра базовых требований к защите ГИС [3].

Для проверки применимости упомянутых выше нормативных требований на практике была установлена и настроена, согласно выбранному сценарию, операционная система РЕД ОС в среде VMware Workstation с созданием двух учетных записей: redos (администратор) и support (специалист техподдержки).

Настройка защиты велась поуровнево. На уровне аутентификации через libpwquality заданы требования к сложности паролей (minlen=8, minclass=3, maxrepeat=2, difok=3), а в /etc/login.defs – срок действия 30 дней и предупреждение за 7 дней. Запрет повторного использования пяти паролей обеспечен параметром remember=5 в PAM.

Разграничение доступа реализовано файлом /etc/sudoers.d/support с псевдонимами: SUPPORT_NET, SUPPORT_LOG, SUPPORT_SYS (разрешенные утилиты) и SUPPORT_SHELL (запрещенные bash, su, passwd). SELinux оставлен в режиме Enforcing без дополнительной корректировки политик. Контроль целостности ПО обеспечил fapolicyd с правилом запуска только из /usr/bin и /usr/lib64. Межсетевое экранирование настроено через firewalld (зона public, открыт только порт 5900/TCP для VNC). Аудит выполнялся подсистемой auditd с отслеживанием всех sudo-вызовов пользователя support [3].

Опора исключительно на механизмы защиты, встроенные в гостевую ОС, требуют выстраивания многоуровневой архитектуры, каждый элемент которой будет решать лишь свою определенную задачу, а их совокупность будет выстраивать эшелонированный рубеж обороны.

Логику построения такой архитектуры можно отразить на следующей схеме (рисунок 1):



Рис. 1. Схема выстраивания логики многоуровневой архитектуры

Для оценки эффективности выстроенной многоуровневой архитектуры было проведено тестирование каждого рубежа обороны в отдельности и их взаимодействия.

На уровне аутентификации попытка задания пользователем support пароля «123» была отклонена модулем pwquality с диагностикой недостаточной сложности – система потребовала наличия символов как минимум трех классов.

На уровне контроля целостности ПО fapolicyd заблокировал попытку запуска тестового скрипта из домашней директории пользователя, зафиксировав событие в журнале аудита. Таким образом, правило белого списка отработало штатно, обеспечивая контроль целостности ПО [2].

На уровне разграничения привилегий пользователь support успешно выполнил разрешенные диагностические команды: sudo ping 127.0.0.1, sudo journalctl --lines=10. Попытка же запуска командной оболочки sudo bash была отклонена. Это подтвердило, что псевдоним SUPPORT_SHELL с запрещающими правилами эффективно блокирует наиболее очевидный вектор повышения привилегий [3].

На сетевом уровне сканирование гостевой ОС с соседнего хоста показало, что порт 5900/TCP (VNC) доступен для администратора, в то время как все остальные порты отфильтрованы политикой зоны public межсетевого экрана firewalld. Принцип «запрещено все, что не разрешено явно» реализован в полном объеме. Наконец, подсистема аудита auditd зафиксировала все перечисленные события – как успешные, так и отклоненные попытки выполнения команд – в журнале.

Таким образом, проведенная верификация подтвердила корректность всех примененных настроек защиты и их согласованность как единого комплекса мер, перекрывающего все основные тактики

потенциального нарушителя. Практическая значимость работы состоит в том, что разработанная конфигурация может служить типовым профилем защиты для тиражирования АРМ специалистов техподдержки в государственных учреждениях. Показано, что даже в среде гипервизора типа 2 штатные механизмы РЕД ОС обеспечивают уровень защищенности, достаточный для обработки конфиденциальной информации.

Список использованных источников:

1. Указ Президента РФ от 30.03.2022 № 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации» – URL: http://www.consultant.ru/document/cons_doc_LAW_297432 (дата обращения 15.04.2026). – Текст: электронный.

2. Информационное сообщение ФСТЭК России от 18 октября 2016 г. N 240/24/4893 «Об утверждении Требований безопасности информации к операционным системам» – URL: https://base.garant.ru/71709444/ (дата обращения 15.04.2026). – Текст: электронный.

3. Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» – URL: https://www.consultant.ru/document/cons_doc_LAW_147084 (дата обращения 15.04.2026). – Текст: электронный.

4. ГОСТ Р 57580.1-2017 «Защита информации. Безопасность финансовых (банковских) операций. Защита информации организаций банковской системы Российской Федерации. Базовый состав организационных и технических мер» URL: https://docs.cntd.ru/document/1200146534 (дата обращения 15.04.2026). – Текст: электронный.

Gizatova E.A.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Ismagilova A.S.
Ufa University of Science and Technology, Ufa

AN APPROACH TO ENSURING INFORMATION SECURITY OF VIRTUALIZED WORKSTATIONS BASED ON RED OS

Abstract. The article presents the development of a secure workstation for a technical support specialist based on RED OS in a VMware Workstation

environment. The implementation of security measures using native tools of the guest OS (SELinux, sudo, fapolicyd, firewalld, auditd) in an untrusted Type 2 hypervisor environment is substantiated. The compliance of the settings with the requirements of the Federal Service for Technical and Export Control (FSTEC) and their operability are experimentally confirmed.

Keywords: RED OS, VMware Workstation, secure automated workstation, mandatory access control, sudo, fapolicyd, firewalld, import substitution, FSTEC

УДК 004.056:351.78:621.39

Джабаров А.М.
Северный (Арктический) Федеральный Университет, Архангельск

Научный руководитель:
Зубарев А.А.
Северный (Арктический) Федеральный Университет, Архангельск

СОВРЕМЕННЫЕ МЕТОДЫ ЗАЩИТЫ КОНТРОЛИРУЕМЫХ ЗОН

Аннотация. Статья рассматривает проблемы обеспечения безопасности контролируемых зон производственных объектов, анализирует современные угрозы и ограничения традиционных методов охраны и обосновывает необходимость применения радиочастотного мониторинга как средства непрерывного контроля перемещений внутри территории.

Ключевые слова: контролируемая зона, физическая безопасность, радиочастотный мониторинг, несанкционированный доступ, промышленные объекты.

Усложнение структуры современных угроз, направленных на критически важные объекты производства, приводит к необходимости пересмотра подходов к организации физической защиты. Традиционные системы, основанные на контроле периметра и работе контрольно-пропускных пунктов, демонстрируют значимые ограничения при использовании на протяженных территориях, таких как карьеры, порты, промышленные и энергетические комплексы. Между «узловыми» точками контроля формируются обширные пространства, где активность персонала, посетителей и потенциальных нарушителей остается неконтролируемой.

Одновременно снижается эффективность систем видеонаблюдения: значительные капитальные затраты, сложность инфраструктуры, необходимость обслуживания и высокая нагрузка на операторов

ограничивают их практическую применимость на масштабных территориях.

Таким образом, возникает объективная потребность в переходе от дискретного контроля к методам непрерывного мониторинга территории. Одним из таких методов является использование радиочастотных технологий, позволяющих фиксировать перемещение источников радиоизлучения внутри контролируемой зоны.

Рассмотрим понятие, структуру и принципы защиты контролируемой зоны.

Контролируемая зона (далее – КЗ) – это пространство, доступ в которое ограничен и регламентирован, а нахождение в нем сотрудников, посетителей, транспортных и иных средств подлежит контролю.

Ключевые признаки КЗ включают наличие физически определенного периметра, организацию пропускного режима и применение технических средств охраны: видеонаблюдения, СКУД, датчиков движения, систем обнаружения вторжений (Российская Федерация. ФСТЭК России. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, 2008).

КЗ подразделяется на несколько уровней:

- неконтролируемая зона – общедоступная зона за пределами объекта. Например: прилегающая территория;
- зона общего назначения – территория внутри основного периметра объекта, доступная для большей части персонала. Например: проходные, холлы, столовые, административные коридоры;
- буферная зона (или – зона ограниченного доступа) – промежуточная зона между общей зоной и зоной особого внимания. Служит для задержки и обнаружения нарушителя. Например: производственные цеха, склады, инженерные коридоры);
- зона особого внимания – зона с максимальным уровнем защиты, где расположены ключевые активы. Доступ строго ограничен. Например: серверные, лаборатории, зоны с дорогостоящим уникальным оборудованием, комната безопасности.

Многозональность и эшелонированность являются фундаментальными принципами физической защиты. Однако эффективность системы определяется не только количеством уровней безопасности, но и полнотой контроля внутри каждой зоны.

Практика показывает, что значительная часть инцидентов безопасности реализуется вследствие получения физического несанкционированного доступа, в том числе инсайдерским путем.

Примеры:

- случай заражения инфосистем Минобороны США посредством USB-накопителя, что привело к компрометации аутентификационных токенов;
- утечка коммерческой тайны DuPont сотрудником-химиком с использованием личных устройств хранения данных;
- многочисленные случаи проникновения «сталкеров» на промышленные объекты.

Статистика подтверждает тенденцию: рост числа атак на критическую инфраструктуру сопровождается увеличением числа инцидентов, связанных с физическим проникновением. Одновременно по данным РБК более 50 % преступлений, совершенных в организациях, приходится на хищения имущества сотрудниками. Таким образом, объектом угрозы являются не только информационные ресурсы, но и материальные активы предприятия, что требует повышения полноты контроля персонала и посетителей на территории КЗ (РБК, 2025).

На промышленных объектах значительная часть контроля реализуется через контрольно-пропускной пункт (далее – КПП). Однако КПП обеспечивает только «точечный» контроль на входе и выходе, а все дальнейшее перемещение сотрудников по территории объекта зачастую остается непрозрачным.

На больших территориях проблема усугубляется: длина периметра исчисляется километрами, а обнаружение и устранение нарушений целостности ограждений требует значительного времени.

Системы видеомониторинга также имеют фундаментальные ограничения:

- высокая капиталоемкость, особенно при сложном рельефе;
- необходимость размещения точек питания и коммуникаций;
- ограниченная пропускная способность операторов (например, по европейскому стандарту EN50132-2-1 рекомендуется не более 16 камер на человека);
- высокая зависимость эффективности от человеческого фактора (ЧОП «Taggerd group», 2025; Solitaired, 2025).

Таким образом, даже при масштабной установке видеокамер невозможно обеспечить полноту контроля, сопоставимую с внутренней динамикой КЗ.

В условиях цифровизации большинство людей, включая сотрудников, посетителей и потенциальных нарушителей постоянно имеют при себе источники радиоизлучения: мобильные телефоны, рации, персональные трекеры, устройства Wi-Fi, Bluetooth, а также радиооборудование, применяемое при попытке обхода системы безопасности.

По данным исследований, до 82 % пользователей не готовы расставаться со смартфоном даже на несколько часов. Это позволяет сделать вывод: в подавляющем большинстве случаев физическое перемещение внутри КЗ сопровождается неизбежным радиоизлучением (СенатИнформ, 2025).

Радиоэфир – сложная среда, содержащая совокупность сигналов различных частот. Анализ присутствия, параметров и динамики этих сигналов способен дать ценные данные о перемещении объектов даже в условиях полного отсутствия визуального покрытия.

Следовательно, контроль радиоэфира становится логически обоснованным способом расширения возможностей традиционных систем физической защиты.

Таким образом, проведенный анализ позволяет утверждать, что существующие методы защиты КЗ недостаточны для обеспечения полноценного мониторинга обширных территорий. Наличие широкого спектра радиоустройств у персонала и нарушителей открывает возможность применения радиочастотных способов слежения за активностью внутри КЗ.

Внедрение систем пеленгации источников радиоизлучения представляется перспективным направлением развития комплексных систем безопасности и служит основой для перехода от дискретного к непрерывному контролю всей территории.

Список использованных источников:

1. Российская Федерация. ФСТЭК России. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных [Электронный ресурс]: метод. док.: от 15.02.2008. – Электрон. дан. – URL: http://pravo.gov.ru/ (дата обращения: 02.10.2025). – Загл. с экрана.

2. РБК [Электронный ресурс]: [офиц. сайт] / РБК. – Электрон. дан. – [Москва]: РБК, 2025. – Режим доступа: https://companies.rbc.ru/, свободный (дата обращения: 20.10.2025). – Загл. с экрана.

3. СенатИнформ [Электронный ресурс]: [офиц. сайт] / СенатИнформ. – Электрон. дан. – [Москва]: СенатИнформ, 2025. – Режим доступа: https://senatinform.ru/, свободный (дата обращения: 20.10.2025). – Загл. с экрана.

4. ЧОП «Taggerd group» [Электронный ресурс]: [офиц. сайт] / ЧОП «Taggerd group» – Электрон. дан. – [Москва]: ЧОП «Taggerd group», 2025. – Режим доступа: https://www.taggerd.su/, свободный (дата обращения: 20.10.2025). – Загл. с экрана.

5. Solitaired [Электронный ресурс]: [офиц. сайт] / Solitaired – Электрон. дан. – [Майами-Бич]: Solitaired, 2025. – Режим доступа:

https://solitaired.com/, свободный (дата обращения: 02.10.2025). – Загл. с экрана.

Dzhabarov A.M.
Northern (Arctic) Federal University, Arkhangelsk

Scientific supervisor:
Zybarev A.A.
Northern (Arctic) Federal University, Arkhangelsk

MODERN METHODS FOR PROTECTING CONTROLLED AREAS

Abstract. The article examines the challenges of ensuring the security of controlled areas at industrial facilities, analyzes modern threats and the limitations of traditional protection methods, and substantiates the need to use radio frequency monitoring as a means of continuous tracking of movements within the territory.

Keywords: controlled area; physical security; radio frequency monitoring; unauthorized access; industrial facilities.

УДК 004.056

Ермолаева А.В.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Яппаров Р.М.
Уфимский университет науки и технологий, Уфа

КОНЦЕПТУАЛЬНЫЙ ПОДХОД К СИСТЕМЕ ЗАЩИТЫ ИНФОРМАЦИИ ЦИФРОВЫХ СЕРВИСОВ

Аннотация. В статье анализируются вызовы и угрозы информационной безопасности цифровых сервисов. Отмечен недостаток существующих подходов – их реактивный характер. Предложен переход к проактивной защите с использованием Big Data, ML и UEBA. Описана архитектура системы, ее компоненты и принципы взаимодействия. Внедрение интеллектуального мониторинга и прогнозирования угроз повышает защищенность, ускоряет обнаружение инцидентов и снижает риски потерь.

Ключевые слова: информационная безопасность, цифровые сервисы, защита информации, поведенческая аналитика, машинное обучение, проактивная защита, система мониторинга.

Цифровая трансформация экономики и социальной сферы привела к повсеместному внедрению онлайн-сервисов в банковскую сферу, электронную коммерцию, государственное управление и медицину. Цифровые сервисы оперируют огромными массивами конфиденциальной информации (персональные данные, финансовая информация, коммерческая тайна), что делает их приоритетной целью для киберпреступников. Согласно отчетам ведущих аналитических агентств, количество и сложность кибератак ежегодно растет в геометрической прогрессии.

Традиционные системы защиты информации (далее - СЗИ), основанные на сигнатурном анализе и использовании статических правил (например, классические межсетевые экраны и системы обнаружения вторжений IDS), демонстрируют низкую эффективность против современных угроз [2]. К таким угрозам относятся атаки «нулевого дня» (Zero-day), сложные целевые атаки (APT), а также инсайдерские угрозы. Основная проблема заключается в реактивном характере этих систем: они срабатывают по факту совершения или обнаружения инцидента, когда ущерб уже нанесен или находится в процессе нанесения. В данной работе мы попытаемся определить концептуальные подходы в разработке модели совершенствования СЗИ используя проактивные методы обнаружения и предотвращения угроз.

В этой связи возникает научная и практическая проблема: как обеспечить адекватный уровень защиты цифровых сервисов в условиях динамично меняющегося ландшафта угроз.

Анализ существующих подходов по защите цифровых сервисов показывает, что современный рынок предлагает широкий спектр решений, которые можно классифицировать по нескольким уровням [3]:

1. Сетевой уровень: Межсетевые экраны нового поколения (NGFW), системы предотвращения вторжений (IPS). Их основная задача – фильтрация трафика на основе IP-адресов, портов и известных сигнатур атак.

2. Уровень конечных точек (Endpoint): Антивирусное ПО, системы класса Endpoint Detection and Response (EDR). Обеспечивают защиту рабочих станций и серверов от вредоносного ПО.

3. Уровень приложений: Web Application Firewall (WAF) для защиты веб-приложений от специфических атак (SQL-инъекции, XSS).

Несмотря на свою функциональность, эти уровни имеют общие фундаментальные недостатки [4]:

1. Эффективность напрямую зависит от оперативности выпуска сигнатур производителем программного обеспечения. Атаки «нулевого дня» проходят незамеченными.

2. Статические правила часто блокируют легитимную активность пользователей, что создает нагрузку на администраторов безопасности.

3. Традиционные СЗИ не способны отличить действия легитимного пользователя от действий злоумышленника, который уже получил доступ к системе под чужими учетными данными.

Следовательно, для совершенствования СЗИ цифровых сервисов необходимо внедрение таких систем, которые способны анализировать контекст событий в реальном времени и выявлять аномалии, не опираясь на заранее известные шаблоны атак [5].

Для решения этой задачи мы предлагаем взять за основу концепцию проактивной системы защиты на основе поведенческой аналитики. Так, анализ архитектуры интеллектуальной системы проактивной защиты информации показывает, что ключевой идеей является переход от поиска «плохого» к поиску «необычного», система должна строить динамические профили нормального поведения пользователей, приложений и сетевых узлов (так называемые «белые списки» или baseline) и выявлять любые отклонения от них.

Основу предлагаемой нами проактивной системы защиты на основе поведенческой аналитики составляют следующие компоненты:

1. Единый центр сбора и нормализации данных (SIEM-ядро) осуществляет централизованный сбор логов со всех элементов инфраструктуры: сетевого оборудования, серверов, баз данных, приложений и средств защиты. Данные приводятся к единому формату для последующей обработки.

2. Модуль поведенческого анализа (UEBA-ядро) использует алгоритмы машинного обучения (в частности, методы кластеризации и классификации) для анализа поступающих данных.

Для каждого субъекта (пользователь) и объекта (сервер) система создает математическую модель его типичного поведения: время входа в систему, используемые IP-адреса, объем передаваемых данных, типичные запросы к БД. Любое действие, статистически нехарактерное для данного профиля (например, вход бухгалтера в систему в 3 часа ночи из другой страны или резкое увеличение объема выгрузки данных с сервера разработки), классифицируется как аномалия с присвоением соответствующего уровня риска.

3. Модуль корреляции и реагирования. На основе данных от UEBA-модуля система автоматически генерирует инциденты безопасности. При достижении критического порога риска система может выполнять автоматические действия по реагированию: блокировка учетной записи, изоляция узла из сети VLAN, отправка уведомления в SOC (Security Operations Center).

Таким образом, внедрение описанной системы позволит достичь следующих преимуществ по сравнению с классическими реактивными СЗИ:

1. Проактивное обнаружение угроз: система способна выявлять атаки «нулевого дня» и действия инсайдеров на ранних стадиях (разведка, горизонтальное перемещение), еще до достижения злоумышленником своей цели.

2. Снижение нагрузки на персонал: автоматизация анализа событий и корреляции инцидентов позволяет специалистам по безопасности сосредоточиться на расследовании действительно критичных событий, а не на рутинном просмотре логов.

3. Адаптивность: система самообучается в процессе работы. При изменении бизнес-процессов или инфраструктуры она автоматически корректирует базовые профили поведения без необходимости ручного перенастраивания сотен правил.

4. Снижение ущерба: сокращение времени обнаружения инцидента (MTTD – Mean Time To Detect) с дней/недель до минут/часов напрямую ведет к минимизации финансового и репутационного ущерба для цифрового сервиса.

Мы знаем, что эволюция киберугроз требует качественного изменения подходов к построению систем защиты информации. Переход от реактивных сигнатурных методов к проактивным интеллектуальным системам на базе поведенческой аналитики является неизбежным этапом развития информационной безопасности современных цифровых сервисов. Предложенная нами концептуальная модель позволяет не просто реагировать на инциденты, а прогнозировать их возникновение и предотвращать их на самых ранних этапах. Дальнейшие исследования в данной области могут быть направлены на оптимизацию алгоритмов машинного обучения для снижения числа ложных срабатываний и интеграцию данной системы с технологиями Threat Intelligence (киберразведка, разведка угроз) для обогащения данными о глобальных угрозах.

Список использованных источников:

1. CODE RED 2026: Актуальные киберугрозы для российских организаций. – URL: https://ptsecurity.com/research/analytics/russia-cyberthreat-landscape-2026/ (дата обращения: 02.04.2026).

2. ГОСТ Р ИСО/МЭК 27001-2021. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. – М.: Стандартинформ, 2021.

3. Сидоров С.С. Современные угрозы информационной безопасности // Информационная безопасность регионов. – 2024. – № 2(37). – С. 45-50.

4. Шагапов И.А. К вопросу построения системы защиты информации / И.А. Шагапов // 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. 51-54.

5. Андреев М. Ф. Анализ возможностей фильтрации трафика на межсетевом экране xFirewall / М.Ф. Андреев, А.С. Исмагилова // Инженерный вестник Дона. – 2025. – № 7(127). – С. 421-432.

Ermolaeva A.V.
Ufa university of science and technology, Ufa

Scientific supervisor:
Yapparov R.M.
Ufa university of science and technology, Ufa

A CONCEPTUAL APPROACH TO THE INFORMATION PROTECTION SYSTEM OF DIGITAL SERVICES

Abstract. The article analyzes the challenges and threats to information security of digital services. The drawback of existing approaches — their reactive nature — is highlighted. A transition to proactive protection using Big Data, ML, and UEBA is proposed. The system architecture, its components, and interaction principles are described. The implementation of intelligent monitoring and threat forecasting enhances security, speeds up incident detection, and reduces the risk of losses.

Keywords: information security, digital services, information protection, behavioral analytics, machine learning, proactive protection, monitoring system.

УДК 004

Ефимова С.В.
Уфимский университет науки и технологий, Уфа

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

АНАЛИЗ УТЕЧЕК DNS и WEBRTC в VPN-СЕРВЕРЕ НА ОСНОВЕ ТРАССИРОВКИ СЕТЕВЫХ ПАКЕТОВ В WIRESHARK

Аннотация. В данной работе представлены результаты экспериментального анализа утечек DNS и WebRTC в VPN-соединениях. С использованием трассировки сетевых пакетов в Wireshark был исследован трафик, проходящий в обход активного VPN-туннеля. В ходе анализа были обнаружены утечки: системные обходы VPN и STUN Binding Requests на STUN-серверы. Последние приводят к раскрытию реального публичного IP-адреса пользователя. Также была разработана система фильтров для выявления и классификации утечек и были предложены практические рекомендации по уменьшению рисков.

Ключевые слова: VPN, DNS-утечка, WebRTC-утечка, STUN, Wireshark, анализ трафика.

Современные VPN-сервисы позиционируются как надежное средство обеспечения безопасности передачи данных, тем не менее исследования и практические эксперименты показывают, что наличие VPN-соединения не гарантирует защиты от утечек конфиденциальных данных. Наиболее распространенными векторами утечек являются DNS-запросы, отправляемые в обход туннеля, и технология WebRTC, раскрывающая реальный IP-адрес устройства через механизмы STUN и ICE. Целью данной работы является экспериментальный анализ утечек DNS и WebRTC на примере конкретного VPN-сервера с применением трассировки сетевых пакетов в Wireshark.

Для правильного понимания сути данной статьи важно отметить, что в соответствии с ФЗ от 29.07.2017 N 276-ФЗ использование VPN для доступа к заблокированным ресурсам на территории РФ строго запрещено. Согласно этому закону владельцы VPN-сервисов обязаны сотрудничать с властями путем ограничения доступа к запрещенным на территории России ресурсам. В противном случае подобным сервисам грозит блокировка. Однако само существование VPN не запрещается. В соответствии с постановлением правительства №1279, запрещается

только доступ к заблокированным Роскомнадзором сайтам с помощью VPN в том числе [4].

Известно, что DNS-утечка – это нарушение конфиденциальности при использовании VPN, при котором DNS-запросы устройства направляются на DNS-сервер интернет-провайдера или другой недоверенный сервер, вместо того чтобы передаваться через зашифрованный VPN-туннель. В результате провайдер или владельцы DNS-серверов могут видеть реальный IP-адрес пользователя, его историю просмотров и посещаемые сайты. Утечка происходит, когда операционная система или приложение отправляют DNS-запрос напрямую через физический сетевой интерфейс [1-2].

WebRTC-утечка – это уязвимость на уровне браузера, возникающая при использовании технологии WebRTC, которая позволяет веб-сайту или злоумышленнику получить реальный публичный IP-адрес устройства пользователя, даже при активном VPN-соединении. Для согласования параметров соединения браузер формирует STUN-запросы, которые, в отличие от основного трафика, часто отправляются в обход VPN-туннеля. Получив ответ от STUN-сервера, JavaScript-код на веб-странице может извлечь реальный IP-адрес [2-3].

Исследовательская часть работы заключается в том, чтобы подключить VPN и осуществить захват трафика в Wireshark. Захват производится на физическом сетевом интерфейсе (Wi-Fi), через который устройство имеет выход в интернет, так как захват на виртуальном VPN-интерфейсе не позволяет выявить трафик, идущий в обход туннеля. Во вовремя захвата были реализованы входы на несколько сайтов, а также осуществлен Web-звонок, для того чтобы проверить наличие WebRTC-утечек. На основании полученной трассировки пакетов проведен анализ с использованием фильтров, которые позволили сделать процесс анализа более эффективным, где получили:

1) (ip or ipv6) and not (ip.addr == ip vpn сервера and udp.port == порт vpn сервера) and not (icmpv6 or llmnr or dhcp or mdns) and not (ip.host matches ".255$" or ip.addr == 224.0.0.0/4) - основной фильтр, который показывает трафик идущий в обход VPN.

2) dns and ip.dst != 94.180.146.224 , tcp.port == 443 or tcp.port == 853 or udp.port == 53 - дополнительные фильтры для выявления DNS-утечек.

3) stun or (udp.port >= 3478 and udp.port <= 3479) - дополнительный фильтра для выявления Web-RTC-утечек.

Проведенный экспериментальный анализ трафика при активном VPN-соединении выявил наличие нескольких типов утечек, которые классифицированы в таблице 1.

Таблица 1

Результаты анализа

№	Тип утечки	Протокол	Порт	IP-адрес назначения	Кол-во	Пояснение
1	WebRTC	UDP	3478-3479	155.212.193.40/49/59	88	Серьезная утечка
2	Google FCM/Microsoft Azure	TCP	5228	74.125.71.188/20.86.94.139	4/18	Системный обход
3	Microsoft Azure	TLSv1.2	433	20.86.94.139	18	Системный обход

По результатам анализа трафика, были сделаны следующие выводы:

1) Выявлена критическая утечка WebRTC – 88 STUN Binding Requests на серверы 155.212.193.x (порты 3478-3479), раскрывающая реальный публичный IP-адрес устройства.

2) Зафиксирован системный обход VPN – трафик к Google FCM (74.125.71.188:5228) и Microsoft Azure (20.86.94.139:443, TLSv1.2), что обусловлено намеренными решениями Google (документированный обход FCM) и работой системных служб Windows [5].

3) Классические DNS-утечки отсутствуют – DNS-запросы не направлялись на публичные серверы или серверы провайдера в обход VPN.

Таким образом, проведенный экспериментальный анализ показал, что исследованный VPN-сервер не обеспечивает полной защиты от утечек. Наиболее критичной является утечка через WebRTC, позволяющая любому веб-сайту получить реальный IP-адрес пользователя в обход VPN-туннеля. Отдельного внимания заслуживает обнаруженный обход VPN сервисами Google FCM и Microsoft. В отличие от DNS- и WebRTC-утечек, которые могут быть устранены настройкой VPN-клиента или браузера, системный обход требует более серьезных решений. Разработанная система фильтров может быть использована для тестирования других VPN-сервисов.

Список использованных источников:

1) Куроуз, Д. Ф. Компьютерные сети. Нисходящий подход / Д. Ф. Куроуз, К. У. Росс. – 6-е изд. – Москва: Эксмо, 2016. – 907 с. – ISBN 978-5-699-78090-7.

2) Храмов, Н. Р. Защита ресурсов сетей на основе технологии VPN / Н. Р. Храмов // Международный студенческий научный вестник. – 2019. – № 1. – С. 39.

3) Дружинин Б.Н., Терехин И.Э. Развитие архитектуры доступа к услуге IP Centrex [Электронный ресурс]. URL:

http://lib.tssonline.ru/articles2/fixop/razv_arh_dost_uslug_ip_centrex (дата обращения 03.04.2026).

4) Козлова, Н. О. Уязвимость VPN / Н. О. Козлова, А. Н. Герасимова, Е. Д. Кухтенкова // Вестник Тульского филиала Финуниверситета. – 2024. – № 1. – С. 154-156.

5) Google. Firebase Cloud Messaging: Network Configuration [Электронный ресурс] // Firebase Documentation. – 2026. – Режим доступа: https://firebase.google.com/docs/cloud-messaging/network-configuration (дата обращения: 10.04.2026).

Efimova S.V.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Fatkhelislamov A.F.
Ufa University of Science and Technology, Ufa

EXPERIMENTAL ANALYSIS OF DNS AND WEBRTC LEAKS IN A VPN SERVER BASED ON NETWORK PACKET TRACING IN WIRESHARK

Abstract. This article presents the results of an experimental analysis of DNS and WebRTC leaks in VPN connections. Using network packet tracing in Wireshark, traffic bypassing an active VPN tunnel was investigated. The analysis revealed several types of leaks: system-level VPN bypasses and STUN Binding Requests to STUN servers. The latter lead to the disclosure of the user's real public IP address. A system of filters for detecting and classifying leaks was also developed, and practical recommendations for risk mitigation were proposed.

Keywords: VPN, DNS leak, WebRTC leak, STUN, Wireshark, traffic analysis.

УДК 004

Кудакаев И.Ф.
Уфимский университет науки и технологий, Уфа

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

EDR VS XDR В ГЕТЕРОГЕННОЙ СРЕДЕ: КАКОЙ ПОДХОД ЭФФЕКТИВНЕЕ?

Аннотация. В статье рассматривается сравнительная эффективность двух подходов к защите конечных точек – EDR (Endpoint Detection and Response) и XDR (Extended Detection and Response) – в условиях разнородной инфраструктуры российских организаций. Установлено, что выбор между EDR и XDR определяется не только техническими возможностями решений, но и организационной зрелостью службы безопасности, масштабом инфраструктуры и отраслевой спецификой.

Ключевые слова: EDR, XDR, информационная безопасность, гетерогенная среда, киберугрозы, обнаружение инцидентов, корпоративная сеть

Технология Endpoint Detection and Response возникла как ответ на недостатки традиционных антивирусов. Если классический антивирус работает по принципу «обнаружить и заблокировать известную угрозу», то EDR фокусируется на обнаружении аномального поведения, сборе детальной телеметрии с конечных точками и возможности ретроспективного расследования инцидентов.

Преимущество EDR – глубокий мониторинг процессов на уровне конечной точки. Современные EDR-системы собирают и анализируют сотни параметров: запуск процессов, сетевые соединения, обращения к файловой системе, изменения реестра, попытки эскалации привилегий.

Однако в гетерогенной среде EDR сталкивается с принципиальным ограничениями. Во-первых, EDR-агенты разрабатываются не на все платформы одинаково хорошо. Windows-устройства обычно защищены лучше всего – здесь наиболее развиты возможности мониторинга и реагирования. Linux-серверы поддерживаются, но с меньшей функциональностью. MacOS и мобильные платформы могут не поддерживаться вообще или иметь существенно урезанный функционал. Промышленные системы управления, работающие на специализированных ОС, почти всегда остаются вне зоны контроля EDR. Во-вторых, изолированность данных. EDR собирает телеметрию с

конечных устройств, но плохо видит то, что происходит за их пределами – в сетевом трафике, на почтовых серверах, в облачных хранилищах, в системах идентификации. Это создает «слепые зоны» в картине безопасности. Атака может начаться с компрометации почтового ящика, продолжиться движением по сети через легитимные учетные записи и лишь на финальной стадии проявиться как подозрительная активность на конечной точке. EDR обнаружит только последний этап, упустив ранние индикаторы компрометации. В-третьих, сложность корреляции событий между разнотипными устройствами. Даже если EDR установлен на устройствах разных типов, корреляция событий между ними требует дополнительной интеграции с SIEM (Security Information and Event Management). Без этого аналитик видит отдельные фрагменты активности, но не целостную картину атаки, разворачивающейся одновременно на серверах, рабочих станциях и в облаке.

XDR (Extended Detection and Response) представляет собой эволюцию концепции EDR (Endpoint Detection and Response) [1]. Если EDR сосредоточен на конечных точках, то XDR расширяет зону видимости на всю инфраструктуру – конечные точки, сетевую активность, облачные сервисы, электронную почту, системы идентификации и управления доступом. Цель – получить единую картину происходящего и автоматизировать корреляцию событий между разными источниками данных.

Архитектурно XDR объединяет множество источников телеметрии в единую платформу анализа. Данные с конечных точек, сетевых сенсоров, межсетевых экранов, прокси-серверов, почтовых шлюзов, облачных API стекаются в единый центр анализа. Здесь применяются методы машинного обучения и поведенческого анализа для выявления комплексных многоступенчатых атак.

Однако XDR – это не универсальное решение всех проблем безопасности. Существует некоторые серьезные ограничения. Во-первых – сложность и стоимость внедрения. XDR требует интеграции с множеством источников данных, что предполагает совместимость с существующими системами безопасности [2]. Не все устройства и сервисы могут быть легко интегрированы. Унаследованные системы, не поддерживающие современные API, остаются вне поля зрения XDR. Кроме того, развертывание XDR требует значительных инвестиций не только в лицензии, но и в инфраструктуру – серверы для обработки больших объемов телеметрии, каналы связи для передачи данных, системы хранения. Во-вторых – зависимость от вендора. Большинство XDR-решений эффективно работают только с продуктами того же производителя. Если в организации используются межсетевые экраны одного вендора, почтовые шлюзы второго, а системы защиты конечных

точек третьего, полноценная интеграция в единую XDR-платформу может оказаться невозможной или потребует дополнительных затрат на кастомизацию. В-третьих, требования к квалификации персонала [3]. XDR генерирует большие объемы аналитической информации, и для ее эффективного использования требуются специалисты с навыками анализа данных, понимания тактик, техник и процедур атакующих (TTP), опыта расследования инцидентов.

XDR критически важен для организаций, сталкивающихся с целевыми атаками (APT – Advanced Persistent Threat). Принципиально важный момент: выбор не обязательно является бинарным. Существуют гибридные сценарии, когда организация начинает с внедрения EDR на критичных устройствах, а затем постепенно наращивает возможности за счет интеграции с SIEM, добавления сетевых сенсоров и облачных коннекторов, эволюционируя в сторону XDR.

Выбор между EDR и XDR в гетерогенной корпоративной среде не имеет универсального решения [4]. EDR остается эффективным и экономически оправданным инструментом для организаций с относительно однородной инфраструктурой, умеренным уровнем угроз и ограниченным бюджетом на информационную безопасность. Он обеспечивает глубокую видимость процессов на конечных точках и возможности быстрого реагирования на инциденты в границах своей зоны ответственности.

XDR представляет собой качественно иной уровень защиты, необходимый для организаций с высокой степенью гетерогенности инфраструктуры, активным использованием облачных сервисов, распределенной структурой и высоким уровнем угроз. Интеграция множества источников телеметрии в единую аналитическую платформу позволяет обнаруживать сложные многоэтапные атаки, которые остались бы незамеченными при использовании изолированных средств защиты.

Список использованных источников:

1. Forrester: EDR уже нет, а XDR все еще не решает проблемы SIEM // itweek.ru. 2023. URL: https://www.itweek.ru/security/article/detail.php?ID=228081 (дата обращения: 20.04.2026).

2. Козловский С.С. Преимущества XDR перед EDR: неэффективность EDR решений в современной киберзащите // Научный форум: Технические и физико-математические науки: сб. ст. по материалам LXXIX междунар. науч.-практ. конф. – М., Изд. «МЦНО», 2024. – № 11(79). – С. 1-7. URL: https://cyberleninka.ru/article/n/preimuschestva-xdr-pered-edr-neeffektivnost-edr-resheniy-v-sovremennoy-kiberzaschite (дата обращения: 18.04.2026).

3. Кудинов Д. Как внедрить решение класса Extended Detection and Response и сохранить деньги, время и нервы // cisoclub.ru. 2023. URL: https://cisoclub.ru/kak-vnedrit-reshenie-klassa-extended-detection-and-response-i-sohranit-dengi-vremja-i-nervy/ (дата обращения: 17.04.2026).

4. Внедрение EDR/XDR на предприятиях КИИ: интеграция с существующими системами и оптимизация детектирования сложных атак // cisoclub.ru. 2025. URL: https://cisoclub.ru/vnedrenie-edr-xdr-na-predprijatijah-kii-integracija-s-sushhestvujushhimi-sistemami-i-optimizacija-detektirovanija-slozhnyh-atak/ (дата обращения: 19.04.2026).

Kudakaev I.F.
Ufa University of Science and Technology, Ufa

Scientific supervisor
Yunusova D.S.
Ufa University of Science and Technology, Ufa

EDR VS XDR IN HETEROGENEOUS ENVIRONMENTS: WHICH APPROACH IS MORE EFFECTIVE?

Abstract. The article examines the comparative effectiveness of two approaches to endpoint protection – EDR (Endpoint Detection and Response) and XDR (Extended Detection and Response) – in the context of heterogeneous infrastructure of Russian organizations. It has been established that the choice between EDR and XDR is determined not only by the technical capabilities of solutions, but also by the organizational maturity of the security service, the scale of infrastructure, and industry specifics.

Keywords: EDR, XDR, information security, heterogeneous environment, cyber threats, incident detection, corporate network

УДК 004.056

Куликова В.Е., Колузанов Д.В.
Уфимский университет науки и технологий

Научный руководитель:
Байрушин Ф.Т.
Уфимский университет науки и технологий, Уфа

ИСПОЛЬЗОВАНИЕ КРИПТОГРАФИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ НА ОСНОВЕ ДИСКРЕТНЫХ НОСИТЕЛЕЙ

Аннотация. В статье рассматриваются основные риски при использовании дискретных носителей и разбираются способы выбора защиты. Показано, как объединить эти элементы в согласованную политику с проверяемыми критериями и записями аудита, подходящую для масштабируемого применения.

Ключевые слова: криптография, дискретные носители, ключ, пароль, информационная безопасность, архитектура защиты данных.

В современном мире все больше развивается сфера информационных технологий и немаловажным аспектом является информационная безопасность. Актуальность защиты данных на внешних носителях обусловлена их широким распространением и связанными с этим рисками.

Особенностью всех дискретных устройств является высокий риск потери, несанкционированного доступа, кражи или заражения через USB при подключении к чужому компьютеру.

Так как выбор криптографической защиты должен опираться на понимание рисков, стоит начать с их систематизации и сформулировать модель угроз для носителей.

Утрата или кража носителя является наиболее вероятной угрозой. Злоумышленник может получить побитную копию и просмотреть содержимое. Даже при использовании криптографической защиты не исключается риск внешнего воздействия, носитель мог быть похищен в разблокированном состоянии, ключи дешифрования могли сохраниться в оперативной памяти подключенного хоста. Впоследствии данные действия могут привести к компрометации конфиденциальности и, к возможности незаметной подмены данных при отсутствии аутентифицированного шифрования.

Стоит отметить и офлайн-атаку методом перебора [1]. Если злоумышленник имеет копию зашифрованного объема данных или

контейнера, то он сможет подобрать пароль. В данной ситуации атакующий свободен в выборе вычислительных ресурсов и выборе методик.

Класс атак «evil-maid» также требует внимания при анализе [2]. Метод реализуется в случае, когда злоумышленник получает физический доступ к носителю или компьютеру, под видномзаконного владельца для установки вредоносного ПО или аппаратных средств слежения. В результате, атакующий может перехватывать пароли, копировать файлы или производить другие виды вмешательства в работу устройства.

Источником компрометации данных выступают и атаки на уровень USB-классов и подмена устройства при подключении носителя к небезопасному хосту [3]. Такие атаки позволяют перехватывать ввод, запускать код с помощью драйверов и получать доступ к секретам в памяти.

Проблемой остается и утечка метаданных и других объектов, поскольку шифрование файлов без контейнеризации не скрывает эти данные. На дискретных носителях возникают дополнительные сложности, из-за которых некоторые фрагменты данных могут сохраняться в резерве, например, в неиспользуемых областях последнего сектора файла, в журналах файловой системы, в теневых копиях или кэшах, а также из-за того, что при удалении файла его блоки не перезаписываются, а помечаются как свободные. Это приводит к компрометации или изменению данных без взлома основного шифра. При шифровании на уровне отдельных файлов метаданные остаются незашифрованными, что также способствует утечке информации.

Отдельное внимание требует корректное обращение с копиями – бэкапами и снапшотами. Их защита требует согласования, а экспорт данных на носители с низкой степенью политики шифрования строго запрещен.

После определения актуальных векторов атак, стоит обозначить требования к целям и критериям, которым система должна соответствовать.

Из модели угроз следуют цели защиты. Конфиденциальность должна сохраняться как при владении носителем, так и при контролируемом доступе к хосту. Целостность должна быть проверяемой, чтобы незаметная подмена данных или среды предзагрузки была невозможна или обнаруживалась при проверке. Эти цели трансформируются в проверяемые критерии, например, сокрытие служебных данных и структуры каталога, прозрачность для пользователя, переносимость между средами, независимость от доверия к аппаратуре там, где это критично, и управляемость.

Значимой частью является криптографическая основа, которая задает рамки последующих архитектурных решений и сводится к согласованной работе нескольких механизмов.

Для полной защиты используют полное шифрование диска (FDE) [3]. При использовании этого метода шифруется весь том, защите подлежат все пользовательские данные, кэши и журналы. Также существуют самошифрующиеся диски (SED), в которых шифрование реализовано в контроллере накопителя. Итоговый уровень защиты зависит от корректности реализации прошивки контроллера и наличия цепочки загрузки.

На практике чаще всего применяются комбинации данных архитектурных подходов. Для сплошного шифрования и прозрачности используют FDE или SED в качестве базового слоя, а сверху – контейнеры для чувствительных наборов данных. При этом политики резервного копирования и очистки носителей должны учитывать совокупность перечисленных мер.

Надежность выбранного подхода также определяется управлением ключами. Управление ключами строится на связке парольной фразы, функции вывода ключа и разделении ключей шифрования данных (DEK) и ключей шифрования ключей (KEK) с возможностью многофакторной аутентификации.

Для накопителей на базе флэш-памяти стоит использовать встроенные средства безопасного удаления (Secure Erase / Crypto Erase или аналогичные механизмы в спецификации NVMe / ATA/NVMe-Sanitize) [4].

В случаях, когда накопитель выводится из эксплуатации, передается третьим лицам, продается, хранит критичные/чувствительные данные, решением будет его физическое уничтожение.

Организационные правила должны сопровождаться средствами регистрации и контроля. На первом этапе каждому устройству присваивается уникальный идентификатор, а его VID/PID вносятся в разрешенный список. На втором этапе в SIEM-системе коррелируются события подключения, разблокировки и попытки доступа, тогда как EDR/DLP отслеживает аномальные объемы чтения или записи и запуск кода с носителя. Третий этап обеспечивает автоматическое отклонение неодобренных устройств политикой USB-классов, выдача ключей привязывается к аттестации хоста, а любое несоответствие фиксируется как инцидент. На четвертом этапе механизмы целостности блокируют расшифровку при доступе в несогласованном состоянии.

Даже при грамотной настройке шифрования, работе с ключами и соблюдении стандартных процедур, уязвимости сохраняют свою

актуальность, особенно в контексте метаданных, системных журналов, резервных копий и эксплуатационных уязвимостей.

Кроме того, существуют аппаратно-программные уязвимости, такие как побочные каналы, ошибки реализации, дефекты стека шифрования/дешифрования, которые могут быть использованы для извлечения ключей, деталей шифрования или метаданных, особенно если носитель или хост – доверенные, но не полностью проверенные.

Поэтому при проектировании политики защиты носителей важно предусмотреть как механизм шифрования, так и меры контроля, иначе криптография может оказаться бесполезной перед человеческой оплошностью или побочными утечками.

Для практического применения все рассмотренные положения стоит объединить в единую методику защиты дискретных носителей информации. Это позволит рассматривать защиту носителей как последовательный и контролируемый процесс:

1. Определение типа носителя и условий его использования
2. Анализ актуальных угроз и возможных векторов компрометации
3. Выбор криптографических механизмов и архитектуры шифрования
4. Организация управления ключами и правил эксплуатации носителей
5. Контроль, аудит и процедуры безопасного удаления данных

Таким образом, защита дискретных носителей информации является согласованием архитектуры, управления ключами и организационными мерами под соответствующую модель угроз.

Список использованных источников:

1. System Password Security: Attack and Defense Mechanisms. URL: https://arxiv.org/html/2510.10246v1 (дата обращения: 20.03.2026).

2. Атака «evil maid». URL: https://habr.com/ru/articles/259781/ (дата обращения 20.03.2026).

3. Васильева, И. Н. Криптографические методы защиты информации: учебник и практикум для вузов / И. Н. Васильева. Москва: Издательство Юрайт, 2026. 310 с. – ISBN 978-5-534-02883-6.

4. Процессы удаления данных с твердотельного жесткого диска. URL: https://clck.ru/3Qadu6 (дата обращения: 25.03.2026).

Kulikova V.E., Koluzanov D.V.
Ufa University of Science and Technology

Scientific supervisor:
Bayrushin F.T.
Ufa University of Science and Technology, Ufa

USING CRYPTOGRAPHIC INFORMATION SECURITY TOOLS BASED ON DISCRETE MEDIA

Abstract. This article examines the main risks associated with using portable media and discusses methods for selecting protection against these risks. It demonstrates how these elements can be represented in a consistent policy with verifiable criteria and audit trails, suitable for scalable deployment.

Keywords*:* cryptography, local storage media, key, password, information security, data protection architecture.

УДК 004

Латыпов М.Р.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Салов И.В.
Уфимский университет науки и технологий, Уфа

СКВОЗНОЕ ШИФРОВАНИЕ

Аннотация. Сквозное шифрование представляет собой криптографическую технологию, обеспечивающую защиту данных от момента их отправки до момента получения адресатом без возможности промежуточного доступа. В условиях цифровизации российской экономики и государственного управления вопросы криптографической защиты информации приобретают особую актуальность. Особое внимание уделяется противоречиям между требованиями информационной безопасности и необходимостью обеспечения государственного контроля. определяется систематизацией подходов к внедрению технологий сквозного шифрования в российских организациях.

Ключевые слова: сквозное шифрование, криптографическая защита, информационная безопасность, цифровая коммуникация, протоколы шифрования, российское законодательство, защита персональных данных.

Криптографическая модель сквозного шифрования строится на принципе, исключающем доступ к содержимому передаваемых данных для любых промежуточных узлов – включая серверы провайдеров услуг связи и операторов цифровых платформ. Ключи шифрования генерируются и хранятся исключительно на устройствах отправителя и получателя.

В отличие от традиционной криптографии, где данные расшифровываются на серверах провайдера и повторно шифруются при передаче следующему узлу, сквозное шифрование реализует модель «нулевого доверия». Сообщение остается зашифрованным на всем пути следования. Провайдер видит лишь метаданные, отправителя, получателя, временные метки. Содержание – недоступно даже администраторам системы.

Технологически это обеспечивается криптографическими протоколами с использованием асимметричного шифрования. Каждый участник коммуникации располагает парой ключей, открытым, публикуемым в доступном реестре, и закрытым, хранимым локально на устройстве. Отправитель шифрует сообщение открытым ключом получателя. Расшифровка возможна только закрытым ключом получателя, который никогда не покидает его устройство.

Наиболее распространенной реализацией выступает протокол Signal, используемый в мессенджерах Signal, WhatsApp. Протокол обеспечивает Perfect Forward Secrecy – свойство, при котором компрометация долгосрочных ключей не приводит к расшифровке предыдущих сообщений. Для каждой сессии генерируются эфемерные ключи, удаляемые после завершения передачи [1].

Крупные западные платформы – Telegram, WhatsApp – формально не подпадают под юрисдикцию российского законодательства либо демонстрируют выборочное соблюдение требований. Российские разработчики, напротив, вынуждены либо отказываться от полноценного сквозного шифрования, либо создавать гибридные модели с возможностью выборочного доступа по запросам правоохранительных органов.

Ключевой момент – система предусматривает возможность интеграции с корпоративными инфраструктурами управления ключами, что позволяет администраторам организаций сохранять контроль над шифрованными коммуникациями сотрудников.

Другая проблема – вычислительные затраты. Асимметричное шифрование требует существенно больших ресурсов по сравнению с симметричными алгоритмами. На практике используется гибридный подход: асимметричное шифрование применяется лишь для обмена сессионными ключами, само же содержимое шифруется симметричным

алгоритмом – AES-256 или российским «Кузнечиком» (ГОСТ Р 34.12-2015).

По данным аналитического центра InfoWatch, в 2023 году 68% крупных российских компаний использовали для внутренних коммуникаций платформы со сквозным шифрованием – преимущественно зарубежные решения [2]. Одновременно лишь 23% из них внедрили корпоративные системы управления ключами шифрования, что создает риски утраты доступа к архивам переписки при увольнении сотрудников или компрометации устройств.

Практика внедрения сквозного шифрования формирует несколько различающихся по архитектуре моделей, каждая из которых представляет компромисс между безопасностью, удобством и регуляторными требованиями.

Первая модель – полностью децентрализованное шифрование без корпоративного контроля. Пользователи самостоятельно устанавливают мессенджеры с поддержкой E2EE, ключи генерируются и хранятся на личных устройствах. Такая модель типична для малого бизнеса и стартапов.

Вторая модель – гибридная архитектура с корпоративным управлением ключами. Сквозное шифрование реализуется, но мастер-ключи или их резервные копии хранятся в защищенном корпоративном хранилище. Доступ к ним строго регламентирован и требует многофакторной авторизации.

Третья модель – шифрование на уровне приложения с централизованным управлением политиками. Корпоративная платформа обеспечивает шифрование данных, но администратор может устанавливать правила: для каких групп пользователей включено E2EE, для каких применяется обычное транспортное шифрование с возможностью аудита. Такое решение позволяет дифференцировать уровень защиты в зависимости от чувствительности данных.

Важный аспект – мобильные устройства. Смартфоны и планшеты сотрудников представляют слабое звено в архитектуре E2EE. Потеря устройства или его компрометация вредоносным ПО дает злоумышленнику прямой доступ к ключам шифрования, хранящимся локально.

Международное измерение также значимо. Ограничения на экспорт криптографических технологий, введенные западными странами после 2022 года, стимулируют разработку отечественных решений, но одновременно создают риск технологической изоляции.

Сквозное шифрование представляет собой технологию, находящуюся на пересечении криптографической науки, инженерных практик и правового регулирования. Анализ российской ситуации

выявляет устойчивое противоречие между технологическими возможностями обеспечения максимальной защиты данных и регуляторными требованиями сохранения государственного контроля над коммуникациями.

Технологически E2EE достигло уровня зрелости, достаточного для массового внедрения. Протоколы Signal, Matrix, OMEMO демонстрируют надежность и производительность, приемлемую для корпоративного использования. Российские криптографические стандарты ГОСТ обеспечивают сопоставимый уровень защиты, но их интеграция в популярные платформы остается ограниченной.

Предложения определяются тремя сценариями. Первый – либерализация регулирования с признанием права на приватность коммуникаций и ограничением требований о предоставлении ключей шифрования исключительно делами о тяжких преступлениях по судебному решению. Второй – ужесточение контроля с обязательным депонированием ключей и сертификацией всех криптосредств. Третий, наиболее вероятный – отраслевая дифференциация с жестким регулированием в критических секторах и либеральным режимом для коммерческих коммуникаций.

Список использованных источников:

1. Ахметзянова Л.М., Газизов Т.Т. Анализ перспектив применения постквантовой криптографии в системах защищенной связи // Вопросы кибербезопасности. 2024. № 1 (59). С. 12–21. URL: https://cyberleninka.ru/article/n/analiz-perspektiv-primeneniya-postkvantovoy-kriptografii-v-sistemah-zaschischyonnoy-svyazi (дата обращения: 18.04.2026).

2. Годовой отчет InfoWatch: утечки конфиденциальной информации в России в 2023 году. Аналитический центр InfoWatch. URL: https://www.infowatch.ru/analytics/reports (дата обращения: 18.04.2026).

Latypov M.R.
Ufa University of Science and Technology, Ufa

Scientific supervisor
Salov I.V.
Ufa University of Science and Technology, Ufa

END-TO-END ENCRYPTION

Abstract. End-to-end encryption is a cryptographic technology that protects data from the moment it is sent to the moment it is received by the addressee without the possibility of intermediate access. In the context of the

digitalization of the Russian economy and public administration, the issues of cryptographic information protection are becoming particularly relevant. The article analyzes the technological foundations of end-to-end encryption, examines the specifics of its application in Russian information systems, and explores the legal aspects of using cryptographic protocols in the context of domestic legislation. Particular attention is paid to the contradictions between the requirements of information security and the need to ensure state control. The practical significance of the work is determined by the systematization of approaches to the introduction of end-to-end encryption technologies in Russian organizations.

Keywords: end-to-end encryption, cryptographic protection, information security, digital communication, encryption protocols, Russian legislation, personal data protection.

УДК 004.056.5

Лукашов Н.П.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Салов И.В.
Уфимский университет науки и технологий, Уфа

РЕАЛИЗАЦИЯ ЗАЩИТЫ ВЕБ-ПРИЛОЖЕНИЙ ОТ SQL-ИНЪЕКЦИЙ С ИСПОЛЬЗОВАНИЕМ MODSECURITY И FAIL2BAN В СРЕДЕ ОПЕРАЦИОННОЙ СИСТЕМЫ ASTRA LINUX

Аннотация. Статья посвящена задаче защиты веб-приложений от SQL-инъекций с использованием бесплатного межсетевого экрана приложений ModSecurity и системы Fail2ban в среде защищенной операционной системы Astra Linux Special Edition. Предложены пользовательские правила ModSecurity, дополняющие стандартный набор OWASP Core Rule Set, и показана их эффективность. Оповещение об атаках осуществляется через централизованную систему логирования.

Ключевые слова: SQL-инъекции, ModSecurity, Fail2ban, WAF, Astra Linux, защита веб-приложений.

SQL-инъекции остаются одной из наиболее опасных уязвимостей веб-приложений. По данным BI.ZONE [1], в зимнем дайджесте 2025 – 2026 годов SQL-инъекции лидируют среди уязвимостей с критическим уровнем последствий. Стандартные средства защиты, такие как экранирование спецсимволов или использование подготовленных запросов, часто реализуются разработчиками не в полном объеме, а

типовые правила WAF не всегда эффективны против скрытых или многоэтапных атак.

Целью работы является разработка и реализация системы защиты веб-приложений на базе ModSecurity [2] с пользовательскими правилами, автоматической блокировкой IP-адресов злоумышленников и централизованным логированием событий безопасности.

Структурная схема развернутого решения представлена на рисунке 1. Веб-сервер Apache2 обрабатывает входящие HTTP-запросы, а модуль ModSecurity анализирует их на наличие SQL-инъекций. При обнаружении атаки, опираясь на пользовательские правила, ModSecurity блокирует запрос, формируя лог. Система Fail2ban [3] анализирует лог ModSecurity и при превышении порога в 3 попытки блокирует IP-адрес злоумышленника на уровне межсетевого экрана. Оповещение об атаках осуществляется через бот ВКонтакте: при срабатывании правила ModSecurity вызывается bash-скрипт, который через VK API отправляет администратору сообщение с информацией о заблокированной SQL-инъекции.

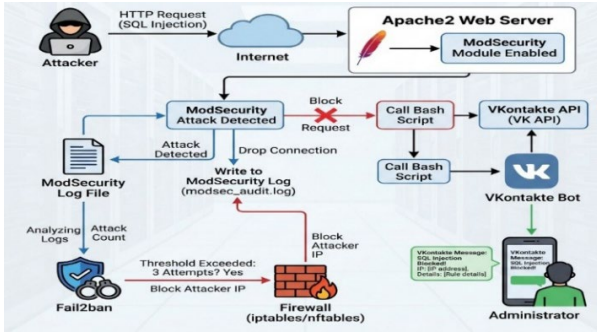


Рис. 1. Архитектура системы защиты веб-приложений

Развертывание операционной системы Astra Linux Special Edition [4] версии 1.8 с ядром 6.1.152-1-generic было реализовано в среде виртуализации Oracle Virtual Box. Для обеспечения корректной работы веб-сервера в сетевой инфраструктуре был настроен статический IP-адрес.

Далее был установлен веб-сервер Apache2. Особенностью операционной системы Astra Linux является наличие системы мандатного контроля доступа Parsec, которая без дополнительной настройки блокирует работу Apache2. Для решения этой проблемы в конфигурационном файле /etc/apache2/apache2.conf был отключен параметр AstraMode, что позволило серверу обрабатывать запросы без обязательной авторизации.

Для обеспечения защиты от SQL-инъекций был установлен модуль ModSecurity (libapache2-mod-security2). После установки модуль был активирован в Apache. В конфигурационном файле /etc/modsecurity/modsecurity.conf был включен параметр SecRuleEngine и настроено логирование.

В ходе работы был установлен стандартный набор правил OWASP Core Rule Set [5], загруженный из официального репозитория GitHub. Правила были размещены в директории /etc/modsecurity/rules/. Кроме того, была создана отдельная директория /etc/modsecurity/custom_rules/ для размещения пользовательских правил.

В ходе анализа эффективности стандартного набора OWASP Core Rule Set были выявлены типовые сценарии атак, обнаружение которых средствами CRS не является достаточным. В дополнение к ним были разработаны пять пользовательских правил, нацеленных на обнаружение UNION SELECT с вложенными запросами, многоуровневого кодирования, обхода через комментарии, многоэтапных атак и буферизации через несколько полей.

Автоматическая блокировка IP-адресов злоумышленников реализована с помощью Fail2ban. Был создан фильтр /etc/fail2ban/filter.d/modsecurity.conf, который анализирует логи ModSecurity и извлекает IP-адреса атакующего. Регулярное выражение фильтра учитывает срабатывание пользовательских правил.

Также была создана jail-конфигурация /etc/fail2ban/jail.d/modsecurity.local, включающая в себя: максимальное количество неудачных попыток, окно обнаружения, а также время блокировки.

Для обработки логов в формате JSON и отправки HTTP-запросов были установлены утилиты jq и curl.

Для тестирования разработанных правил было установлено уязвимое веб-приложение DVWA и необходимые расширения PHP, а также создан bash-скрипт для отправки уведомлений через VK API, интегрированный в ModSecurity с помощью директивы exec, что позволяет получать мгновенные сообщения о попытках SQL-инъекций (рис. 2). В ходе тестирования при отключенном ModSecurity SQL-инъекция приводила к краже данных, тогда как при включенном – запрос блокировался с ошибкой 403, IP-адрес атакующего фиксировался в логе (рис. 3) и блокировался Fail2ban после трех попыток.



Рис. 2. Уведомление об атаке UNION SELECT

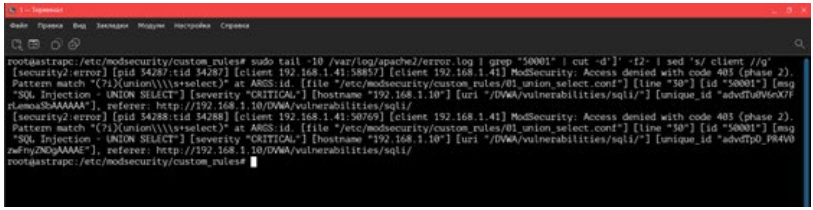


Рис. 3. Логи с информацией об атаке

Тестирование подтвердило, что предложенные правила эффективно блокируют атаки, которые стандартный OWASP CRS не обнаруживает. Среди них – SQL-инъекции с несколькими вложенными запросами.

Таким образом, развернута и настроена система защиты веб-приложений на ОС Astra Linux Special Edition с использованием ModSecurity и Fail2ban. Разработанные пользовательские правила расширяют OWASP CRS, компенсируя его недостаточную эффективность при обнаружении специфических векторов SQL-инъекций. Такое решение может применяться в корпоративных и государственных ИС, работающих с конфиденциальной информацией.

Список использованных источников:

1. BI.ZONE. Зимний дайджест уязвимостей от команды BI.ZONE WAF. – Текст: электронный. – URL: https://bi.zone/news/zimniy-daydzhest-uyazvimostey-ot-komandy-bi-zone-waf/ (дата обращения: 02.04.2026).

2. SpiderLabs. ModSecurity Reference Manual. – Текст: электронный. – URL: https://github.com/SpiderLabs/ModSecurity (дата обращения: 03.04.2026).

3. Fail2ban Documentation. – Текст: электронный. – URL: https://www.fail2ban.org (дата обращения: 07.04.2026).

4. АО «НПО РусБИТех». Операционная система Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.8). – Текст: электронный

// Справочный центр Astra Linux. – URL: https://wiki.astralinux.ru/pages/viewpage.action?pageId=318164553 (дата обращения: 02.04.2026).

5. OWASP Core Rule Set – How CRS Works. – Текст: электронный. – URL: https://coreruleset.org/docs/2-how-crs-works/ (дата обращения: 01.04.2026).

Lukashov N.P.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Salov I.V.
Ufa University of Science and Technology, Ufa

IMPLEMENTATION OF WEB APPLICATION PROTECTION AGAINST SQL INJECTIONS USING MODSECURITY AND FAIL2BAN IN THE ASTRA LINUX OPERATING SYSTEM ENVIRONMENT

Abstract. The article is devoted to the task of protecting web applications from SQL injections using the free ModSecurity web application firewall and the Fail2ban system in the secure operating system Astra Linux Special Edition. Custom ModSecurity rules that complement the standard OWASP Core Rule Set are proposed and their effectiveness is demonstrated. Attack alerts are carried out through a centralized logging system.

Keywords: SQL injections, ModSecurity, Fail2ban, WAF, Astra Linux, web application protection.

УДК 004.056.53

Мартинкевич Д.М., Янислaвский К.О.
Национальный детский технопарк, Минск

Научный руководитель:
Белоусова Е.С.
Белорусский государственный университет информатики и радиоэлектроники, Минск

БЛОКИРОВКА ПРИЛОЖЕНИЙ НА МЕЖСЕТЕВОМ ЭКРАНЕ CHUWALL

Аннотация. Данная статья является логическим продолжением авторской разработки межсетевого экрана CHUWALL и представляет реализацию функции блокировки приложений. Произведен

сравнительный анализ сервисов для обоснования выбора и внедрения ntopng. Разработан и реализован алгоритм работы функции блокировки приложений, тестирование которого показало успешность блокировки доступа к приложениям YouTube, Telegram и др.

Ключевые слова: CHUWALL; DPI; ntopng; Susp. Device Protocol; nftables; IP; URL; bash-скрипт; Telegram; YouTube.

На сегодняшний день актуальным вопросом в обеспечении информационной безопасности организаций является блокировка приложений, которые могут нелегитимно использоваться сотрудниками организаций и потенциально нанести вред внутренней инфраструктуре. Поэтому было принято решение дополнить функционал разработанного авторами межсетевого экрана CHUWALL [1] функцией блокировки доступа к приложениям.

Существует множество корпоративных решений с закрытым исходным кодом для обнаружения и блокировки приложений (Kaspersky NGFW, PT NGFW, UserGate и др.). Все они основаны на DPI (Deep Packet Inspection) – методе глубокого анализа пакетов на прикладном уровне модели OSI посредством сигнатур либо методов машинного обучения [2].

Для поиска оптимального решения по блокировке приложений было произведено исследование популярных сервисов с открытым исходным кодом (nDPI, ntopng, ufdbGuard, E2Guardian). По результатам сравнения был выбран сервис ntopng [3]. Он активно обновляется и поддерживается на актуальной версии ядра Linux, обладает удобным веб-интерфейсом, имеет мощный движок для классификации приложений.

Для внедрения сервиса ntopng в межсетевой экран CHUWALL был составлен алгоритм блокировки приложений (рисунок 1). Сервис ntopng проверяет поток в соответствии с политиками обработки. Если приложение (протокол) не соответствует правилу Susp. Device Protocol, анализ трафика продолжается без блокировки. В противном случае сервис ntopng создает событие типа Alert, при котором в формате JSON передаются данные об обнаруженном приложении в Shell Script alert.sh (рисунок 2).

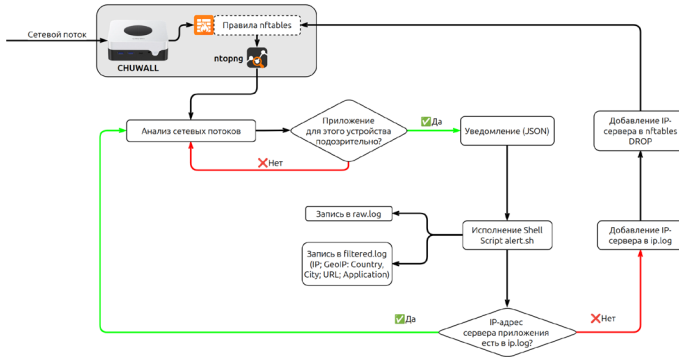


Рис. 1. Алгоритм работы блокировки приложений

Для последующей обработки события были созданы 3 файла логов:

- raw.log – содержит все данные, переданные ntopng при событии Alert;
- filtered.log (рисунок 3) – содержит IP-сервера, URL, название приложения (например, TLS.Youtube), страну и город сервера по базе GeoIP;
- ip.log – содержит IP-адреса, которые затем вносятся в список nftables для блокировки всех пакетов для этого IP-адреса.

Предварительно был создан список @ntopng_blocked в конфигурационном файле nftables с целью добавления IP-адресов, которые нужно заблокировать. Стоит отметить, что во избежание дублирования IP-адреса перед его блокировкой проверяется его наличие в файле ip.log. Если адрес уже был записан в файл ip.log, то повторно он записан не будет.

File: **alert.sh**

```
#!/bin/bash

# 1. Запись stdin в переменную PAYLOAD
PAYLOAD=$(cat)

# 2. Определение директории для записи файлов raw.log, filtered.log, ip.log и объявление их переменных
DIR="/var/log/ntopng_alerts"
RAW_LOG="$DIR/raw.log"
FILTERED_LOG="$DIR/filtered.log"
IP_LOG="$DIR/ip.log"

# 3. Определение переменной IP для взаимодействия с nftables
IP=$(echo "$PAYLOAD" | jq -r '.srv_ip // empty')

# 4. Запись stdin в raw.log
echo "$PAYLOAD" >> "$RAW_LOG"

# 5. Выборочная запись параметров из stdin в filtered.log
echo "$PAYLOAD" | jq -r '[
  (.srv_ip // "-"),
  (.srv_country_name // "-"),
  (.srv_city_name // "-"),
  (.info // "-"),
  (."proto.ndpi" // "-")
] | @tsv' >> "$FILTERED_LOG"

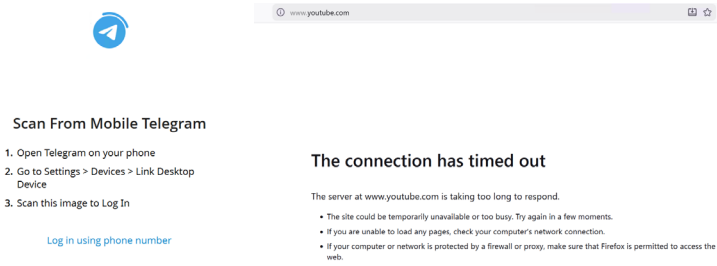
# 6. Проверка на отсутствие IP в файле ip.log. Если условие истинно, производится запись в файл ip.log и сет ntopng_blocked с таймаутом 7 дней
if ! grep -qw "$IP" "$IP_LOG"; then
    echo "$IP" >> "$IP_LOG"
    sudo nft add element inet filter ntopng_blocked { "$IP" timeout 7d }
fi
```

Рис. 2. Содержимое файла alert.sh

File: **filtered.log**

```
64.233.163.198  US  Mountain View   yt3.ggpht.com   TLS.YouTube
86.57.206.24    BY  Minsk   rr5---sn-cxauxaxjvh-hn9ee.googlevideo.com   TLS.YouTube
173.194.19.132  DE  Frankfurt am Main   rr4---sn-2of5f5-5p.c.youtube.com    TLS.YouTube
173.194.73.119  US  Mountain View   i.ytimg.com TLS.YouTube
86.57.206.92    BY  Minsk   rr9---sn-cxauxaxjvh-hn9el.googlevideo.com   TLS.YouTube
74.125.3.103    US  Dallas  rr2---sn-q4fl6n6s.googlevideo.com   TLS.YouTube
86.57.206.30    BY  Minsk   rr11---sn-cxauxaxjvh-hn9ee.googlevideo.com  TLS.YouTube
74.125.104.135  DE  Frankfurt am Main   rr2---sn-f5f7kn7e.googlevideo.com   TLS.YouTube
74.125.162.71   DE  Frankfurt am Main   rr2---sn-4g5lzner.googlevideo.com   TLS.YouTube
74.125.109.102  AU  Sydney  rr1---sn-ntqe6nee.googlevideo.com   TLS.YouTube
173.194.191.167 US  Chicago rr2---sn-q4flrnes.googlevideo.com   TLS.YouTube
173.194.10.231  IT  Milan   rr2---sn-f5f7lnl6.c.youtube.com TLS.YouTube
173.194.143.135 MX  Querétaro City rr2---sn-q4flrnek.googlevideo.com   TLS.YouTube
74.125.8.102    US  Mountain View   rr1---sn-5hne6nzs.googlevideo.com   TLS.YouTube
149.154.166.110 GB  London  api.telegram.org    TLS.Telegram
149.154.167.99  GB  London  kws2.web.telegram.org   TLS.Telegram
```

Рис. 3. Содержимое файла filtered.log



а *б*

Рис. 4. Попытки подключения к приложениям Telegram Desktop (а) и YouTube (б) при активной функции блокировки на межсетевом экране CHUWALL

Для проверки правильности работы блокировки приложений использовано устройство с операционной системой Microsoft Windows 11, подключенное к межсетевому экрану CHUWALL. На рисунке 4 показаны примеры подключений к приложениям Telegram Desktop и YouTube при активации функции блокировки приложений, которые демонстрируют ограниченное подключение.

Таким образом, функционал межсетевого экрана CHUWALL был дополнен возможностью блокировки доступа к определенным приложениям, что позволяет контролировать доступ сотрудников организации.

Список использованных источников:

1 Мартинкевич, Д.М. Функции фильтрации и шифрования DNS-сообщений на межсетевом экране CHUWALL / Д.М. Мартинкевич, К.О. Янославский, Е.С. Белоусова // Технические средства защиты информации: матер. XXIV Междунар. науч.-техн. конф. (Республика Беларусь, Минск, 08 апреля 2026 года). – Минск: БГУИР, 2025. – С. 90–93.

2 Контроль приложений / АО «Лаборатория Касперского: [сайт]. – Москва, 2026. – URL: https://support.kaspersky.com/help/NGFW/1.1/ru-RU/269838.htm (дата обращения: 28.03.2026).

3 GitHub – ntop/ntopng: Web-based Traffic and Security Network Traffic Monitoring: [сайт]. – 2026. – URL: https://github.com/ntop/ntopng (дата обращения: 28.03.2026).

Martsinkevich D.M., Yanislauski K.O.
National Children's Technopark, Minsk

Scientific supervisor:
Belousova E.S.
Belarusian State University of
Informatics and Radioelectronics, Minsk

APPLICATION BLOCKING ON THE CHUWALL FIREWALL

Abstract. This article describes the realization of app blocking function on the CHUWALL firewall. A comparison of services was carried out to implement ntopng. A developed algorithm showed success in blocking YouTube, Telegram, etc.

Keywords: CHUWALL; DPI; ntopng; Susp. Device Protocol; nftables; IP; URL; bash-script; Telegram; YouTube.

УДК 004.056

Муллаяров И.Р.
Нефтекамский филиал
Уфимского университета науки и технологий, Нефтекамск

Научный руководитель:
Аюпова А.Р.
Нефтекамский филиал
Уфимского университета науки и технологий, Нефтекамск

ПРОЕКТИРОВАНИЕ И ПРОГРАММНАЯ РЕАЛИЗАЦИЯ КОМПЛЕКСНЫХ СИСТЕМ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В ОБРАЗОВАТЕЛЬНЫХ ОРГАНИЗАЦИЯХ НА ОСНОВЕ КОНЦЕПЦИИ PRIVACY BY DESIGN

Аннотация. В статье рассматривается архитектурный подход к защите персональных данных (ПДн) в вузах через призму концепции Privacy by Design. Проведен анализ изменений законодательства 2025

года, включая оборотные штрафы и требования Приказа ФСТЭК № 117. Описана реализация программного комплекса «Журнал куратора» на Python 3.12 с применением PySide6, SQLite и криптостандартов AES-256 и PBKDF2. Представлена таблица соответствия реализованных мер базовому набору защиты для уровня УЗ-3

Ключевые слова: персональные данные, Privacy by Design, Python 3.12, AES-256, PBKDF2, ФСТЭК России, Приказ № 117, УЗ-3, образовательная организация

Цифровая трансформация образования в РФ сопровождается беспрецедентным ростом киберугроз. В первом полугодии 2025 года количество инцидентов в образовательном секторе выросло на 20% по сравнению с 2024 годом, а объем утекших записей составил 1,7 млн. Ситуация осложняется радикальным ужесточением регуляторных требований, с 2025 года введены «градуированные» штрафы (до 15–20 млн руб. за первичную утечку и до 500 млн руб. за повторную), а также действует безусловный запрет на хранение ПДн россиян вне территории РФ. С 1 сентября 2025 года также введено требование об обязательном оформлении согласия на обработку ПДн в виде отдельного документа, исключающее его включение в общие оферты.

Для образовательных организаций наиболее актуальными являются угрозы 3-го типа, не связанные с программными закладками в ОС. Среди внешних векторов доминируют атаки на цепочки поставок (Supply Chain) – 21% случаев – и целевой AI-фишинг (17%). Внутренние угрозы, согласно данным InfoWatch, остаются критическими из-за халатности персонала (использование слабых паролей, несанкционированное копирование).

Традиционный подход «наложения» средств защиты на готовую систему более неэффективен. Концепция Privacy by Design (PbD) предполагает интеграцию защитных механизмов в архитектуру ПО на этапе проектирования.

В разработанном комплексе реализованы четыре принципа PbD:

– предотвращение рисков через анализ кода и моделирование угроз;

– ПДн защищены автоматически без действий пользователя;

– криптография является частью бизнес-логики;

– контроль данных от сбора до автоматизированного уничтожения (через 3 года после выпуска студента).

Программный комплекс «Журнал куратора» реализован как модульное настольное приложение на языке Python 3.12 с использованием графической библиотеки PySide6. Выбор настольной архитектуры в связке с локальной СУБД SQLite исключает риски, характерные для передачи данных в облачные среды.

Проектирование велось по принципу минимизации, система собирает только сведения, необходимые для учебного процесса. Критичные поля хранятся в бинарном зашифрованном виде (BLOB).

Таблица 1

Схема хранения данных в таблице students

Поле	Тип данных	Назначение	Режим безопасности
id	INTEGER	Первичный ключ	Открыто
first_name, last_name	TEXT	Имя, Фамилия	Открыто
passport_data	BLOB	Паспортные данные	Шифрование AES-256
inn_snils	BLOB	ИНН и СНИЛС	Шифрование AES-256

Для обеспечения надежности в Python 3.12 использованы встроенные реализации hashlib, базирующиеся на формально верифицированном коде проекта HACL*, что минимизирует риск низкоуровневых ошибок.

Пароли хешируются с использованием алгоритма PBKDF2-HMAC-SHA256 с солью 16 байт и 200 000 итерациями. Формула вычисления ключа:

$$DK = PBKDF2(PRF, Password, Salt, c, dkLen)$$

Применено симметричное шифрование AES-256 в режиме CBC (Cipher Block Chaining). Для каждой записи генерируется случайный вектор инициализации (IV), что предотвращает частотный анализ. Управление ключами реализовано через концепцию Master Key: 256-битный ключ генерируется при первом запуске и хранится в изолированном файле secret.key. Пример реализации представлен на рисунке 1.

```
def hash_password(password: str, salt: bytes = None, iterations: int = 200_000):  5 usages
    if salt is None:
        salt = secrets.token_bytes(16)
    dk = hashlib.pbkdf2_hmac( hash_name: "sha256", password.encode("utf-8"), salt, iterations)
    return {
        "salt": binascii.hexlify(salt).decode("ascii"),
        "iterations": iterations,
        "hash": binascii.hexlify(dk).decode("ascii"),
    }
```

Рис. 1. Реализация алгоритма

В системе внедрена ролевая модель RBAC (Администратор, Куратор, Студент). Примечательно, что администратор имеет права на управление учетными записями, но не обладает прямым доступом к расшифрованным данным студентов без соответствующей функциональной роли. Все действия логируются в защищенный Audit Log.

Архитектура комплекса позволяет выполнять требования Приказа № 117 по динамическому управлению уязвимостями. Для обеспечения этого требования в комплексе реализована модульная структура, позволяющая оперативно обновлять криптографические сервисы. Также Приказ № 117 предписывает внедрение систем контроля привилегированного доступа (PAM), что реализовано в нашем ПО через жесткую привязку сессий к ролям.

Программный комплекс обеспечивает выполнение базового набора мер защиты для уровня УЗ-3.

Таблица 2

Соответствие реализованных мер требованиям регулятора

Код меры	Группа мер	Реализация в системе
ИАФ	Идентификация	PBKDF2-HMAC-SHA256, блокировка при переборе
УПД	Управление доступом	Модель RBAC, параметризованные SQL-запросы
РСБ	Регистрация событий	Сквозное логирование всех CRUD-операций
ОЦЛ	Целостность	Контроль хэш-сумм файлов БД и приложения
ЗНИ	Защита носителей	Построчное шифрование БД алгоритмом AES-256

Тестирование на проникновение (Penetration Testing) подтвердило устойчивость системы к SQL-инъекциям за счет использования исключительно параметризованных запросов.

Разработанный программный комплекс «Журнал куратора» демонстрирует эффективность встраивания механизмов защиты (AES-256, PBKDF2) непосредственно в бизнес-логику приложения. В условиях 2025–2026 годов применение принципов Privacy by Design позволяет образовательным организациям не только минимизировать риски штрафов до 500 млн рублей, но и обеспечить реальную, а не бумажную защищенность данных. Перспективы развития проекта связаны с внедрением двухфакторной аутентификации (2FA).

Список использованных источников:

1. Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 24.06.2025) "О персональных данных" // справ.-правовая система «КонсультантПлюс». ВерсияПроф. – Электрон. текст. дан. - Послед. Обновление: 01.03.2026 г.

2. Кодекс Российской Федерации об административных правонарушениях» от 30.12.2001 № 195-ФЗ. Статья 13.11. // справ.-правовая система «КонсультантПлюс». ВерсияПроф. – Электрон. текст. дан. - Послед. Обновление: 01.03.2026 г.

3. Постановление Правительства РФ от 01.11.2012 N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» // справ.-правовая система «КонсультантПлюс». ВерсияПроф. – Электрон. текст. дан. - Послед. Обновление: 01.03.2026 г.

4. Приказ Федеральной службы по техническому и экспортному контролю от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» // официальный сайт ФСТЭК России. – Электрон. текст. дан. – URL: https://fstec.ru/ (дата обращения 01.03.2026).

5. Аналитический отчет «Утечки информации ограниченного доступа в России 2023-2024» / [Электронный ресурс] // INFOWATCH.RU: [сайт] URL: https://www.infowatch.ru/sites/default/files/analytics/files/rossiya-utechki-informatsii-ogranichennogo-dostupa-2023-2024.pdf (дата обращение 26.11.2025).

6. Документация Python-библиотеки cryptography / [Электронный ресурс] // cryptography: [сайт] URL: https://cryptography.io/en/latest/ (дата обращение 01.03.2026).

7. Документация Python-библиотеки bcrypt / [Электронный ресурс] // pypi: [сайт] URL: https://pypi.org/project/bcrypt/ (дата обращение 01.03.2026).

Mullayarov I.R.
Neftekamsk Branch of Ufa University of Science and Technology,
Neftekamsk

Scientific supervisor:
Ayupova A.R.
Neftekamsk Branch of Ufa University of Science and Technology,
Neftekamsk

DESIGN AND SOFTWARE IMPLEMENTATION OF COMPLEX PERSONAL DATA PROTECTION SYSTEMS IN EDUCATIONAL ORGANIZATIONS BASED ON THE PRIVACY BY DESIGN CONCEPT

Abstract. The article considers an architectural approach to the protection of personal data (PD) in universities through the prism of the Privacy by Design concept. An analysis of the 2025 legislative changes is conducted, including turnover-based fines and the requirements of FSTEC Order No. 117. The implementation of the "Curator's Journal" software complex in Python

3.12 using PySide6, SQLite, and the AES-256 and PBKDF2 cryptographic standards is described. A table mapping the implemented measures to the basic protection set for the 3rd level of protection (UZ-3) is presented.

Keywords: personal data, Privacy by Design, Python 3.12, AES-256, PBKDF2, FSTEC of Russia, Order No. 117, UZ-3, educational organization.

УДК 004

Мусина К.Ш.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Сенцова А.Ю.
Уфимский университет науки и технологий, Уфа

ОТЕЧЕСТВЕННЫЕ КИБЕРПОЛИГОНЫ КАК СРЕДСТВО ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИМИ ПРОЦЕССАМИ (НА ПРИМЕРЕ ИНТЕГРАЦИИ AMPIRE И ЦДЭС)

Аннотация. Рассматривается проблема обеспечения информационной безопасности автоматизированных систем управления технологическими процессами (АСУ ТП) объектов критической информационной инфраструктуры (КИИ). Проведен анализ отечественных киберполигонов для моделирования атак. Особое внимание уделено интеграции киберполигона Ampire с цифровым двойником энергосистемы (ЦДЭС). Рассмотрен опыт создания полигона в ТУСУРе. Показано, что применение киберполигонов позволяет повысить эффективность подготовки кадров и тестирования средств защиты.

Ключевые слова: киберполигон, цифровой двойник, АСУ ТП, КИИ, моделирование атак, Ampire, ЦДЭС, импортозамещение.

Современные автоматизированные системы управления технологическими процессами (АСУ ТП) объектов критической информационной инфраструктуры (КИИ) подвергаются растущему числу кибератак. Согласно исследованиям, количество инцидентов в промышленном секторе ежегодно увеличивается [1]. При этом отработка навыков защиты и тестирование средств безопасности на реальных объектах невозможны из-за риска нарушения производственных процессов.

Нормативно-правовую основу обеспечения безопасности АСУ ТП составляют Федеральный закон от 26.07.2017 № 187-ФЗ, Постановление Правительства РФ от 08.02.2018 № 127 и Приказ ФСТЭК России от

25.12.2017 № 239, который для значимых объектов КИИ требует реализации мер идентификации и аутентификации [2–4]. Выполнение данных требований невозможно без подготовки квалифицированных кадров и тестирования средств защиты на киберполигонах, что обуславливает актуальность их создания.

Киберполигон представляет собой изолированную программно-аппаратную среду, эмулирующую реальную информационную инфраструктуру и позволяющую безопасно отрабатывать сценарии кибератак, тестировать средства защиты и готовить специалистов-практиков. Киберполигон Ampire, разработанный компанией «ИнфоТеКС», включает шаблоны ИТ-инфраструктур, учебные сценарии компьютерных атак, средства защиты информации, систему управления инцидентами и портал для взаимодействия с пользователями. Пример архитектуры такого решения представлен на рисунке 1.



Рис. 1. Архитектура киберполигона Ampire (разработка ГК «ИнфоТеКС»)

Специфика АСУ ТП требует поддержки промышленных протоколов (Modbus, МЭК 61850, МЭК 60870-5-104) и учета связи информационных воздействий с физическими процессами. В 2021 году введен ГОСТ Р 57700.37-2021, устанавливающий общие требования к цифровым двойникам изделий [5].

Для иллюстрации современных подходов к созданию киберполигонов в России рассмотрим интеграцию киберполигона Ampire с цифровым двойником энергосистемы (ЦДЭС) и разработку специализированного полигона для АСУ ТП в Томском государственном университете систем управления и радиоэлектроники (ТУСУР).

Цифровой двойник энергосистемы (ЦДЭС), разработанный Центром НТИ Московского энергетического института, обеспечивает моделирование в реальном времени режимов работы энергообъектов и энергосистем разного масштаба, функциональное и информационное

моделирование систем защиты, автоматизации и управления, а также интеграцию с кибер-физическими системами по цифровым протоколам МЭК 61850 (GOOSE, SV, MMS), МЭК 60870-5-104, C37.118, Modbus, UDP. Важной функцией является автоматическая генерация и контроль корректности проектных решений для цифровых систем релейной защиты и автоматики.

Ключевой особенностью является интеграция киберполигона Ampire и ЦДЭС. Как отмечает А.А. Пушкин, заместитель генерального директора АО «Перспективный мониторинг»: «Цифровой двойник энергосистемы содержит в себе все компоненты, которые нужны для использования в киберполигоне: отраслевые протоколы, системы управления операторов, моделирование действий конечных устройств, которые показывают, насколько негативно было то или иное воздействие» [6]. Результатом интеграции стала возможность применения сценариев учебных атак, специфичных для электроэнергетической отрасли, и подготовки специалистов по информационной безопасности для конкретных отраслей.

В Томском государственном университете систем управления и радиоэлектроники (ТУСУР) в рамках программы «Приоритет-2030» ведется разработка полигона для моделирования атак на АСУ ТП [7]. Развернут стенд, включающий 14 физических модулей промышленной автоматики и цифровой двойник газоперекачивающей станции. По словам заместителя директора ЦК НТИ «Технологии доверенного взаимодействия» А. Конева, разработка полигона направлена на решение двух ключевых задач: моделирование технологических процессов в АСУ ТП с созданием методических рекомендаций, а также отработка сценариев атак и разработка механизмов защиты для низкого уровня передачи данных. На стенде моделируются атаки следующих типов: отказ в обслуживании, несанкционированное чтение данных из контроллеров, сканирование сети АСУ ТП. Работа со стендом уже внедрена в учебный процесс [8].

Применение киберполигонов позволяет решать задачи моделирования угроз до внедрения систем защиты, тестирования средств защиты информации, подготовки специалистов (дефицит в России оценивается более чем в 20 000 человек), проведения киберучений без риска для реального производства.

К числу проблем развития киберполигонов можно отнести дефицит квалифицированных кадров в области информационной безопасности, необходимость дальнейшей стандартизации подходов (серия ГОСТ 57700) [5], а также сложность обеспечения полной реалистичности генерируемого трафика и атакующих воздействий. Перспективными направлениями являются развитие гибридных полигонов, сочетающих

физические и виртуальные компоненты, интеграция с реальными центрами мониторинга (SOC), а также автоматизация генерации сценариев атак.

Проведенный анализ показал, что отечественные киберполигоны для АСУ ТП демонстрируют высокий уровень технологической проработки. Интеграция киберполигона Ampire с цифровым двойником энергосистемы (ЦДЭС) позволяет моделировать специфические для электроэнергетики сценарии атак с оценкой последствий для физических процессов. Опыт ТУСУРа показывает возможность эффективного использования киберполигонов в образовательном процессе для подготовки кадров [8]. Дальнейшее развитие отечественных киберполигонов позволит повысить уровень защищенности объектов КИИ.

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. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» // Собрание законодательства РФ. 2017. № 31. Ст. 4736.

3. Постановление Правительства РФ от 08.02.2018 № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации» // Собрание законодательства РФ. 2018. № 8. Ст. 1204.

4. Приказ ФСТЭК России от 25.12.2017 № 239 (ред. от 28.08.2024) «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» // Официальный интернет-портал правовой информации.

5. ГОСТ Р 57700.37-2021. Компьютерные модели и моделирование. Цифровые двойники изделий. Общие положения. М.: Стандартинформ, 2021.

6. Пушкин А.А. Цифровые двойники на киберполигоне Ampire // Панельная сессия «Цифровые двойники в энергетике» в рамках III Научно-практической конференции «Территория энергетического диалога – 2024».

7. Программа «Приоритет-2030» [Электронный ресурс]. URL: https://priority2030.ru/ (дата обращения: 12.03.2026).

8. В ТУСУРе создают российский полигон моделирования атак в АСУ ТП [Электронный ресурс]. URL: https://tusur.ru/ru/novosti-i-meropriyatiya/novosti/prosmotr/-/novost-v-tusure-sozdayut-rossiyskiy-poligon-modelirovaniya-atak-v-asu-tp (дата обращения: 12.03.2026).

Musina K.Sh.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Sentsova A.Yu.
Ufa University of Science and Technology, Ufa

DOMESTIC CYBER RANGES AS A MEANS OF ENSURING THE SECURITY OF INDUSTRIAL CONTROL SYSTEMS (ON THE EXAMPLE OF AMPIRE AND DTPS INTEGRATION)

Abstract. The problem of ensuring information security of industrial control systems (ICS) of critical information infrastructure facilities is considered. The analysis of domestic cyber ranges for attack simulation is carried out. Special attention is paid to the integration of the Ampire cyber range with the digital twin of the power system (DTPS). The experience of creating a cyber range at TUSUR University is considered. It is shown that the use of cyber ranges improves the efficiency of personnel training and testing of information security tools.

Keywords: cyber range, digital twin, industrial control systems, CII, attack simulation, Ampire, DTPS, import substitution.

УДК 004.056

Мухаметшина Р.А.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Яппаров Р.М.
Уфимский университет науки и технологий, Уфа

ПРОВЕРКА ЗАЩИЩЕННОСТИ МЕЖСЕТЕВОГО ВЗАИМОДЕЙСТВИЯ НА БАЗЕ ПЛАТФОРМЫ VIPNET COORDINATOR

Аннотация. В статье представлены результаты экспериментальной проверки корректности начального развертывания защищенного межсетевого взаимодействия на базе двух координаторов ViPNet в лабораторной среде. Верификация выполнялась поэтапно: от диагностики DHCP-конфигурации и маршрутизации до подтверждения факта передачи зашифрованного трафика средствами собственного командного интерпретатора платформы. Приводятся конкретные команды диагностики, их интерпретация и итоговый критерий подтверждения

защищенного канала. Определены направления дальнейшего исследования политики фильтрации и туннелирования.

Ключевые слова: ViPNet Coordinator, защищенный канал, взаимодействие, журналирование, маршрутизация, сетевая конфигурация.

Защита межсетевого взаимодействия в распределенных информационных системах требует использования не только криптографических механизмов, но и проверку защищенного межсетевого взаимодействия, которая подтверждается корректностью сетевой конфигурации. При построении защищенной сети между удаленными сегментами необходимо обеспечить адресное распределение, маршрутизацию, связность транспортного участка и регистрацию факта передачи зашифрованного трафика.

В данном исследовании мы хотим подтвердить корректность начального развертывания защищенного взаимодействия между двумя координаторами ViPNet в лабораторной схеме с подсетями 192.168.10.0/24 и 192.168.20.0/24. Для реализации поставленной задачи нами была разработана экспериментальная схема, представленная на рисунке 1.

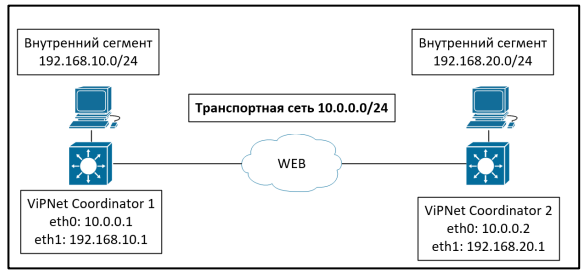


Рис. 1. Экспериментальная схема проверки защищенного межсетевого взаимодействия на базе VIPNET COORDINATOR

Отметим, что внешние интерфейсы координаторов работают в транспортной сети 10.0.0.0/24 с адресами 10.0.0.1 и 10.0.0.2, а внутренние интерфейсы используют адреса 192.168.10.1 и 192.168.20.1 соответственно. Проверку будем выполнять средствами командного интерпретатора с помощью команд:

inet show dhcp server
inet show routing
inet ping 10.0.0.2
inet ping 10.0.0.1
iplir ping 0x1971000b
iplir view

В результате вывод inet show dhcp server на первом координаторе показал, что DHCP-сервер запущен, автозапуск включен, обслуживание ведется через интерфейс eth1, диапазон выдачи адресов составляет 192.168.10.3-192.168.10.9, а в качестве маршрутизатора клиентам передается адрес 192.168.10.1. Следовательно, внутренний сегмент 192.168.10.0/24 обслуживается корректно и координатор выполняет функцию сетевого узла доступа.

В свою очередь вывод inet show routing подтвердил наличие ключевых маршрутов: маршрута по умолчанию через 10.0.0.2 по интерфейсу eth0, непосредственно подключенных сетей 10.0.0.0/24 и 192.168.10.0/24, а также статического маршрута к удаленной сети 192.168.20.0/24 через 10.0.0.2. На наш взгляд, этого набора достаточно для доставки трафика из локального сегмента к удаленной подсети через соседний координатор.

Команды inet ping 10.0.0.2 и inet ping 10.0.0.1 были успешно выполнены в обоих направлениях без потерь пакетов. Полученный результат подтвердил исправность транспортного участка и базовую IP-связность между координаторами [1]. Однако такая проверка сама по себе не доказывает криптографическую обработку трафика, поскольку ICMP-ответ может быть получен и при отсутствии защищенного соединения [2].

Поэтому для проверки защищенного межсетевого взаимодействия была использована команда iplir ping 0x1971000b. Успешный ответ Connection successful подтвердил достижимость именно защищенного узла сети ViPNet. После этого был открыт журнал IP-пакетов командой iplir view. В журнале для интерфейса eth0 зафиксировано событие Encrypted IP packet allowed; в деталях события указаны Source Node: Server 1 и Destination Node: Server 2. Это означает, что между координаторами прошел зашифрованный IP-пакет, а не обычный открытый трафик. На рисунке 2 приведена выгрузка из журнала событий при помощи команды iplir view.

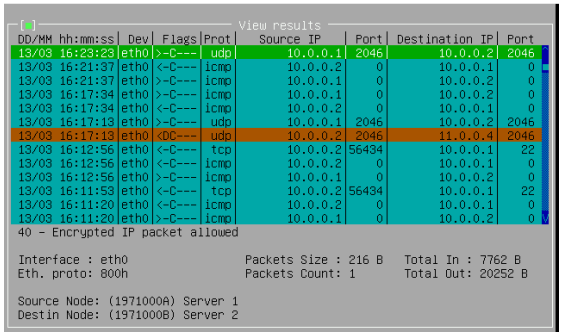


Рис. 2. Регистрация событий в журнале iplir view

Таким образом, совокупностью конкретных признаков: исправной раздачей адресов во внутреннем сегменте, корректной маршрутной таблицей, двусторонней IP-связностью внешних интерфейсов, положительным ответом на iplir ping и регистрацией события Encrypted IP packet allowed во встроенном журнале было подтверждено защищенное межсетевое взаимодействие.

Представленная методика охватывает лишь начальный этап обследования стенда. На следующем этапе имеет смысл перейти анализу режимов обработки трафика: проверить правила межсетевого экрана в цепочках local, forward, vpn и tunnel, сравнить прохождение открытого и защищенного трафика при изменении политики фильтрации, настроить туннелирование Linux-узлов за координаторами и зафиксировать в журнале iplir view различие между транзитным, защищенным и туннельным трафиком. Такой переход позволит исследовать не только наличие защищенного канала, но и управляемость политики доступа в сети ViPNet.

Полученные результаты имеют практическое значение в контексте защиты информации. Применение ViPNet Coordinator обеспечивает криптографически подтвержденное межсетевое взаимодействие, что отвечает общему требованию о защите передаваемых данных при использовании незащищенных каналов связи в распределенных информационных системах. Регистрация события Encrypted IP packet allowed в журнале iplir view напрямую реализует требование об учете событий информационной безопасности — обязательного элемента системы защиты в распределенных информационных системах.

Список использованных источников:

1. ViPNet Coordinator HW 4. Настройка с помощью командного интерпретатора [Электронный ресурс]. URL: https://infotecs.ru/downloads/documents/vipnet-coordinator-hw-4/.

2. Андреев, М.Ф. Анализ возможностей фильтрации трафика на межсетевом экране xFirewall / М.Ф. Андреев, А.С. Исмагилова // Инженерный вестник Дона. – 2025. – № 7(127). – С. 421-432.

Mukhametshina R.A.
Ufa university of science and technology, Ufa

Scientific supervisor:
Yapparov R.M.
Ufa university of science and technology, Ufa

TESTING THE SECURITY OF INTERNETWORK INTERACTION USING THE VIPNET COORDINATOR PLATFORM

Abstract. This article presents the results of an experimental verification of the initial deployment of secure inter-network communication based on two ViPNet devices in a laboratory coordinate system. Verification was performed in stages: from diagnosing the DHCP configuration and routing to confirming encrypted traffic transmission using a proprietary command interpreter platform. Specific readings are interpreted, and the final criterion for confirming a secure channel is determined. Directions for further research, filtering, and tunneling policies are identified.

Keywords: ViPNet Coordinator, secure channel, interaction, logging, routing, and network configuration.

УДК 621.396.96:004.056

Сауляк А.Ф.
Северный (Арктический) Федеральный Университет, Архангельск

Научный руководитель:
Зубарев А.А.
Северный (Арктический) Федеральный Университет, Архангельск

МЕТОДЫ ЗАЩИТЫ КОНТРОЛИРУЕМОЙ ЗОНЫ С ИСПОЛЬЗОВАНИЕМ ПЕЛЕНГАЦИИ

Аннотация. В статье приводятся сравнительные характеристики наиболее распространенных методов радиопеленгации, делается оценка эффективности их применения для промышленных объектов и приводятся рекомендации по построению системы безопасности предприятия с использованием методов пеленгации.

Ключевые слова: радиопеленгация, TDoA, корреляционная интерферометрия, защита предприятия, информационная безопасность.

Введение. В условиях увеличения масштабов промышленных объектов и роста сложности угроз возрастает значение методов

пассивного радиообнаружения, позволяющих обеспечивать непрерывный и скрытый мониторинг активности внутри контролируемой зоны.

Если традиционные средства охраны фиксируют лишь факт пересечения объектов физического периметра, то методы пеленгации позволяют определять направление и местоположение источников радиоизлучения, обеспечивая динамическое отслеживание перемещений.

Основы пеленгации источников радиоизлучения. Пеленгация представляет собой процесс определения углового направления на источник сигнала относительно выбранного опорного направления, после чего посредством метода триангуляции может быть вычислено метаположение источника радиосигнала. На практике используются следующие варианты опорных систем: направление географического севера, магнитного севера, курс собственных средств или относительное положение другого объекта.

По способу воздействия на источник различают:

- активную пеленгацию (РЛС), основанную на регистрации отраженного сигнала;
- пассивную пеленгацию, при которой фиксируется излучение самого источника [1].

Для задач скрытого мониторинга внутри контролируемых зон предпочтительной является пассивная пеленгация, поскольку она не демаскирует систему и позволяет отслеживать устройства без необходимости их опроса или подсветки.

Методы радиопеленгации. Существующие методы пеленгации основаны на анализе различных параметров радиосигнала: амплитуды пойманного сигнала, фазы уловленного сигнала, величины доплеровского сдвига при движении антенны по окружности, времени прихода сигнала.

Амплитудный метод использует различия уровня сигнала при повороте направленной антенны, например рамки. Является наиболее простым в реализации методом пассивной пеленгации, но имеет очень низкую точность (3–15°), по сравнению с другими видами пеленгации. Так же очень чувствителен к помехам и чаще всего работает в ручном режиме под управлением оператора, что не позволяет отслеживать более 2-3 источников одновременно.

Фазовый метод определяет разность фаз сигнала, приходящего на пространственно разнесенные антенны. Позволяет уточнять направление с точностью 1–5°, однако требует точного изготовления антенн и калибровки системы перед использованием. Является более совершенным методом по сравнению с амплитудной пеленгацией, поскольку является наиболее технически ложным устройством, что позволяет внедрять его в автоматизированные комплексы, но при этом

проблема количества определяемых одновременно источников сигнала остается [2].

Доплеровский метод основан на измерении изменения частоты принимаемого сигнала при создании искусственного относительного движения антенн. Ограничен по применимости – эффективен преимущественно в диапазонах длинных и средних волн. На высоких частотах требует высокоточного проектирования и изготовления. Обеспечивает точность 1–3°, что хороший показатель по сравнению с амплитудным и фазовым методами, но из-за специфики метода, даже при высоких вычислительных мощностях позволяет отслеживать одновременно не более 3 устройств [3].

Временной метод (TDoA) основан на измерении разницы времени прихода фронта сигнала на разнесенные в пространстве приемники. Позволяет определять координаты источника в плоскости и пространстве. Главная сложность – точная синхронизация времени, но при грамотном техническом проектировании системы и точной синхронизации приемников, например с помощью систем GPS, позволяет добиться высокой точности с погрешностью до 0,5°. Так же за счет увеличения вычислительных мощностей увеличивается и количество одновременно отслеживаемых сигналов.

Корреляционно-интерферометрический метод – наиболее совершенная и устойчивая к помехам технология. Использует анализ корреляционных матриц сигналов, приходящих на множество антенн. Обеспечивает погрешность менее 1°, при этом имеет возможность отслеживать множество устройств одновременно. Так же данный метод эффективно работает на куда большем диапазоне частот по сравнению с другими методами пеленгации [4].

Таким образом интерферометрический и временной методы обладают наибольшей точностью, помехоустойчивостью и пригодностью для построения полноценных систем позиционирования.

Фазовый метод обеспечивает хорошую точность, но требует сложной аппаратурной базы. Амплитудный и доплеровский методы пригодны скорее для вспомогательных задач.

Таким образом, для промышленных объектов целесообразно использовать комбинацию TDoA и интерферометрии, что позволяет одновременно определять координаты источника и уточнять пеленг с долей градуса. Итоговое сравнение всех видов пеленгации представлены в таблице 1.

Таблица 1

Сравнение методов пеленгации

	Амплитудная	**Фазовая**	**Доплеровская**	**Временная**	**Интерферометрическая**
Точность пеленгации	Низкая (3°-15°)	Средняя (1°- 5°)	Средняя (1° - 3°)	Высокая (0.5°-2°)	Высокая (<1°)
Техническая сложность	Низкая	Средняя	Высокая	Высокая	Высокая
Требования к вычислительным мощностям	Низкая	Средняя	Средняя	Высокая	Высокая
Одновременное количество отслеживаемых устройств	1-3	1	1-3	Ограничено вычислительными мощностями	Ограничено вычислительными мощностями
Диапазон рабочих частот	СВЧ (1ГГц-30ГГц)	УВЧ, СВЧ (3МГц-300ГГц)	УВЧ, СВЧ (30МГц – 3ГГц)	СВЧ (0.5 - 6 ГГц)	СЧ, ВЧ, СВЧ, УВЧ (10МГц-300ГГц)

Рекомендации по построению системы пеленгации на производственном объекте. На основе анализа методов предлагается следующая архитектура пеленгационной системы:

Для уверенного определения координат в трехмерном пространстве достаточно 4–6 стационарных станций, размещенных по периметру объекта или на ключевых высотных точках. Такая конфигурация обеспечивает устранение неоднозначности направления, высокую точность триангуляции, перекрытие зоны контроля [5].

Оптимальными являются диапазоны частот 2.4 ГГц и 5.8 ГГц, поскольку большинство мобильных устройств и Wi-Fi работают именно на этих частотах; управление БПЛА также осуществляется в этих частотных диапазонах; а также антенны таких пеленгаторов будут компактными, что упростит внедрение на производство [6].

Предложенная система способна обеспечивать анализ кратковременных всплесков радиосигнала, составить классификацию обнаруженных источников, устойчива к многолучевому распространению и вторичным отражениям сигнала, имеет возможность интеграции с СКУД и системами видеонаблюдения.

Заключение. Пассивная радиопеленгация представляет собой перспективный и технологически оправданный инструмент повышения безопасности контролируемых зон крупных промышленных объектов.

Использование комбинации методов временной разности прихода сигнала и корреляционной интерферометрии позволяет обеспечить высокую точность определения местоположения источников

радиоизлучения, отслеживание перемещения персонала и техники, а также обнаружение несанкционированной активности.

Рекомендованная архитектура системы пеленгации обеспечивает непрерывный мониторинг территории и может служить основой для создания комплексного интеллектуального контура безопасности.

Список использованных источников:

1. Современная электроника и технологии автоматизации: сайт. – URL: https://www.cta.ru/ (дата обращения: 17.11.2025).

2. Алексеев М. В., Молоканов А. А. Фазовый метод радиопеленгации // Форум молодых ученых. – 2019. – №12 (40). – С. 23-26.

3. Кафедра радиотехнических и телекоммуникационных систем: офиц. сайт. – URL: https://rts.sfedu.ru/ (дата обращения: 5.12.2025).

4. Ашихмин А. В., Крыжко И. Б., Токарев А. Б., Фатеев А. А. Сравнение характеристик корреляционно-интерферометрического пеленгатора при использовании направленных и ненаправленных антенных элементов // Вестник ВГТУ. – 2021. – №5. – С. 59-69.

5. Тихомиров А. В., Иванов М. С., Омельянчук Е. В. Разработка акустического пеленгатора // Национальный исследовательский университет «Московский институт электронной техники». – 2016. – №90. – С. 1-13.

6. Информационное агентство ТАСС: офиц. сайт. – URL: https://tass.ru/ (дата обращения: 8.12.2025).

Saulyak Andrey Fedorovich
Northern (Arctic) Federal University, Arkhangelsk

Scientific supervisor:
Zybarev Aleksandr Andreevich
Northern (Arctic) Federal University, Arkhangelsk

METHODS FOR PROTECTING A CONTROLLED ZONE USING DIRECTION FINDING

Abstract. This article provides comparative characteristics of the most common radio direction finding methods, assesses their effectiveness for industrial facilities, and provides recommendations for building an enterprise security system using direction finding methods.

Keywords: radio direction finding, TDoA, correlation interferometry, enterprise security, information security.

УДК 004

Хакимов А.И.
Уфимский университет науки и технологий, Уфа

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

УЯЗВИМОСТИ ПРОТОКОЛА BLUETOOTH LOW ENERGY (BLE) В СИСТЕМАХ УМНОГО ДОМА И МЕТОДЫ ИХ НЕЙТРАЛИЗАЦИИ

Аннотация. В статье анализируются актуальные угрозы безопасности протокола Bluetooth Low Energy (BLE) в экосистемах «умного дома». Проведен разбор типовых уязвимостей на этапах сопряжения, передачи данных и аутентификации. Особое внимание уделено атакам типа «человек посередине», повторного воспроизведения и перехвата трафика. На основе выявленных рисков предложен комплекс мер. Обоснована необходимость перехода от реактивной защиты к проактивному мониторингу BLE-активности в потребительских IoT-сетях.

Ключевые слова: Bluetooth Low Energy, умный дом, IoT-устройства, киберугрозы, аутентификация, шифрование, LE Secure Connections.

В эпоху цифровой трансформации технологии интернета вещей (IoT) стали неотъемлемой частью повседневной жизни. Особую популярность приобрели системы «умного дома», где протокол Bluetooth Low Energy (BLE) выступает одним из ключевых стандартов беспроводной связи благодаря низкому энергопотреблению, широкой совместимости и простоте интеграции. По данным аналитических агентств, к 2025 г. количество BLE-устройств в потребительском секторе превысит 5 млрд единиц [1]. Однако массовое внедрение таких решений сопровождается экспоненциальным ростом поверхности атаки. Многие производители умных датчиков, замков, термостатов и камер приоритизируют удобство развертывания и стоимость в ущерб безопасности, оставляя в протоколе и прошивках критические уязвимости.

Архитектура BLE, несмотря на наличие встроенных механизмов криптографической защиты, содержит ряд проектных и реализационных недостатков. Анализ уязвимостей целесообразно разделить на три этапа жизненного цикла BLE-соединения: обнаружение и реклама, сопряжение

и установление защищенного канала, эксплуатация канала передачи данных.

На этапе трансляции служебных сигналов (advertising) устройства рассылают пакеты с идентификаторами (MAC-адресами, UUID сервисов) в открытом виде. Это позволяет злоумышленникам проводить пассивное отслеживание и составлять профили поведения пользователей. Многие бюджетные IoT-устройства используют статические MAC-адреса, что критически снижает уровень конфиденциальности.

Процесс сопряжения BLE исторически оставался слабым звеном. До внедрения спецификации Bluetooth 4.2 широко использовался режим Just Works, не обеспечивающий взаимную аутентификацию и защищающий только от пассивного прослушивания. Это открывает возможность для реализации атак типа «человек посередине». Даже при использовании кода подтверждения злоумышленники применяют методы понижения энтропии или эксплойты уязвимостей KNOB (Key Negotiation of Bluetooth), позволяющие согласовать минимально допустимую длину ключа шифрования, что делает его подбор вычислительно тривиальной задачей.

В канале передачи данных угрозы включают перехват и модификацию команд управления. Исследователями задокументированы атаки типа BIAS (Bluetooth Impersonation Attacks), позволяющие выдавать себя за доверенное устройство без знания долгосрочных ключей шифрования. Также актуальны атаки повторного воспроизведения (replay attacks), когда злоумышленник перехватывает легитимную команду (например, сигнал на открытие замка) и транслирует ее повторно. Уязвимости в реализации GATT-сервисов (Generic Attribute Profile — профиль атрибутов общего назначения) часто приводят к несанкционированному чтению или записи характеристик без должной проверки прав доступа и валидации сессии.

Для нейтрализации перечисленных угроз необходим многоуровневый подход. Предлагаются следующие ключевые меры защиты:

1. Криптографическая модернизация сопряжения с использованием LE Secure Connections и Out-of-Band аутентификации;
2. Сегментация и изоляция BLE-трафика в логически обособленных сетевых сегментах;
3. Внедрение механизма приватных адресов (Private Resolvable Addresses) для защиты от отслеживания;
4. Мониторинг и поведенческий анализ BLE-активности с интеграцией в SIEM-системы;
5. Организационные меры: политики Secure by Design, регулярный аудит прошивок, обучение пользователей.

Рассмотрим каждую меру подробнее. Для нейтрализации перечисленных угроз необходим многоуровневый подход, сочетающий модернизацию протоколов, архитектурную изоляцию и внедрение политик безопасной разработки. В первую очередь, обязательным стандартом для новых устройств должно стать использование LE Secure Connections, основанного на алгоритме эллиптических кривых ECDH P-256, что обеспечивает взаимную аутентификацию и генерацию стойких сеансовых ключей, устойчивых к атакам понижения энтропии [2]. Для критически важных узлов инфраструктуры (умных замков, медицинских датчиков) целесообразно дополнить эту схему аутентификацией Out-of-Band (OOB) через NFC, QR-коды или аппаратные токены, что полностью исключает перехват ключей сопряжения по радиоканалу. Одновременно с криптографическим усилением требуется архитектурная сегментация: BLE-шлюзы и хабы умного дома должны функционировать в логически обособленных сетевых сегментах (VLAN), изолированных от основной корпоративной инфраструктуры [3]. Взаимодействие с облачными сервисами следует выстраивать исключительно по зашифрованным каналам со строгой проверкой сертификатов и принципом минимальных привилегий (Zero Trust). Для защиты от пассивного отслеживания и подмены устройств необходимо внедрять механизм приватных адресов (Private Resolvable Addresses), при котором MAC-адрес в транслируемых пакетах регулярно меняется [4], а разрешение возможно только для сопряженных узлов с ключом Identity Resolving Key (IRK). Непрерывный контроль за BLE-активностью обеспечивается интеграцией шлюзов с системами мониторинга безопасности и легковесными системами обнаружения вторжений, адаптированными под BLE-стек, что позволяет в реальном времени выявлять аномалии, такие как нестандартные интервалы подключения, попытки множественных сопряжений и фаззинг сервисов [5]. Наконец, устойчивость экосистемы зависит от организационных мер: производители обязаны внедрять политики Secure by Design на этапе проектирования, проводить статический и динамический анализ прошивок и гарантировать поддержку обновлений не менее 5 лет [6], в то время как пользователям рекомендуется отключать неиспользуемые сервисы, использовать сложные PIN-коды и своевременно обновлять микропрограммное обеспечение.

Протокол Bluetooth Low Energy остается фундаментом экосистемы умного дома, однако его безопасность напрямую зависит от корректности реализации спецификаций и осознанности производителей. Переход от устаревших методов сопряжения к LE Secure Connections, внедрение приватных адресов и сегментация сетей позволяют нейтрализовать большинство известных векторов атак. В перспективе требуется разработка единых стандартов обязательной сертификации BLE-

устройств для потребительского рынка. Только комплексный подход, объединяющий криптографическую стойкость, архитектурную изоляцию и непрерывный мониторинг, способен обеспечить доверенную среду для умных устройств.

Список использованных источников:

1. State of IoT 2024: Number of connected IoT devices growing 13% to 18.8 billion globally // IoT Analytics: [сайт]. URL: https://iot-analytics.com/number-connected-iot-devices/.

2. Шаньгин, В. Ф. Комплексная защита информации в корпоративных системах: учебное пособие / В. Ф. Шаньгин. – М.: ИД ФОРУМ, НИЦ ИНФРА-М, 2013. – 592 с. – ISBN 978-5-8199-0456-7.

3. Гришина, Н. В. Организация комплексной системы защиты информации: учебное пособие / Н. В. Гришина. – М.: МГУЛ, 2015. – 218 с. – ISBN 978-5-8135-0712-3.

4. Bluetooth Core Specification. Version 5.4 [Электронный ресурс] // Bluetooth SIG: [сайт]. URL: https://www.bluetooth.com/specifications/specs/core-specification-5-4/.

5. Якупова И.Р. Проблемы безопасности IoT-устройств и направления защиты интернета вещей // Информационные технологии обеспечения комплексной безопасности в цифровом обществе. 2025. С. 213–216.

6. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» [Электронный ресурс] // КонсультантПлюс. URL: https://www.consultant.ru/document/cons_doc_LAW_220885/.

Khakimov.A.I.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Fatkhelislamov A.F.
Ufa University of Science and Technology, Ufa

VULNERABILITIES OF THE BLUETOOTH LOW ENERGY (BLE) PROTOCOL IN SMART HOME SYSTEMS AND METHODS FOR THEIR NEUTRALIZATION

Abstract. The article examines current information security threats associated with the use of the Bluetooth Low Energy (BLE) protocol in smart home ecosystems. An analysis of typical vulnerabilities at the stages of pairing, data transmission, and device authentication is carried out. Particular attention

is paid to man-in-the-middle, replay, and traffic interception attacks. Based on the identified risks, a set of technical and organizational measures for threat neutralization is proposed, including the implementation of LE Secure Connections, network segmentation, Out-of-Band authentication, and regular firmware audits. The study results demonstrate the need to transition from reactive protection to proactive BLE traffic monitoring in consumer IoT ecosystems.

Keywords: Bluetooth Low Energy, smart home, information security, IoT devices, cyber threats, authentication, encryption, LE Secure Connections.

УДК 004

Чернышев К.В.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Сенцова А.Ю.
Уфимский университет науки и технологий, Уфа

УГРОЗЫ НАРУШЕНИЯ ИЗОЛЯЦИИ КОНТЕЙНЕРОВ В СОВРЕМЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

Аннотация. Контейнеризация приложений на сегодняшний день стала доминирующей технологией развертывания программных систем, однако механизмы изоляции контейнеров содержат критические уязвимости, эксплуатация которых позволяет злоумышленникам получить доступ к атакующему узлу. В работе рассматриваются актуальные векторы атак, приводящие к нарушению изоляции контейнеров, включая уязвимости ядра Linux, небезопасные конфигурации среды выполнения и проблемы разграничения привилегий. Предложены практические меры защиты, основанные на многоуровневой модели безопасности и применении специализированных инструментов управления доступом.

Ключевые слова: контейнеризация, изоляция процессов, уязвимости, Docker, привилегии, Linux

Контейнеры Linux строятся на комбинации пространств имен, контрольных групп и возможностей ядра – механизмов, изначально не предназначавшихся для создания жестких границ безопасности. Это фундаментальное противоречие между назначением технологии и ее практическим применением порождает проблемы, которые являются причиной появления уязвимостей, связанных с нарушением границ безопасности или нарушением изоляции контейнеров [1].

Пространства имен изолируют представление контейнера о системных ресурсах, процессах, сетевых интерфейсах, точках монтирования. Однако все процессы в конечном счете выполняются в едином ядре хост-системы, разделяя критические структуры данных.

Каждое системное обращение из контейнера обрабатывается ядром хоста. Уязвимость в коде ядра, обрабатывающем такой вызов, открывает прямой путь к компрометации всей системы.

Чтобы решить вышеизложенные проблемы, крупные облачные провайдеры применяют дополнительные слои изоляции – виртуализацию на уровне гипервизора для критичных рабочих нагрузок. Но в корпоративном секторе, где контейнеры развертываются непосредственно на физических серверах или в слабо защищенных виртуальных машинах, риски возрастают многократно.

Привилегированный режим контейнера отключает практически все механизмы изоляции, предоставляя процессам внутри контейнера полный доступ к устройствам хост-системы. Иногда это техническая необходимость – контейнеру требуется доступ к аппаратному обеспечению для выполнения своих функций. В большинстве же случаев речь идет о некомпетентности или спешке, где привилегированный режим решает проблемы с правами доступа.

Монтирование Docker-сокета внутрь контейнера – еще одна распространенная ошибка. Файл /var/run/docker.sock предоставляет полный контроль над демоном Docker, включая возможность запуска новых контейнеров с произвольными параметрами. Процесс внутри контейнера, получивший доступ к этому сокету, способен запустить привилегированный контейнер с примонтированной корневой файловой системой хоста – по сути, получив root-доступ обходным путем.

Неправильная конфигурация профилей, контролирующих доступные системные вызовы, расширяет поверхность атаки. По умолчанию Docker блокирует около 44 потенциально опасных системных вызовов из примерно 300 доступных в современных ядрах Linux. Отключение seccomp или использование профиля с большим количеством разрешений открывает доступ к вызовам, эксплуатация которых может привести к повышению привилегий [2].

Ядро Linux – единая точка отказа для всех контейнеров на хосте. Временной промежуток между публикацией информации об уязвимости и установкой обновлений на системах контейнеризации составляет в среднем 23-43 дня. В контейнерной среде это означает, что злоумышленник располагает месяцем для эксплуатации известной уязвимости ядра [3].

Среды выполнения контейнеров такие как, containerd, CRI-O, runc сами содержат уязвимости. Уязвимость CVE-2024-21626 в runc позволяла

злоумышленнику через специально подготовленный образ контейнера записать файл в произвольное расположение на хосте в процессе создания контейнера [4]. Уязвимость критична, поскольку runc используется практически всеми популярными контейнерными платформами как низкоуровневая среда выполнения.

Минимизация поверхностной атаки начинается на этапе проектирования. Принцип наименьших привилегий требует, чтобы контейнер получал только строго необходимые capabilities, а не все по умолчанию или, тем более, привилегированный режим. Большинство приложений функционируют нормально вообще без дополнительных capabilities – достаточно правильно настроить права доступа к файлам и использовать непривилегированного пользователя внутри контейнера.

Мониторинг безопасности через инструменты Falco позволяет обнаруживать подозрительную активность внутри контейнеров в реальном времени, попытки обращения к критичным файлам хоста, подозрительные системные вызовы, сетевые соединения к неожиданным адресатам. Согласно статистике, данные по ряду российских организаций пока недостаточны для однозначного вывода об эффективности этого подхода, многие внедрения ограничиваются сбором логов без реакции на инциденты [5].

Технология gVisor от Google предлагает радикальное решение, замену прямых системных вызовов к ядру хоста на вызовы к user-space ядру, реализующему значительную часть функциональности Linux в изолированном процессе. Это сокращает поверхность атаки – уязвимость в gVisor не дает прямого доступа к ядру хоста.

Важность регулярного обновления компонентов невозможно переоценить. Ядро хоста, среда выполнения контейнеров, образы приложений – каждый компонент должен своевременно получать обновления безопасности.

Наиболее критичные приложения выполняются в изолированных кластерах с усиленными мерами безопасности, обычные бизнес-приложения – в отдельной среде с базовыми настройками защиты. Это требует дополнительных инфраструктурных затрат, но радикально снижает последствия возможной компрометации.

Заключение

Угрозы нарушения изоляции контейнеров представляют собой системную проблему, корни которой лежат в архитектурных особенностях технологии контейнеризации. Механизмы изоляции, построенные на namespaces, cgroups и capabilities, не обеспечивают того уровня разделения, который необходим для размещения приложений с разными уровнями доверия на общей инфраструктуре.

Особую тревогу вызывает высокая распространенность небезопасных конфигураций, привилегированные контейнеры, избыточные capabilities, отсутствие регулярного обновления компонентов.

Защита требует многоуровневого подхода. Технические меры – применение минимальных привилегий, мониторинг безопасности в реальном времени, использование расширенных средств изоляции вроде gVisor должна дополняться процессными изменениями, регулярным аудитом безопасности конфигураций, автоматизацией применения обновлений.

Перспективным направлением развития представляется дальнейшая эволюция технологий изоляции. Появление в ядре Linux новых механизмов безопасности, таких как Landlock LSM, открывает возможности для более тонкой настройки изоляции без избыточных накладных расходов. Развитие аппаратных средств защиты в современных процессорах также может усилить границы изоляции на аппаратном уровне.

Дальнейшие исследования должны сосредоточиться на разработке автоматизированных инструментов оценки безопасности конфигураций и методик количественной оценки рисков в контейнерных средах.

Список использованных источников:

1. Контейнеры и Docker, обзор, первые шаги и примеры [Электронный ресурс]. URL: https://ipsoftware.ru/posts-cloud/docker-start-1/ (дата обращения: 01.04.2026).

2. Профили безопасности Seccomp для Docker [Электронный ресурс]. URL: https://docs.docker.com/engine/security/seccomp/ (дата обращения: 12.04.2026).

3. Окно в несколько недель, как CVE фикс доходит до контейнера [Электронный ресурс]. URL: https://clck.ru/3TAvaJ (дата обращения: 18.04.2026).

4. Уязвимость runc (CVE-2024-21626) [Электронный ресурс]. URL: https://redos.red-soft.ru/support/secure/uyazvimosti/uyazvimost-runc-cve-2024-21626/ (дата обращения: 29.03.2026).

5. Разбор инцидентов в российских компаниях [Электронный ресурс]. URL: https://habr.com/ru/companies/securitm/articles/986954/ (дата обращения: 12.04.2026).

Chernyshev K.V.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Sentsova A.Yu.
Ufa University of Science and Technology, Ufa

THREATS OF VIOLATION OF CONTAINER ISOLATION IN MODERN INFORMATION SYSTEMS

Abstract. Application containerization has become the dominant technology for deploying software systems today. However, container isolation mechanisms contain critical vulnerabilities that, when exploited, allow attackers to gain access to the attacking node. This paper examines current attack vectors that lead to violation of container isolation, including Linux kernel vulnerabilities, insecure runtime configurations, and privilege differentiation issues. Practical protective measures based on a multi-layered security model and the use of specialized access control tools are proposed.

Keywords: containerization, process isolation, vulnerabilities, Docker, privileges, Linux

СЕКЦИЯ 5. СОВРЕМЕННЫЕ ВЫЗОВЫ В ОБЛАСТИ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

УДК 004

Аетбаева Р.Г.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Сенцова А.Ю.
Уфимский университет науки и технологий, Уфа

ПРОТИВОДЕЙСТВИЕ АТАКАМ НА ПРОТОКОЛ SPANNING TREE С ИСПОЛЬЗОВАНИЕМ ROOT GUARD И BPDU GUARD В КОРПОРАТИВНЫХ СЕТЯХ

Аннотация. Исследование демонстрирует риски атак на STP и способы их нейтрализации. Практическая часть выполнена в симуляторе сети передачи данных Cisco Packet Tracer: смоделирована корпоративная сеть, смоделированы атаки, протестирована работа механизмов защиты BPDU Guard и Root Guard.

Ключевые слова: STP, безопасность канального уровня, BPDU Guard, Root Guard, сетевые атаки, Cisco Packet Tracer, моделирование, защита коммутируемых сетей.

Spanning Tree Protocol (STP) является фундаментальным механизмом обеспечения отказоустойчивости в коммутируемых сетях Ethernet. Он устраняет петли и создает резервные пути передачи данных. Однако уязвимости протокола могут быть использованы злоумышленниками для проведения атак на сеть компании.

Атаки на канальном уровне особенно опасны, так как традиционные средства защиты (МСЭ, системы обнаружения вторжений) не контролируют трафик внутри коммутируемого сегмента. Успешная атака на сеть, коммутируемую с помощью протокола STP, способна: изменить топологию сети, привести к перехвату трафика, широковещательным штормам и полному отказу инфраструктуры.

Цель данной работы – проанализировать уязвимости STP, смоделировать типовые атаки в Cisco Packet Tracer и оценить эффективность механизмов защиты BPDU Guard и Root Guard.

Тестовая топология сети (рис. 1) соответствует стандартной иерархической модели и включает три уровня: ядро, уровень распределения и уровень доступа.

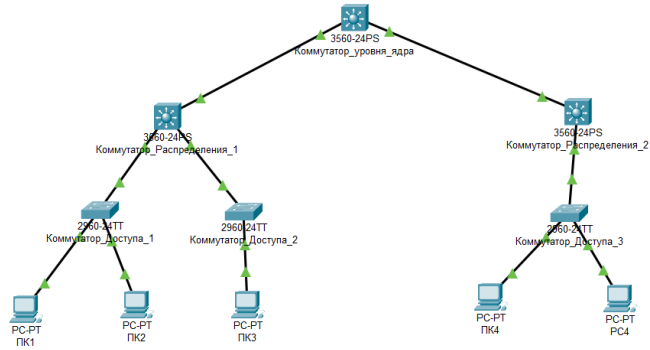


Рис.1. Топология сети

На всех устройствах созданы VLAN 10 (USERS) и 99 (MANAGEMENT), настроены транковые соединения между коммутаторами с разрешением передачи указанных VLAN, а порты доступа клиентов переведены в режим access с назначением в VLAN 10 и активацией PortFast. Установлены приоритеты STP: Коммутатор_уровня_ядра (8192) определен как корневой мост, Коммутатор_Распределения (16384) и Коммутатор_Доступа (32768). Для защиты от атак на канальном уровне на портах доступа включен BPDU Guard, а на downlink-портах коммутаторов распределения настроен Root Guard. Клиентским ПК присвоены статические IP-адреса из подсети 192.168.10.0/24 с шлюзом 192.168.10.1.

Для демонстрации уязвимости STP к порту Fa0/5 Коммутатор_Доступа_1 подключен Коммутатор_Злоумышленника с приоритетом STP 0 для VLAN 10 и 99. На порту коммутатора доступа BPDU Guard отключен. После подключения на корневом коммутаторе выполнена проверка топологии STP (рис. 2). Установлено, что в VLAN 10 и VLAN 99 корневым мостом стал атакующий коммутатор (MAC 0001.645A.52C2). В VLAN 1 корневой мост остался неизменным. Захват корневого моста в пользовательском и управляющем сегментах подтверждает успешность атаки и демонстрирует критическую уязвимость протокола STP при отсутствии защиты.

```
VLAN0010
  Spanning tree enabled protocol rstp
  Root ID    Priority    32778
             Address     0001.645A.52C2
             Cost        23
             Port        26(GigabitEthernet0/2)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32778  (priority 32768 sys-id-ext 10)
             Address     0060.2F44.CA30
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Gi0/1            Desg FWD 4         128.25   P2p
Gi0/2            Root FWD 4         128.26   P2p

VLAN0099
  Spanning tree enabled protocol rstp
  Root ID    Priority    32867
             Address     0001.645A.52C2
             Cost        23
             Port        26(GigabitEthernet0/2)
```

Рис.2. Топология STP на Коммутатор_уровня_ядра

Для проверки эффективности механизма BPDU Guard на порту Fa0/5 коммутатора коммутатора доступа активирована защита: spanning-tree bpduguard enable. После подключения атакующего коммутатора (Коммутатор_Злоумышленника) к порту Fa0/5 сработала защита, о чем свидетельствуют сообщения на консоли (Рис.3).

```
Switch(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/5, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed state to up
%SPANTREE-2-BLOCK_BPDUGUARD: Received BPDU on port FastEthernet0/5 with BPDU Guard enabled.
Disabling port.

%PM-4-ERR_DISABLE: bpduguard error detected on 0/5, putting 0/5 in err-disable state


%LINK-5-CHANGED: Interface FastEthernet0/5, changed state to administratively down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed state to down
```

Рис.3. Сообщения на консоли Коммутатор_доступа_1

Для демонстрации эффективности Root Guard на коммутаторе распределения, на портах которого заранее активирована защита командой spanning-tree guard root, выполнен эксперимент по имитации попытки захвата корневого моста со стороны уровня доступа. Для этого на коммутаторе доступа изменен приоритет STP в VLAN 10 с 32768 на 4096. При попытке стать корневым мостом сработала защита на коммутаторе распределения, о чем свидетельствует сообщение на консоли (Рис. 4).

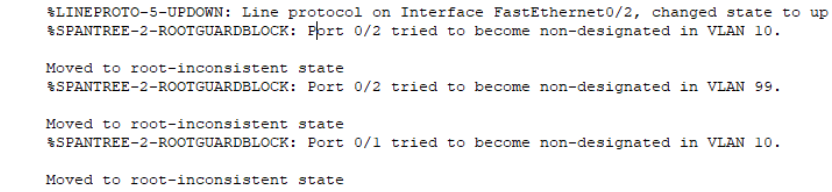


Рис.4. Сообщение на консоли Коммутатор_Распределения_1

В работе проведен анализ уязвимостей и исследование методов защиты в Cisco Packet Tracer от атак, для реализации которых могут быть использованы уязвимости протокола STP. Подтверждена возможность захвата корневого моста при отсутствии защиты. Показано, что BPDU Guard эффективно блокирует подключение Коммутатора_Злоумышленника, а Root Guard предотвращает попытки захвата корневого моста.

Список использованных источников:

1 Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы [Электронный ресурс]: учебник для вузов. – 6-е изд. – СПб.: Питер, 2021. – 1008 с. – Режим доступа: https://psv4.userapi.com/s/v1/d/8b7Y8EQmaD8vA6I3jWBVz2fNNfxOt3ZrJJoZ-qT0YdizDVrRSDbYJdbHZOBCej6WOzCHp1LaRJzxku9con3kSEq0_GaL7XXG14NT2JWahH0odErJ/Kompyuternye_seti_Printsipy_tekhnologii_protokoly_Yubileynoe_izdanie_dop_i_ispr.pdf (дата обращения: 18.03.2026).

2. Таненбаум Э., Уэзеролл Д. Компьютерные сети [Электронный ресурс] / пер. с англ. – 6-е изд. – СПб.: Питер, 2021. – 1905 с. – Режим доступа: https://books.yandex.ru/books/tKspUYe0 (дата обращения: 18.03.2026).

Aetbaeva R.G.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Sentsova A.Yu.
Ufa University of Science and Technology, Ufa

COUNTERING SPANNING TREE PROTOCOL ATTACKS USING ROOT GUARD AND BPDU GUARD IN CORPORATE NETWORKS

Abstract. This study demonstrates the risks of STP attacks and how to neutralize them. The practical part is performed in Cisco Packet Tracer: a

corporate network is simulated, attacks are reproduced, BPDU Guard and Root Guard are tested.

Keywords: STP, data link layer security, BPDU Guard, Root Guard, network attacks, Cisco Packet Tracer, modeling, protection of switched networks.

УДК 004.056

Аетбаева Р.Г.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Яппаров Р.М.
Уфимский университет науки и технологий, Уфа

VPN-СОЕДИНЕНИЕ КАК НАДЕЖНЫЙ КАНАЛ УДАЛЕННОГО ДОСТУПА К КОРПОРАТИВНОЙ СЕТИ

Аннотация. Целью данного исследования является проверка защищенного канала удаленного доступа к корпоративной сети на основе анализа современных угроз и практического применения технологии VPN. Разработка защищенного канала удаленного доступа к корпоративной сети актуальна из-за рисков информационной безопасности и необходимости соблюдения требований законодательства и внутренних политик организации.

Ключевые слова: информационная безопасность, удаленный доступ, VPN, Cisco Packet Tracer, локальная сеть, шифрование, IPsec.

Актуальность удаленной работы и уязвимость данных в незащищенных каналах требуют комплексного подхода к информационной безопасности. Одно из решений – использование технологий VPN и шифрования в продуктах Cisco для защиты конфиденциальности и целостности данных.

Каналы удаленного доступа обеспечивают связь с корпоративной сетью из филиалов или домашних офисов, но передача через публичные сети сопряжена с высокими рисками. Наиболее опасны перехват трафика (атака «Man-in-the-Middle») и несанкционированный доступ [3]. Традиционных методов аутентификации в этих условиях недостаточно, поскольку они не защищают сам канал связи [1].

VPN позволяет создать зашифрованный туннель между устройством сотрудника и корпоративной сетью, гарантируя конфиденциальность, целостность и достоверность данных [4].

Для практической демонстрации в эмуляторе Cisco Packet Tracer разработана модель сети, включающая главный офис (маршрутизатор Cisco 4321, коммутатор 2950-24, сервер, ПК) и удаленного сотрудника (маршрутизатор, ноутбук). Транспортная сеть (Интернет) имитируется коммутатором. На маршрутизаторах настроены статические маршруты для связности.

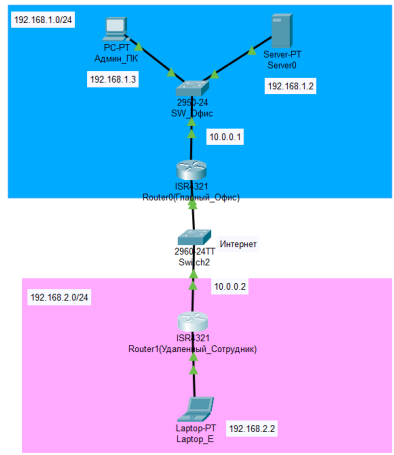


Рис.1. Схема сети

В эксперименте по перехвату трафика в незащищенном канале (ICMP-пакет от ноутбука к серверу) содержимое пакета между маршрутизаторами передавалось в открытом виде, что демонстрирует возможность вмешательства злоумышленника. (Рис.2).

Для защиты на маршрутизаторах настроен VPN на базе IPsec (режим site-to-site). Заданы единые политики: шифрование AES-256, аутентификация SHA, предварительный общий ключ, группа Диффи-Хеллмана DH5. Создан трансформ-набор (ESP с AES-256 и SHA), расширенные списки доступа для трафика туннеля и крипто-карты. После настройки VPN поле данных пакета стало зашифрованным, что подтверждает невозможность прочтения информации при перехвате.

Таким образом, результаты практического моделирования подтверждают, что использование VPN является эффективным и необходимым средством защиты информации при организации удаленного доступа к корпоративным ресурсам.

Использование шифрования позволяет гарантировать конфиденциальность и целостность данных даже при передаче через потенциально опасные публичные сети, что делает VPN неотъемлемым компонентом современных корпоративных информационных систем [2].

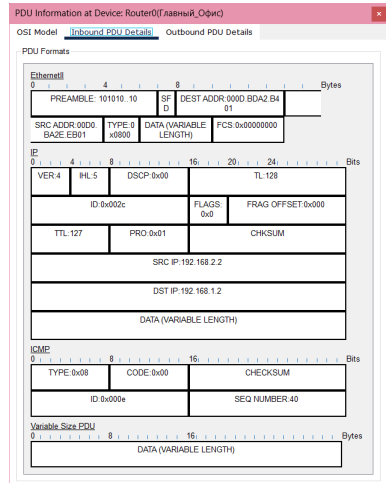


Рис.2. Структура пакета №1

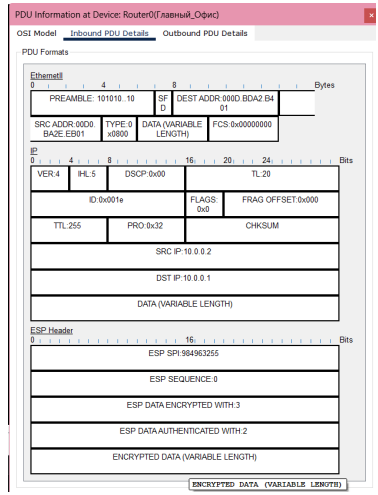


Рис.3. Структура пакета №2

В ходе моделирования использовалась упрощенная топология, не учитывающая многие факторы. Дальнейшее развитие работы может включать усложнение модели за счет добавления дополнительных сегментов сети, внедрения систем обнаружения вторжений (IDS/IPS), а также оценки производительности VPN-соединения при различной интенсивности трафика.

Список использованных источников:

1. Исмагилова, А.С. Алгебраические инструменты для построения криптографических систем / А.С. Исмагилова // Кибернетика и информационная безопасность "КИБ-2025": Сборник научных трудов Третьей Всероссийской научно-технической конференции. В 2-х томах, Москва, 03–04 декабря 2025 года. – Москва: Национальный исследовательский ядерный университет МИФИ, 2025. – С. 114-115. – EDN DDMYVA. – URL: https://elibrary.ru/item.asp?id=88832315/ (дата обращения: 02.04.2026).
2. Иванов, М.А. Криптографические методы защиты информации в компьютерных системах и сетях [Электронный ресурс]. – М.: КУДИЦ-ОБРАЗ, 2022. – 368 с. – URL: https://www.phantastike.com/encryption/kriptograf_metody_zaschity_inform/djvu/view/ (дата обращения: 18.03.2026).
3. Олифер, В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы [Электронный ресурс]: учебник для вузов. – 6-е изд. – СПб.: Питер, 2021. – 1008 с. – URL: https://psv4.userapi.com/s/v1/d/8b7Y8EQmaD8vA6I3jWBVz2fNNfxOt3ZrJJox-qT0YdizDVrRSDbYJdbHZOBCej6WOzCHp1LaRJzxku9con3kSEq0_GaL7XXG14NT2JWahH0odErJ/Kompyuternye_seti_Printsipy_tekhnologii_protokoly_Yubileynoe_izdanie_dop_i_ispr.pdf (дата обращения: 18.03.2026).
4. Таненбаум Э., Уэзеролл Д. Компьютерные сети [Электронный ресурс] / пер. с англ. – 6-е изд. – СПб.: Питер, 2021. – 1905 с. – URL: https://books.yandex.ru/books/tKspUYe0 (дата обращения: 18.03.2026).

Aetbaeva R.G.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Yapparov R.M.
Ufa University of Science and Technology, Ufa

VPN CONNECTION AS A RELIABLE REMOTE ACCESS CHANNEL TO THE CORPORATE NETWORK

Abstract. The purpose of this study is to test a secure remote access channel to a corporate network based on the analysis of modern threats and the practical application of VPN technology. The development of a secure remote access channel to a corporate network is relevant due to the risks of information security and the need to comply with legal requirements and internal policies of the organization.

Keywords: information security, remote access, VPN, Cisco Packet Tracer, local area network, encryption, IPsec.

УДК 004.056

Аминев Б.Р.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Миронова Н.Г.
Уфимский университет науки и технологий, Уфа

OPEN-SOURCE РЕШЕНИЯ И API-ИНТЕРФЕЙСЫ КАК ВЕКТОР ПРОНИКНОВЕНИЯ ВО ВНУТРЕННЮЮ ИНФОРМАЦИОННУЮ СРЕДУ КОМПАНИИ

Аннотация. Рассмотрены актуальные угрозы, связанные с использованием отрытого программного кода и API, в частности, обусловленные расширяющейся практикой применения в разработке ПО генеративных нейросетевых моделей. Рассматриваются направления защиты от этой группы угроз, в том числе на стороне разработчика.

Ключевые слова: кибербезопасность, риски open-source, API.

Современная разработка программного обеспечения зачастую предполагает использование открытых программных компонентов; API как механизм взаимодействия соединяет микросервисы и связывает различные ИТ-системы для обмена данными. Согласно опросу [1] крупнейших российских разработчиков и заказчиков ПО для корпоративного сегмента, 2/3 программной продукции в корпоративном сегменте основаны на открытом исходном коде. При этом open-source решения чаще становятся целью для кибератак и источником рисков. Например, за 2025 год специалисты нашли больше 450 тысяч вредоносных пакетов в отрытом программном обеспечении [2].

По мере роста использования агентных систем на базе ИИ, где API выполняют роль исполнительного уровня, контроль за безопасностью этого уровня усложняется. Автоматизация разработки с помощью генеративного ИИ (почти 90% организаций используют или планируют использовать GenAI для API) создает новые риски, включая безопасность генерируемого кода. Обеспечить безопасность ИИ невозможно без безопасности поддерживающих его API. Согласно исследованию Salt Security [3], почти треть компаний в мире в 2025 г. сталкивалась с ИБ-инцидентами, связанными с безопасностью API, а почти половина

разработчиков (47%) с ИИ-компонентами отложили выпуск приложений именно из-за проблем с безопасностью API [4].

Например, среди актуальных угроз ИБ, связанных с использованием open source-продуктов - атаки на цепочки поставок (через зараженные или специально созданные вредоносные пакеты). Так, еще в 2024 г. «Лаборатория Касперского» зафиксировала порядка 14 тысяч вредоносных пакетов в популярных opensource-хранилищах (наполовину больше, чем годом ранее); эту тенденцию подтверждает и Sonatype, обнаружившая уже в 2025 году более 450 тысяч опасных пакетов. Хакеры либо взламывают аккаунт автора популярной библиотеки, либо создают пакет-двойник с очень похожим именем (typosquatting), либо используют вредоносы для заражения. Например, осенью 2025 г. была зарегистрирована серьезная атака вредоноса Shai-Hulud, который атаковал токены из GitHub, заразив сотни пакетов популярной opensource-библиотеки npm, [5] десятки тысяч репозиториев, приведя к многочисленным утечкам и проч.

Опасность использования open-source решений усугубляется тем, что использующие такое ПО компании годами не обновляют уязвимые open-source библиотеки, потому что разработчики библиотек их забросили и больше не создают обновлений; по данным HeroDevs, библиотеки без поддержки (EOL) до сих пор используются в 5–15% проектов, а в пяти крупных реестрах таких пакетов с известными уязвимостями - 81 тысяча [6]. Из примеров неустраненных разработчиком открытого ПО старых уязвимостей - уязвимость Log4Shell (CVSS 10) в библиотеке Log4j, которую обнаружили еще в 2021 году – но и в 2025 году 40 миллионов загрузок Log4j все еще содержали ту же уязвимость.

Публичные источники об уязвимостях (CVE, NVD) часто бывают неполными, особенно когда речь про open-source. По данным Sonatype, примерно у 65% open-source-уязвимостей, которые получили CVE-идентификатор, вообще нет оценки критичности (CVSS) в базе NVD. А из тех, у кого оценки нет, почти половина (46%) на самом деле заслуживали бы высокой оценки [5]. В среднем уязвимости присваивают оценку CVSS за 41 день. А некоторые дефекты могут тянуться до года. При этом эксплойты (код, который позволяет использовать дыру) появляются в открытом доступе в среднем уже через неделю. А их добавление в реестр NVD занимает еще 15 дней. В итоге возникает «окно возможностей»: уязвимость уже все знают, включая хакеров, а нормальной оценки и патча пока нет.

Проблемой безопасности становится, как отмечено выше, и применение ИИ-агентов в разработке ПО. Около 45% кода от ИИ содержит ошибки из OWASP Top 10, а 20% приложений – опасные ошибки конфигурации. Когда LLM подбирает версии зависимостей, в

27% случаев она рекомендует неверные или несуществующие – прямой путь к dependency confusion. При этом в мире до 90% организаций уже используют или планируют использовать генеративный ИИ при разработке API, то есть проблемы с ИИ и проблемы с API взаимно усугубляются. Если опираться на OWASP API Security Top 10 и российскую практику, можно выделить несколько ключевых рисков. Во-первых, нарушение авторизации объектов (BOLA) – это доступ к чужим данным через подстановку ID, одна из самых частых причин массовых утечек. Во-вторых, нарушение аутентификации – компрометация учетных записей дает хакеру полный контроль над системой. В-третьих, избыточность раскрываемых данных, когда API возвращает лишнюю информацию, вплоть до персональных данных и коммерческой тайны. И в-четвертых, отсутствие ограничения на количество обращений (Rate Limiting), что открывает дорогу DDoS-атакам и перебору API-ключей. Особенно опасно именно перебор API-ключей. Злоумышленники генерируют кучу ключей и перебирают их, как ID-адреса. По отчету Wallarm, 54% компаний хотя бы раз сталкивались с компрометацией API-ключей, а 62% до сих пор не используют многофакторную аутентификацию для доступа к API [6].

По данным Salt Security, 78% атак на API используют методы из OWASP API Top 10, причем, 99% атак исходят от аутентифицированных источников, в т.ч. от вредоносных агентов. Причина – в том, что многие компании разработчики применяют простые схемы аутентификации, которые легко обходят атакующие (например, один статичный API-ключ без срока действия и без двухфакторной аутентификации легко компрометируем). Чтобы контролировать безопасность открытого кода, целесообразно внедрять SCA – автоматическое сканирование, которое сравнивает хеши компонентов с базами уязвимостей; более продвинутый подход – Supply Chain Security (SCS), - состоит в том, чтобы анализировать не сами компоненты, а всю цепочку их поставки (кто написал код, из какого репозитория взяли, как сообщество реагирует на вопросы безопасности, насколько можно доверять компоненту, с учетом его популярности, авторского состава, количества рецензентов) и проч.

Для работы с open-source безопаснее использовать приватный репозиторий – локальное хранилище библиотек, чтобы не зависеть от того, удалит или изменит автор библиотеку в публичном реестре. Стоит фиксировать версии на уровне хешей коммитов, а не мутабельных тегов вроде v1 или latest. Может быть полезным регулярное сканирование зависимости компонентов (инструментами типа Snyk, Dependabot или OWASP Dependency-Check), отслеживание обновлений, новостей об уязвимостях для используемых open-source продуктов.

Что касается API-рисков, то для их снижения разработчику рекомендуется провести инвентаризацию всех API, особенно важно найти «теневые» API, о которых команда безопасности может даже не подозревать. Для генерации API-ключей применять двухфакторную аутентификацию и обязательно ограничивать срок их действия; стоит внедрить инструмент с функцией API Gateway - единую точку входа, контролирующую интенсивность трафика, с ограничением числа запросов к серверу за определенное время, аутентификацию (например, использовать схему с двумя токенами - Access Token и Refresh Token - по OAuth 2.0, чтобы контролировать временное окно, в течение которого токеном могут злоупотребить), применять методы безопасной разработки API (методами DAST, SAST, фаззинга и проч.).

Можно констатировать, что старая модель использования open-source и API не отвечает требованиям безопасности; новые условия требуют постоянной верификации компонентов, зависимостей, каждого API-вызова, что создает значительные сложности.

Список использованных источников:

1. Коммерческий Open Source в России: темпы внедрения и перспективы 2023-2025 / Институт изучения мировых рынков – URL: https://worldmarketstudies.ru/article/kommerceskij-open-source-v-rossii-tempy-vnedrenia-i-perspektivy-2023-2025 (Дата публикации: 18.03.2024).

2. Лаборатория Касперского. Уязвимости в open source: теперь это касается каждого бизнеса [Электронный ресурс]. – 2026. – Режим доступа: https://www.kaspersky.ru/blog/open-source-vulnerabilities-in-ai-era/41635/ (дата обращения: 13.04.2026).

3. Schwake E. The Era of Agentic Security is Here: Key Findings from the 1H 2026 State of AI and API Security Report / salt.security – URL: https://salt.security/blog/the-era-of-agentic-security-is-here-key-findings-from-the-1h-2026-state-of-ai-and-api-security-report (April 8, 2026).

4. Salt Security Research: As AI Agents Outpace Security, Most Organizations Face an Unsecured API Surge / prnewswire.com – URL: https://www.prnewswire.com/news-releases/salt-security-research-as-ai-agents-outpace-security-most-organizations-face-an-unsecured-api-surge-302736506.html (Дата публикации: 8.04.2026).

5. 81,000 Open Source Package Versions Have Known CVEs and No Patch. Here's Why That Number Is Probably Much Higher – URL: https://www.herodevs.com/blog-posts/eol-package-versions-unpatchable-cve-open-source (Дата публикации: 13 марта 2026).

6. Wallarm / Zuplo. 2026 API ThreatStats Report: APIs Are Now the #1 Exploited Attack Surface [Электронный ресурс]. – 2026. – Режим доступа:

https://zuplo.com/blog/wallarm-2026-api-threatstats-api-security (дата обращения: 13.04.2026).

Aminev B.R.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Mironova N.G.
Ufa University of Science and Technology, Ufa

OPEN-SOURCE SOLUTIONS AND API INTERFACES AS A VECTOR OF INTRUSION INTO A COMPANY'S INTERNAL INFORMATION ENVIRONMENT

Abstract. This article examines current threats associated with the use of open source software and APIs, particularly those arising from the growing use of generative neural network models in software development. Defenses against this group of threats are also explored.
Keywords: cybersecurity, open source risks, API.

УДК 004.056

Бурангулов Д.Б.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Миронова Н.Г.
Уфимский университет науки и технологий, г. Уфа

ПОДХОДЫ К ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ОБЛАЧНОГО КОНТЕНТА В ГИБРИДНЫХ ИНФРАСТРУКТУРАХ

Аннотация. В статье выполнен анализ рисков хранения конфиденциальной информации в облаке и обзор современных мер защиты электронных документов, с учетом требований российского законодательства.
Ключевые слова: облачное хранилище, информационная безопасность, персональные данные.

Облачное хранение документов привлекает экономией и удобством: не нужно тратиться на свою IT-инфраструктуру, легко масштабируется, у сотрудников организаций есть оперативный удаленный доступ к рабочим сервисам, документам или рабочим местам и т.д. Оборотной стороной

удобства гибридных сред организаций являются риски утечки персональных данных, коммерческой или служебной тайны, риски потери доступности цифровых средств выполнения рабочих процессов.

Если «традиционная» система защиты дает организации возможность полного контроля над безопасностью локальной информационной инфраструктуры, то часть корпоративной информационной инфраструктуры на ресурсах провайдера облачных услуг размывает зону контроля и предполагает разделение с провайдером услуг ответственности за безопасность. Типовые риски, связанные с использованием облачных сред:

- потеря контроля над данными [1] (организация не всегда может точно определить физическое местоположение и условия обработки информации, круг лиц с доступом);
- возможность несанкционированного доступа со стороны провайдера или третьих лиц, особенно если облачная платформа не прошла сертификацию по требованиям безопасности;
- нарушение требований законодательства (в частности, ФЗ № 152-ФЗ «О персональных данных»), если инфраструктура провайдера находится за пределами территории Российской Федерации;
- зависимость от политики безопасности провайдера облачных услуг и операторов услуг связи (изменение условий оказания услуг, блокировка аккаунта, технические сбои могут привести к временной или полной потере доступа к данным).

Особую опасность представляют облачные сервисы, не сертифицированные в установленном порядке, поскольку в них отсутствуют технические и организационные меры, необходимые для защиты конфиденциальной информации.

Закрывать подобные угрозы для гибридной инфраструктуры целесообразно комплексно, настраивая безопасность по всем фронтам. В России использование облачных хранилищ для конфиденциальной информации опирается на ряд ключевых документов, в числе которых Федеральный закон № 152-ФЗ «О персональных данных», требования ФСТЭК России к информационным системам, работающим с конфиденциальной информацией, НПА о необходимости использовать только сертифицированные средства защиты для определенных категорий информационных систем. Если организация подпадает под действие таких НПА, она должна:

- убедиться, что серверы облачного провайдера находятся на территории Российской Федерации;
- проверить наличие сертификата соответствия информационной системы провайдера требованиям безопасности;

– заключить договор, в котором четко прописаны меры ответственности за утрату или разглашение информации.

Для хранения и работы с конфиденциальными электронными документами во внешних облачных хранилищах и сервисах требуется применять сертифицированные ФСТЭК, ФСБ средства криптографической защиты. Шифрование целесообразно при передаче (через TLS/SSL) и при хранении (на уровне файловой системы или самого приложения); надежный вариант – шифрование на стороне клиента (client-side encryption) – позволяет исключить просмотр провайдером содержимого хранимых на его мощностях данных. Снизить риски несанкционированного доступа позволяют и такие меры защиты как многофакторная аутентификация (например, пароль + одноразовый код или аппаратный токен), применение сертифицированных средств доверенной загрузки, ограничивающих вход в систему только авторизованным пользователям. Для контроля за перемещением конфиденциальной информации и предотвращения ее утечки целесообразно применять DLP-системы. Обязательная часть защиты - журналы учета действий пользователей, фиксирующие операции с конфиденциальными электронными документами (фиксирующие время доступа, тип операции (просмотр, копирование, удаление), IP-адрес и устройство входа, иное). Для отслеживания инцидентов безопасности в реальном времени эффективно применение SIEM-систем. Технические средства защиты дополняются организационными мероприятиями, направленными на обеспечение безопасности конфиденциального контента от угроз. Так, чтобы данные не пропали при сбое облачной инфраструктуры, необходима реализации продуманной политики резервного копирования, для конфиденциальной информации ее резервные копии тоже должны быть зашифрованы и закрыты от несанкционированного доступа [2]. Электронные документы с истекшим сроком хранения подлежат уничтожению на общих основаниях согласно действующим в организации регламентам (в части уничтожения конфиденциальных документов с истекшими сроками хранения) – и т.д.

Облачное хранение конфиденциальных документов возможно только при строгом соблюдении требований российского законодательства и применении комплексных мер защиты. Ключевыми условиями являются: размещение данных на территории РФ, использование сертифицированных информационных систем, криптографическая защита, управление доступом, аудит и участие экспертной комиссии в управлении жизненным циклом документов. Только такой подход позволяет безопасно использовать преимущества облачных технологий без ущерба для информационной безопасности и без нарушения законодательства.

Список использованных источников:

1. Бабаш А. В., Баранова Е. К. Криптографические методы и средства защиты информации: учебник. – М.: КНОРУС, 2024. – 224 с.

2. Экспертиза ценности и отбор в состав Архивного фонда Российской Федерации документов по личному составу: метод. рекомендации / Росархив, ВНИИДАД. – 2-е изд., перераб. и доп. – М., 2022. – 35 с.

Burangulov D.B.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Mironova N.G.
Ufa University of Science and Technology, Ufa

APPROACHES TO ENSURING CLOUD CONTENT SECURITY IN HYBRID INFRASTRUCTURES

Abstract. The article analyzes the risks of storing confidential information in the cloud and reviews modern measures to protect electronic documents, taking into account the requirements of Russian legislation.

Keywords: cloud storage, information security, personal data.

УДК 004:056:004.7.056.4

Войткус И.А.
Белорусский государственный университет информатики и радиоэлектроники, Минск

Научный руководитель:
Белоусова Е.С.
Белорусский государственный университет информатики и радиоэлектроники, Минск

BSUIR OSINT SYSTEM – ИНСТРУМЕНТ ДЛЯ КИБЕРРАЗВЕДКИ

Аннотация. В статье демонстрируется развитие авторского инструмента OSINT разведки, заключающееся в реализации изолированного веб-приложения. Представлены результаты разработки веб-терминала на базе фреймворка FastAPI. Описана внедренная ролевая модель доступа, необходимость которой продиктована как требованиями информационной безопасности, так и аппаратными ограничениями серверов при обработке тяжеловесных биометрических моделей Facenet.

Ключевые слова: кибербразведка, OSINT, FastAPI, ролевая модель доступа, информационный суверенитет, биометрия.

С ростом актуальности различных инструментов для OSINT разведки, растет и риск утечки данных при проведении аудита в локальных сегментах. Поэтому такие системы требуют строгого контроля в области обеспечения сохранения персональных данных. Ранее протестированное решение на базе Telegram-агента [1] обладало критическим недостатком – все запросы оператора, включая отправку фотографии обрабатывались на серверах стороннего сервера, находящихся за территорией государства. В контексте закона о персональных данных Республики Беларусь № 99-З «О защите персональных данных», использование облачных серверов создает критические риски передачи цифрового следа оператора, а также возрастает возможность реализации атак перехвата таких как «Man-in-the-middle».



Рис. 1. Окно авторизации веб-терминала

В рамках данного исследования был усовершенствован инструмент и реализован переход на изолированный веб-терминал. Программное решение «BSUIR OSINT SYSTEM» разработано на языке Python с использованием высокопроизводительного асинхронного фреймворка FastAPI. Данный подход позволил создать систему в изолированном локальном сегменте. База данных субъектов функционирует в виде локального JSON-файла, синхронизируемого с официального API университета. Таким образом, система не отправляет запросы во внешний интернет и база данных хранится локально в периметре инструмента.

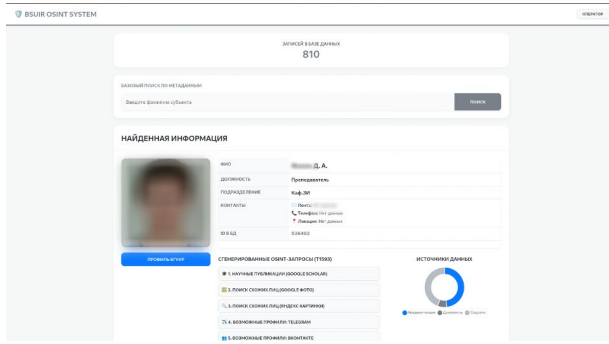


Рис. 2. Панель оператора

Важным этапом при переходе на веб-платформу стал отказ от функционала, который был доступен каждому пользователю, в пользу ролевой модели управления доступом. Введение ролей было обусловлено не только политиками безопасности, но и выявленными аппаратными ограничениями.

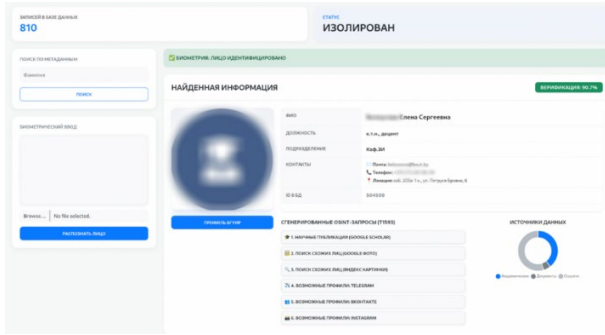


Рис. 3. Панель администратора ИБ

Интеграция в систему модуля биометрии на базе нейросети Facenet показала, что процесс извлечения биометрических векторов требует значительных объемов оперативной памяти и вычислительных мощностей процессора. Для обеспечения более стабильной работы функционал был сегментирован.

Уровень «Оператор» предоставляет доступ только к текстовому поиску по локальной БД. Система генерирует досье, а также данных найденные с использованием Dork-запросов, для дальнейшего ручного анализа.

Уровень «Администратор ИБ» включает в себя модуль биометрической верификации. Данный функционал позволяет загрузить

фотографию субъекта, провести сканирование, при котором происходит сопоставление с эталонным изображением из локальной базы данных.

Система реализует автоматический сбор информации по поисковым запросам из открытых источников, согласно матрице MITRE ATT&CK T1593 [2]. Алгоритм осуществляет транслитерацию кириллических идентификаторов в латиницу и формирует матрицу запросов, используя различные сочетания имени, фамилии и разделители.

Массив полученных данных в дальнейшем может быть использован для решения ряда задач. Во-первых, осуществление оценки риска компрометации конкретного сотрудника. Чем шире область найденной информации, тем уязвимее субъект. Во-вторых, собранные данные могут быть применены для выявления и изъятия из публичного доступа конфиденциальных документов.

Переход к собственному веб-интерфейсу позволил трансформировать инструмент в аналитическую защищенную платформу, а назначение ролевых моделей позволило добиться более стабильной работы.

Список использованных источников:

1. Войткус И.А. Инструмент для OSINT-разведки и реализации техники MITRIE ATTA&CK T1593 / И.А. Войткус, Е.С. Белоусова // Технические средства защиты информации: матер. XXIV Междунар. науч.-техн. конф. (Республика Беларусь, Минск, 08 апреля 2026 года) / редкол.: О. В. Бойправ [и др.]. – Минск: БГУИР, 2026. – С. 342–345.

2. Блэр, Р. Согласование операций безопасности с фреймворком MITRE ATT&CK / Р. Блэр. – Бирмингем: Packt Publishing, 2022. – 268 с. – ISBN 978-1804616697.

Voitkus I.A.
Belarusian State University of
Informatics and Radioelectronics, Minsk
Scientific supervisor:
Belousova E.S.
Belarusian State University
of Informatics and Radioelectronics, Minsk

BSUIR OSINT SYSTEM – AN INSTRUMENT FOR CYBER INTELLIGENCE

Abstract. The article demonstrates the development of the author's OSINT intelligence tool, which consists in the implementation of an isolated web application. The results of the development of a web terminal based on the

FastAPI framework are presented. An embedded role-based access model is described, the need for which is dictated by both information security requirements and hardware limitations of servers when processing heavy-duty Facenet biometric models.

Keywords: cyber intelligence, OSINT, FastAPI, role model of access, information sovereignty, biometrics.

УДК 004.451.042.3

Гизатова Е.А., Насибуллина А.В.
Уфимский университет науки и технологии, Уфа

Научный руководитель:
Исмагилова А.С.
Уфимский университет науки и технологии, Уфа

КИБЕРГРАМОТНОСТЬ: ПОЧЕМУ ОБУЧЕНИЕ СОТРУДНИКОВ – ГЛАВНЫЙ ЩИТ ОТ СОВРЕМЕННЫХ УГРОЗ

Аннотация. В статье обосновывается необходимость перехода от периодических тренингов к непрерывному адаптивному обучению персонала в условиях ИИ-угроз. Предложена модель на базе Zero Trust и поведенческого скоринга, включающая микрообучение, адаптивные сценарии атак, интеграцию в KPI и внутренний аудит. Рассмотрено соответствие требованиям ФСТЭК, ГОСТ Р 57580.1-2017 и 152-ФЗ. Показана экономическая эффективность предложенного подхода.

Ключевые слова: информационная безопасность, социальная инженерия, Zero Trust, адаптивное обучение, поведенческий скоринг, дипфейки, фишинг, микрообучение, риск-менеджмент, KPI

В современном мире, где цифровые технологии пронизывают все сферы жизни и бизнеса, информационная безопасность становится одним из ключевых факторов устойчивого развития и конкурентоспособности. Цифровая трансформация бизнеса и экспансия удаленной работы приводят к постепенному исчезновению классического понятия защищенного периметра. Сотрудники работают из кафе, коворкингов и домашних офисов, используя личные ноутбуки и смартфоны. Поэтому концепция Zero Trust, предполагающая исходное недоверие к любому пользователю, устройству или процессу, независимо от их местоположения в сети, становится ведущей концептуальной моделью построения системы кибербезопасности [1]. А также выдвигает на первый план не только техническую составляющую защиты системы, но и самое труднопрогнозируемое ее звено – человеческий фактор, который согласно

отчетам Verizon DBIR за 2023–2024 гг., фигурировал в 68% инцидентов, связанных с компрометацией данных [2].

Однако именно здесь обнаруживается концептуальный разрыв: современные технологии ИИ обеспечивают злоумышленникам возможность генерировать персонализированные фишинговые письма без грамматических ошибок, а также создавать голосовые и видео дипфейки высокого качества [3], тогда как подходы к обучению персонала в большинстве организаций остаются статичными, ежегодными и не успевают за скоростью мутации векторов атак. Цель данного исследования – обосновать необходимость перехода от периодических тренингов к модели непрерывного адаптивного обучения и предложить ее архитектурную интеграцию в риск-менеджмент организации.

Традиционная модель обучения ИБ строится на допущении, что определенный объем знаний, переданный сотруднику раз в год или раз в квартал, формирует у него устойчивый навык распознавания угроз. Однако ландшафт угроз меняется с беспрецедентной скоростью. Если пять лет назад основным вектором социальной инженерии оставались массовые фишинговые рассылки с шаблонными текстами, то сегодня злоумышленники оперируют инструментарием, сопоставимым по сложности с корпоративными ИИ-решениями. Генеративные языковые модели позволяют создавать персонализированные сообщения, учитывающие должность, контекст деловой переписки и даже стилистику общения конкретного руководителя.

Параллельно развиваются технологии синтеза голоса и видеоизображения: дипфейки перестали быть экспериментальной разработкой и превратились в рабочий инструмент мошенников, способных имитировать голос генерального директора в телефонном звонке [4].

В этих условиях статичный тренинг, разработанный даже год назад, безнадежно устаревает, а сотрудник оказывается безоружным перед гладким, стилистически безупречным текстом, сгенерированным нейросетью. Поэтому принципиальное отличие предлагаемого метода заключается в отказе от единой для всех программы в пользу концепции поведенческого скоринга, заимствованной из арсенала кредитных организаций, но переосмысленной применительно к кибербезопасности.

Каждый сотрудник организации, независимо от должности, генерирует цифровые следы, которые могут быть проанализированы с точки зрения рискованности его поведения: реагирует ли он на имитационные фишинговые рассылки, блокирует ли экран при выходе с рабочего места, подключает ли неавторизованные устройства, соблюдает ли политику использования съемных носителей. Совокупность таких данных позволяет формировать динамический индекс риск-профиля,

который, во-первых, определяет частоту и содержание обучающих интервенций, а во-вторых, может быть интегрирован в архитектуру Zero Trust как один из параметров принятия решений о предоставлении доступа [5].

Предлагаемая модель помимо поведенческого скоринга будет базироваться еще на трех компонентах:

1. Микрообучение, встроенное в рабочий процесс. Вместо того, чтобы один раз в году отрывать сотрудника от работы на длительное централизованное обучение, предлагается реализовать обучение через короткие модули по 5-7 минут, предъявляемые в нужный момент. Например, после того как система зафиксировала переход пользователя по подозрительной ссылке в учебной симуляции, ему немедленно предлагается целевой модуль, разбирающий именно этот тип угрозы, а не общий курс по парольной политике. Такая синхронизация обучения с реальными поведенческими инцидентами серьезно повышает усвоение материала.

2. Адаптивность сценариев. Имитация атак будет персонализироваться под должность и актуальный вектор. Например, для бугалтерии будут моделироваться атаки с подменой реквизитов и симуляцией дипфейк-звонков; для разработчиков – атаки через зараженные пакеты кода.

3. Интеграция в KPI. Индекс осведомленности сотрудника должен стать частью аттестационных метрик, наряду с производственными показателями. Это переводит обучение из плоскости формального требования в плоскость деловой репутации и карьерных последствий, что создает устойчивую внутреннюю мотивацию.

4. Внутренний аудит. Необходимо включить агрегированный индекс осведомленности персонала в систему риск-менеджмента как ключевого индикатора риска. Внутренний аудит должен проверять не факт прохождения курса, а динамику снижения доли сотрудников, совершивших целевое действие в ответ на симулированную атаку. Именно этот показатель характеризует реальный уровень защищенности организации.

Нормативная база, регулирующая вопросы подготовки кадров в области информационной безопасности, косвенно, но все настойчивее подталкивает к внедрению именно таких моделей. Требования ФСТЭК России к защите значимых объектов критической информационной инфраструктуры, обновленные в последние три года, фиксируют необходимость поддержания квалификации персонала, актуальной меняющимся угрозам [6]. ГОСТ Р 57580.1-2017, регулирующий безопасность финансовых организаций, прямо предписывает регулярную оценку осведомленности работников [4]. Федеральный закон № 152-ФЗ

обязывает операторов персональных данных проводить ознакомление сотрудников с политиками обработки, но в современной правоприменительной практике регулятор все чаще интерпретирует это как требование к оценке реальных поведенческих навыков, а не к формальной подписи в журнале инструктажа [5]. Таким образом, переход к непрерывному адаптивному обучению – это не просто передовая практика, но и способ снижения регуляторного риска.

Экономический аргумент также заслуживает отдельного внимания. Стоимость одного часа тренинга, даже самого высокотехнологичного, несоизмерима с потенциальными убытками от успешной атаки, включающими прямые финансовые потери, штрафы регуляторов, затраты на восстановление инфраструктуры и, что часто оказывается самым долгосрочным ущербом, репутационные издержки. При этом модель непрерывного адаптивного обучения позволяет не увеличивать бюджет на безопасность, а перераспределить его: средства, ранее расходовавшиеся на масштабные годовые кампании, направляются на автоматизированные платформы микрообучения и симуляции, стоимость которых в пересчете на одного сотрудника не превышает долей процента от общего бюджета информационной безопасности.

Подводя итог, следует подчеркнуть, что эпоха искусственного интеллекта в руках злоумышленников сделала человеческий фактор не просто слабым звеном, а приоритетной точкой отказа любой системы защиты [3]. Поэтому требуется смена парадигмы: от периодического тренинга как формальной процедуры – к непрерывному адаптивному обучению как динамической системе управления поведенческими рисками, органично встроенной в архитектуру Zero Trust, кадровые процессы и контур риск-менеджмента организации.

Список использованных источников:

1. Rose S., Borchert O., Mitchell S., Connelly S. NIST Special Publication 800-207. Zero Trust Architecture. – Gaithersburg: National Institute of Standards and Technology, 2020. – URL: https://doi.org/10.6028/NIST.SP.800-207 (дата обращения: 15.04.2026). – Текст: электронный.

2. Verizon. 2024 Data Breach Investigations Report. – New York: Verizon, 2024. – URL: https://www.verizon.com/business/dbir/2024/ (дата обращения: 15.04.2026). – Текст: электронный.

3. Brundage M., Avin S., Clark J., Toner H., Eckersley P. et al. The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation. – 2018. – URL: https://arxiv.org/pdf/1802.07228 (дата обращения: 15.04.2026). – Текст: электронный.

4. ГОСТ Р 57580.1-2017. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав

организационных и технических мер. – URL: https://files.stroyinf.ru/Data/648/64887.pdf (дата обращения: 15.04.2026). – Текст: электронный.

5. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных». – URL: https://base.garant.ru/12148567/ (дата обращения: 15.04.2026). – Текст: электронный.

6. Приказ ФСТЭК России от 25.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации». – URL: https://www.consultant.ru/document/cons_doc_LAW_294287/ (дата обращения: 15.04.2026). – Текст: электронный.

Gizatova E.A., Nasibullina A.V.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Ismagilova A.S.
Ufa University of Science and Technology, Ufa

CYBER LITERACY: WHY EMPLOYEE TRAINING IS THE MAIN SHIELD AGAINST MODERN THREATS

Abstract. The article substantiates the need to transition from periodic training to continuous adaptive personnel training under AI-driven threats. A model based on Zero Trust and behavioral scoring is proposed, incorporating microlearning, adaptive attack scenarios, integration with KPIs, and internal audit. Compliance with FSTEC requirements, GOST R 57580.1-2017, and Federal Law No. 152-FZ is reviewed. The economic efficiency of the proposed approach is demonstrated.

Keywords: information security, social engineering, Zero Trust, adaptive training, behavioral scoring, deepfakes, phishing, microlearning, risk management, KPI

УДК 004.056.5

Иванов И.П., Хасанов Р.Р.
Уфимский университет науки и технологий, Уфа

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

СКРЫТАЯ ПЕРЕДАЧА ИНФОРМАЦИИ ПО УЛЬТРАЗВУКОВОМУ АКУСТИЧЕСКОМУ КАНАЛУ

Аннотация. Статья посвящена исследованию ультразвукового акустического канала как средства скрытой передачи информации в контексте угроз информационной безопасности. Рассматриваются физические принципы передачи данных через ультразвуковой диапазон частот, методы модуляции сигнала, а также факторы, влияющие на пропускную способность и скрытность канала. Представлен практический сценарий атаки с использованием кейлоггера на изолированном рабочем месте и смартфона в качестве приемника. Предложен комплекс организационных и технических мер защиты от данного класса угроз.

Ключевые слова: ультразвуковой канал, скрытая передача данных, акустическая стеганография, изолированные системы, кейлоггер.

Обеспечение информационной безопасности сегодня вышло далеко за рамки установки привычных антивирусов и классических межсетевых экранов. Защита сетей от утечек и несанкционированного доступа усложняется с каждым днем, поскольку по мере глобальной цифровизации злоумышленники изобретают все более нетривиальные векторы атак. Стандартные периметры защиты часто оказываются бессильны перед лицом нестандартных угроз. В профессиональной среде сейчас все чаще обсуждают проблему скрытых акустических каналов передачи данных, которые позволяют хакерам незаметно выводить информацию в обход любых программных барьеров.

Особый интерес для атакующих представляет ультразвуковой диапазон – то есть частоты выше 18–20 кГц. Главная технологическая уязвимость здесь кроется в том, что такие звуковые волны абсолютно неразличимы для человеческого уха, однако они прекрасно генерируются и улавливаются самой обыкновенной бытовой электроникой. Для обмена данными злоумышленникам не нужно специальное шпионское оборудование: достаточно стандартных динамиков офисного компьютера и микрофона на смартфоне сотрудника. Это превращает акустический

канал в совершенно реальную угрозу, позволяющую красть конфиденциальные данные даже из тех систем, которые физически отключены от интернета (так называемые air-gapped сети) [1].

С точки зрения физики процесса ультразвук – это механические колебания с частотой, превышающей порог восприятия человека (более 20 кГц). Для организации скрытых каналов на практике обычно применяют ближний ультразвуковой спектр от 17 до 24 кГц. Выбор именно этого коридора продиктован сугубо техническими ограничениями: звуковые карты и микрофоны, которые массово ставятся в потребительскую технику, сохраняют здесь отличную чувствительность. Вредоносный код, попав на компьютер, перехватывает управление аудиоподсистемой и заставляет ее излучать модулированные сигналы. Биты данных кодируются за счет микроизменений параметров несущей частоты. Чаще всего применяется метод частотной манипуляции (FSK), когда нули и единицы «звучат» на разных тонах. Отличным примером служит архитектура атаки SmartAttack, где передача логического нуля осуществляется на частоте 18,5 кГц, а единицы – на 19,5 кГц [2].

Рассмотрим, как подобный вектор реализуется в условиях классического опенспейса. На первом шаге атакующим необходимо доставить вредоносное ПО на изолированный компьютер. Обычно это делается через компрометацию цепочки поставок, подкупленного инсайдера или банальную зараженную флешку. Закрепившись в системе, программа начинает работать как тихий кейлоггер: она без привлечения внимания собирает набираемые тексты, пароли и фрагменты ценных документов. В то же время злоумышленники заражают телефон кого-то из сотрудников офиса, используя фишинговые рассылки или скомпрометированные сайты. Приложение-шпион может запросить доступ к микрофону, но это не обязательно. Как доказали исследователи в рамках проекта GAIROSCOPE, в качестве чувствительного приемника можно использовать гироскоп смартфона, к которому мобильные операционные системы дают доступ без запроса разрешений у пользователя [3]. Как только зараженный телефон физически оказывается неподалеку от ПК жертвы, компьютер начинает транслировать собранные пароли ультразвуком. Смартфон принимает эти неслышимые импульсы, демодулирует их и спокойно пересылает своим создателям через офисный Wi-Fi или сотовую вышку.

Конечно, законы акустики накладывают на этот канал свои ограничения. Пропускная способность и дальность связи напрямую зависят от характеристик аудиоаппаратуры, естественного затухания высоких частот в воздухе, эха в кабинете и фонового гула серверов или кондиционеров. Практические тесты показывают, что устойчивый линк

держится на расстоянии от 6 до 9 метров. Скорости здесь не сравнятся с традиционными сетями: алгоритм SmartAttack выдает до 50 бит/с на дистанции в 6 метров, метод MOSQUITO способен передать до 166 бит/с на трех метрах (но скорость падает до 10 бит/с, если отойти на 9 метров), а использование гироскопа в GAIROSCOPE режет скорость до скромных 1–8 бит/с [4]. Кажется, что это мало, однако для выгрузки текстовиков, ключей шифрования или перехваченных нажатий клавиатуры таких скоростей более чем достаточно. Ситуацию усугубляет и то, что роль приемника может сыграть не только лежащий на столе телефон, но и смарт-часы на запястье работника.

Чтобы устранить риски ультразвуковых утечек, компаниям необходимо выстраивать эшелонированную оборону, где технические методы подкрепляются жестким регламентом. Организационные меры предполагают абсолютный запрет на пронос личных смартфонов, смарт-часов и прочей электроники в помещения, где идет работа с гостайной или критически важной коммерческой информацией. Сами рабочие станции имеет смысл отодвигать от гостевых зон на безопасное расстояние – не менее 8–10 метров. Параллельно необходимо тренировать персонал, объясняя механику подобных экзотических атак, а также вводить строжайший контроль за любыми съемными дисками и патчами, приходящими от вендоров.

С технической стороны действовать нужно еще радикальнее. На критичных узлах аудиоустройства должны быть отключены: в идеале – физически выпаяны динамики и микрофоны, в крайнем случае – принудительно удалены драйверы на уровне операционной системы. В качестве активной защиты зарекомендовали себя системы ультразвукового зашумления. Специальные генераторы постоянно транслируют акустический хаос в диапазоне 18–24 кГц. Они создают мощный шумовой фон, который воздействует на мембрану любого микрофона в радиусе поражения и не дает вредоносному приложению вычленить полезный сигнал из общего гула.

В качестве дополнительного программного слоя можно развернуть ультразвуковые межсетевые экраны. Это специализированные агенты, которые в реальном времени слушают входящий аудиопоток и прерывают его при обнаружении модулированных аномалий. В режимных помещениях не лишним будет установить портативные анализаторы спектра и системы постоянного мониторинга, которые зажгут тревогу при появлении активности в высоких частотах. На аппаратном уровне активно применяются полосовые фильтры: они ставятся прямо на вход аудиовыхода и физически срезают все частоты выше отметки в 17–18 кГц. В операционных системах стоит жестко контролировать эксклюзивный доступ приложений к микрофону,

оповещать пользователя о его включении и настраивать DLP-системы на выявление любых аномалий в работе звуковых драйверов.

Эффективность каждой из этих мер зависит от специфики конкретной инфраструктуры. Для объектов критической информационной инфраструктуры (КИИ) полагаться на какой-то один инструмент нельзя – нужна продуманная комбинация нескольких подходов.

В конечном итоге, несмотря на всю экзотичность и низкий битрейт, акустические каналы передачи остаются вполне рабочим инструментом. Скорости в десятки бит в секунду хватает злоумышленникам для кражи самого ценного: паролей и ключей доступа к защищенным хранилищам. Разобранный выше сценарий с кейлоггером и смартфоном доказывает, что реализовать подобную атаку в типичных офисных реалиях более чем возможно. Безусловно, компрометация сразу двух разных устройств (компьютера и телефона) требует от хакеров высокой квалификации и ресурсов, но техническая база для этого существует уже сегодня. Индустрии кибербезопасности еще только предстоит разработать единые стандарты для оценки уязвимости помещений к ультразвуковым утечкам и внедрить надежные средства их раннего обнаружения.

Список использованных источников:

1. Асяев Г.Д., Антясов И.С. Использование ультразвуковых колебаний для реализации технического канала утечки информации // Вестник УрФО. Безопасность в информационной сфере. 2018. № 29. С. 5–12. URL: https://info-secur.ru/is_29/1_asyaev.pdf (дата обращения 18.04.2026).

2. Guri M. SmartAttack: Air-Gap Attack via Smartwatches URL: https://arxiv.org/pdf/2506.08866 (дата обращения 18.04.2026).

3. Guri M. GAIROSCOPE: Injecting Data from Air-Gapped Computers to Nearby Gyroscopes URL: https://arxiv.org/pdf/2208.09764 (дата обращения 18.04.2026).

4. Guri M., Solewicz Y., Daidakulov A., Elovici Y. MOSQUITO: Covert Ultrasonic Transmissions between Two Air-Gapped Computers using Speaker-to-Speaker Communication URL: https://arxiv.org/pdf/1803.03422 (дата обращения 18.04.2026).

Ivanov I.P., Khasanov R.R.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Shagapov I.A.
Ufa University of Science and Technology, Ufa

COVERT INFORMATION TRANSMISSION VIA ULTRASONIC ACOUSTIC CHANNEL

Abstract. This paper investigates ultrasonic acoustic channels as a medium for covert data transmission within the landscape of modern cybersecurity threats. It examines the underlying physical principles of data transfer via the ultrasonic frequency range, signal modulation techniques, and the key factors influencing channel bandwidth and stealth. A practical attack scenario is presented, demonstrating data exfiltration from an air-gapped workstation using a keylogger and a compromised smartphone as a receiver. Finally, the study proposes a comprehensive set of organizational and technical countermeasures to mitigate this class of threats.

Keywords: ultrasonic channel, covert data transmission, acoustic steganography, air-gapped systems, keylogger.

УДК 004

Ишмухаметов И.Р.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Салов И.В.
Уфимский университет науки и технологий, Уфа

УТЕЧКИ БИОМЕТРИИ ЧЕРЕЗ КОСВЕННЫЕ ДАННЫЕ В ИНТЕРНЕТ ВЕЩЕЙ: АНАЛИЗ КОСВЕННЫХ УГРОЗ

Аннотация. Развитие экосистемы Интернета вещей привело к возникновению нового класса угроз – утечке биометрических данных через косвенные каналы. Умные часы, фитнес-браслеты, домашние ассистенты накапливают паттерны поведения, по которым восстанавливаются физиологические характеристики владельца. Исследование выявляет механизмы непрямого извлечения биометрии из телеметрии IoT-устройств, анализирует актуальные атаки на российские системы умного дома и носимой электроники за 2023–2026 годы. Предложена классификация косвенных биометрических утечек и

комплекс организационно-технических мер, адаптированных к особенностям российской нормативной базы и отечественной элементной базы IoT.

Ключевые слова: Интернет вещей, биометрические данные, косвенные каналы утечки, телеметрия носимых устройств, киберугрозы, информационная безопасность, умный дом.

Российский рынок IoT-устройств за период 2022–2025 годов пережил резкую трансформацию. Фитнес-трекеры фиксируют пульс с точностью до миллисекунды, умные замки запоминают паттерны нажатия, голосовые помощники анализируют тембр и ритм речи.

Проблема заключается в следующем: классические системы защиты биометрии ориентированы на прямые атаки, такие как: перехват отпечатка пальца, фото лица, записи голоса [1]. Косвенные каналы утечки долгое время оставались вне поля зрения. Между тем анализ акселерометра смартфона позволяет восстановить походку человека с достоверностью 94%, а по данным гироскопа умных часов – идентифицировать владельца среди группы из пятидесяти человек [2].

Особенность косвенных утечек в том, что они не требуют взлома защищенных хранилищ [3]. Данные собираются легитимными средствами, часто с согласия пользователя, который не осознает биометрическую природу передаваемой телеметрии. Владелец умных весов соглашается на передачу «обезличенной статистики веса», не зная, что динамика массы тела в сочетании с временными метками формирует уникальный поведенческий профиль.

Технологическая база для косвенного извлечения биометрических признаков сформировалась к 2023 году благодаря двум факторам: увеличению вычислительных мощностей пограничных устройств и развитию алгоритмов машинного обучения. Современный фитнес-браслет генерирует до 200 мегабайт сырых данных в сутки – акселерометр, пульсометр, датчик температуры кожи, SpO_2 , микрофон. Каждый поток сам по себе кажется безобидным, но их комбинация превращается в биометрический паспорт.

Акселерометр фиксирует микровибрации запястья при наборе текста на клавиатуре. Частотный анализ этих колебаний позволяет определить скорость печати, длину пальцев, характерные ошибки и даже восстановить часть вводимого текста. Точность определения пользователя по «клавиатурному почерку», извлеченному из акселерометра умных часов, достигает 87%.

Голосовые ассистенты создают еще более богатую картину. Микрофон работает постоянно, анализируя фоновый шум для улучшения распознавания. Фоновый звук несет информацию о ритме дыхания,

частоте кашля, тоне голоса. Анализ семи дней фоновой аудиотелеметрии умной колонки позволяет выявить хронические заболевания дыхательной системы с чувствительностью 78%.

Умные термостаты также представляют угрозу. Анализируя динамику изменения заданной температуры в течение суток, можно восстановить циркадные ритмы жильцов, время пробуждения и отхода ко сну, периоды отсутствия. Эти данные относятся к биометрии поведенческого типа.

Принципиальная схема атаки выглядит так: сбор телеметрии через легитимные API или перехват незашифрованного трафика; агрегация данных с нескольких устройств одного пользователя; применение методов машинного обучения для выделения устойчивых признаков; сопоставление с открытыми базами данных; формирование биометрического профиля.

Предлагается выделить четыре типа косвенных утечек по механизму извлечения биометрии:

Тип 1. Физиологические реконструкции. Восстановление характеристик организма по данным датчиков, не предназначенных для медицинских измерений. Пример: определение вариабельности сердечного ритма по вибрации смартфона в кармане брюк.

Тип 2. Поведенческие слепки. Построение устойчивого профиля действий, уникального для конкретного человека. Поведенческая биометрия в российской правовой системе находится в зоне неопределенности – федеральное законодательство относит к биометрии физиологические и биологические характеристики, но обходит молчанием динамику поведения.

Тип 3. Акустические отпечатки. Извлечение голосовых характеристик из неречевых звуков. Умный пылесос с микрофоном фиксирует фоновые разговоры. Отдельные модели передавали 15-секундные фрагменты фонового аудио каждые три часа, накапливая архив голосовых образцов.

Тип 4. Композитные профили. Синтез биометрии из разнородных косвенных источников. Ни один источник по отдельности не дает биометрического признака, но их комбинация — дает. Например: время активности фитнес-браслета + геолокация смартфона + история покупок умного холодильника формируют поведенческий биометрический профиль.

Перейдем к технико-организационным мерам противодействия. Так, защита от косвенных биометрических утечек требует изменения подхода к проектированию IoT-экосистем.

Принцип избирательной телеметрии. Устройство должно передавать только те данные, которые необходимы для заявленной функции. Фитнес-

браслет для подсчета шагов не нуждается в непрерывной передаче сырых данных акселерометра – достаточно агрегированного счетчика. Внедрение этого принципа осложняется бизнес-моделями производителей: продажа обезличенных данных маркетинговым агентствам приносит до 30% дохода в сегменте умных домашних устройств.

Локальная обработка критичных данных. Все, что может быть вычислено на самом устройстве, не должно покидать его пределы. Распознавание голосовых команд, анализ качества сна, определение типа физической активности – эти алгоритмы сегодня работают на встроенных процессорах. Тем не менее многие производители принудительно выносят обработку в облако.

Дифференциальная приватность телеметрии. Математический аппарат дифференциальной приватности позволяет добавлять контролируемый шум в передаваемые данные так, что агрегированная статистика остается корректной, но индивидуальный профиль извлечь невозможно. Технология активно применяется зарубежными компаниями, но российские производители IoT пока не освоили ее массово.

Временное ограничение хранения телеметрии. Чем дольше хранится архив данных, тем выше риск его компрометации. Разумная политика – удаление телеметрии, не востребованной для текущих сервисов, через 30-90 дней. На практике производители хранят данные годами.

Аудит сторонних библиотек и SDK. Значительная доля утечек происходит из-за использования готовых библиотек аналитики. Разработчик интегрирует популярный фреймворк для сбора метрик, не читая документацию. Библиотека по умолчанию собирает максимум данных, включая косвенные биометрические признаки. Например, некоторые SDK собирают данные гироскопа и акселерометра «для определения качества сети», хотя для этой цели достаточно параметров Wi-Fi (RSSI, SNR).

Таким образом, экосистема Интернета вещей в России за 2022–2026 годы прошла путь от технологического энтузиазма к осознанию комплексных угроз приватности. Косвенные биометрические утечки – не гипотетическая проблема будущего, а реальность, зафиксированная в инцидентах последних лет. Телеметрия устройств, кажущаяся технически безобидной, при агрегации и анализе превращается в инструмент идентификации.

Предложенная классификация утечек на физиологические, поведенческие, акустические и композитные позволяет структурировать угрозы и адресно разрабатывать защитные меры. Практическая значимость исследования определяется возможностью использования

классификации в методиках оценки рисков информационной безопасности IoT-систем.

Дальнейшие направления исследований связаны с разработкой автоматизированных средств детектирования косвенных биометрических утечек, изучением эффективности методов дифференциальной приватности применительно к российской элементной базе IoT, а также формированием предложений по совершенствованию нормативной базы.

Список использованных источников:

1. Гузаиров М.Б. Конкатенация нейронных сетей в системе биометрической аутентификации пользователей компьютерной информационной системы / М.Б. Гузаиров, А.С. Исмагилова, Н.Д. Лушников // Инженерный вестник Дона. – 2025. – № 5(125). – С. 93-103.

2. Лу Ч.С., Ли Ю., Сянли Ю., Ли Ц. Негде спрятаться: кросс-модальная утечка идентичности между биометрией и устройствами // Конференции 2020 (20-24 апреля 2020 г.) – Нью-Йорк: Ассоциация вычислительной техники, 2020. – С. 12. URL: https://arxiv.org/abs/2001.08211 (дата обращения: 12.04.2026).

3. Накиев Р.Р., Ульянов В.В. Анализ уязвимостей интернет вещей (IoT) и способы их предотвращения // Вестник науки, 2023. – №7 (64). – С. 15. URL: https://cyberleninka.ru/article/n/analiz-uyazvimostey-internet-veschey-iot-i-sposoby-ih-predotvrascheniya (дата обращения: 13.04.2026).

I.R. Ishmukhametov
Ufa University of Science and Technology, Ufa

Scientific supervisor:
I.V. Salov
Ufa University of Science and Technology, Ufa

BIOMETRICS LEAKS THROUGH INDIRECT DATA IN THE INTERNET OF THINGS: THREAT ANALYSIS AND PREVENTION MEASURES

Abstract. The development of the Internet of Things ecosystem has led to the emergence of a new class of threats — biometric data leakage through indirect channels. Smart watches, fitness trackers, and home assistants accumulate behavioral patterns from which the owner's physiological characteristics can be reconstructed. The study identifies mechanisms of indirect biometric extraction from IoT device telemetry, analyzes actual attacks on Russian smart home systems and wearable electronics for 2023–2026. A

classification of indirect biometric leaks is proposed along with a set of organizational and technical measures adapted to the specifics of the Russian regulatory framework and domestic IoT component base.

Keywords: Internet of Things, biometric data, indirect leakage channels, wearable device telemetry, cyber threats, information security, smart home.

УДК 004.056.5:311

Казина К.З., Аккужина Ф.Ф.
Уфимский университет науки и технологий, Уфа

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

СТАТИСТИЧЕСКИЙ АНАЛИЗ КИБЕРИНЦИДЕНТОВ 2015–2024

Аннотация. В статье исследуется связь между ключевыми параметрами кибератак – финансовыми потерями, временем устранения инцидента, источником атаки и целевой индустрией – на основе данных за 2015–2024 годы. Проведен анализ двух гипотез с применением коэффициента корреляции Пирсона и теста хи-квадрат.

Ключевые слова: информационная безопасность, кибератака, финансовые потери, время устранения инцидента, источник атаки, целевая индустрия.

Рост числа кибератак и цифровая трансформация компаний требуют новых подходов к обеспечению безопасности. Недостаточная изученность связей между параметрами инцидентов затрудняет выработку эффективных стратегий защиты и оптимизацию ресурсов. В условиях отсутствия абсолютной защищенности систем статистический анализ становится критически важным инструментом прогнозирования угроз.

Целью данной работы являлся анализ набора данных о кибератаках в период с 2015 по 2024 год [1].

Для достижения поставленной цели разработана и реализована программа на языке Python (рис. 1) с применением библиотек с использованием библиотеки pandas (обработка данных) и функций pearsonr() и chi2_contingency из библиотеки scipy.stats (статистические тесты). Данные загружались из CSV-файла с помощью pd.read_csv().

Для анализа сформулированы следующие вопросы:

как связаны финансовые потери со временем устранения инцидента?

как связаны источники атак и целевая индустрия?

```python
import pandas as pd
from scipy.stats import pearsonr, chi2_contingency
import warnings
import sys
sys.stdout.reconfigure(encoding='utf-8')
#1. Загрузка данных
try:
    df = pd.read_csv("Global_Cybersecurity_Threats_2015-2024.csv")
except FileNotFoundError:
    print("Ошибка: Файл не найден.")
    exit()

# Исследовательский вопрос: как связаны финансовые потери со временем устранения инцидента?
# H0: Нет линейной связи между финансовыми потерями и временем устранения инцидента.
# H1: Существует линейная связь между финансовыми потерями и временем устранения инцидента.
corr_coef, p_val = pearsonr(df['Financial Loss (in Million $)'], df['Incident Resolution Time (in Hours)'])
print(f"Коэффициент корреляции Пирсона: {corr_coef}")
print(f"p-значение: {p_val}")
alpha = 0.05
if p_val < alpha:
    print("Отвергаем H0: существует значимая связь между финансовые потери со временем устранения инцидента")
else:
    print("Не отвергаем H0: нет значимой связи между финансовые потери со временем устранения инцидента")

#Исследовательский вопрос: как связан источники атак и целевая индустрия?
#H0: Нет линейной связи между источником атак и целевой индустрии.
#H1: Существует линейная связь между источником атак и целевой индустрии.
contingency_table = pd.crosstab(df['Attack Source'], df['Target Industry'])
chi2, p_value, dof, expected = chi2_contingency(contingency_table)

print(f"Хи-квадрат: {chi2:.3f}")
print(f"p-value: {p_value:.5f}")

if p_value < 0.05:
    print("Отвергаем H0: существует значимая связь между источником атак и целевой индустрии")
else:
    print("Не отвергаем H0: нет значимой связи между источником атак и целевой индустрии")
```

Рис. 1. Реализация программы на языке Python

Гипотезы для исследовательских вопросов приведены в таблице 1.

Таблица 1

Гипотезы для исследовательских вопросов

Исследовательский вопрос	Нулевая гипотеза (H0)	Альтернативная гипотеза (H1)
как связаны финансовые потери со временем устранения инцидента?	нет линейной связи между суммой финансовых потерь и временем устранения инцидента.	существует линейная связь между суммой финансовых потерь и временем устранения инцидента.
Как связаны источники атак и целевая индустрия?	нет статистической связи между источником атак и целевой индустрией	существует статистическая связь между источником атак и целевой индустрией.

Анализ линейной зависимости между суммой финансовых потерь и временем устранения инцидента проводился с использованием коэффициента корреляции Пирсона ($\alpha = 0.05$). Полученное значение (0.49) превышает установленный уровень значимости, что не позволяет отклонить нулевую гипотезу. Таким образом, статистически значимая линейная связь между данными показателями не обнаружена.

При анализе второй гипотезы использовался тест Хи-квадрат между значениями источников атак и целевой индустрии, так как этот метод позволяет оценить статистическую связь между категориальными переменными [2].

При уровне значимости 0.05 полученное p-значение (0.01) позволяет отвергнуть нулевую гипотезу. Следовательно, зависимость между источниками атак и сектором экономики, в котором находится жертва, является статистически значимой.

В ходе анализа данных о кибератаках за 2015–2024 гг. не было обнаружено статистически значимой линейной связи между объемом финансовых потерь и временем устранения инцидентов. Это свидетельствует о том, что в рамках исследуемой выборки длительность ликвидации последствий не является ключевым фактором, определяющим масштаб прямого экономического ущерба. Вместе с тем выявлена значимая зависимость между источниками атак и целевыми индустриями (использовался критерий хи-квадрат (χ^2)). Полученные данные подтверждают гипотезу о наличии выраженной отраслевой специфики киберугроз и таргетированном характере атак.

Таким образом, статистически подтвержденная связь между источником атаки и целевой индустрией указывает на высокую степень профилирования субъектов киберугроз. Это обуславливает переход от общей концепции информационной безопасности к отраслецентричным моделям защиты, основанным на аналитике специфических векторов атак и межкорпоративном обмене данными внутри конкретного сектора экономики.

Список использованных источников:

1. Global Cybersecurity Threats (2015-2024) [Электронный ресурс] // Kaggle. – [Б. м.]. – URL: https://www.kaggle.com/datasets/atharvasoundankar/global-cybersecurity-threats-2015-2024?resource=download (дата обращения: 20.04.2026).

2. Критерий хи-квадрат: [Электронный ресурс] / SkillFactory. – [Б. м.]. – URL: https://blog.skillfactory.ru/glossary/kriteriy-hi-kvadrat/ (дата обращения: 20.04.2026).

Kazina K.Z., Akkuzhina F.F.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Kornilova A.A.
Ufa University of Science and Technology, Ufa

A STATISTICAL ANALYSIS OF CYBERSECURITY INCIDENTS FROM 2015 TO 2024

Abstract. The article examines the relationship between key parameters of cyberattacks-financial losses, incident resolution time, attack source, and target industry-based on data from 2015 to 2024. Two hypotheses are analyzed using Pearson's correlation coefficient and the chi-square test.

Keywords: information security, cyberattack, financial losses, incident resolution time, attack source, target industry.

УДК 004.056.5

Курбатов А.Д.
Уфимский университет науки и технологий, Уфа

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

КОНЕЧНАЯ АУТЕНТИФИКАЦИЯ В MESH-СЕТЯХ MESHTASTIC: ПРОГРАММНО-АППАРАТНАЯ МОДИФИКАЦИЯ ОКОНЕЧНЫХ УЗЛОВ

Аннотация. В статье исследуется уязвимость протокола Meshtastic, связанная с отсутствием конечной аутентификации и целостности данных в канальных сообщениях. На основании анализа стека протоколов предлагается архитектура «Шифрующего Шлюза» – программного адаптера безопасности, работающего на уровне оконечных устройств. Решение реализует AEAD-шифрование и механизм ручной регистрации ключей без модификации сетевой инфраструктуры и сохраняет полную совместимость с немодифицированными узлами.

Ключевые слова: Meshtastic, mesh-сеть, LoRa, конечная аутентификация, AEAD, ESP32, целостность данных.

Современные централизованные системы мобильной связи и доступа в интернет все чаще демонстрируют уязвимость перед техногенными угрозами и чрезвычайными ситуациями. Массовые отключения мобильного интернета и сотовой связи, систематически происходящие в последние пару лет, приобрели устойчивый характер и затрагивают десятки регионов страны. На этом фоне возрастает актуальность поиска альтернативных решений, способных обеспечить базовый уровень коммуникации без опоры на централизованную операторскую инфраструктуру при надлежащем уровне защищенности в чрезвычайных ситуациях, а также местах, удаленных от наземных проводных коммуникаций, требующих передачи текстовых сообщений и GPS сигналов. На данный момент на территории Российской Федерации уже существуют готовые mesh-сети в некоторых городах, что показывает достаточную зрелость проекта Meshtastic для использования в качестве практического решения.

Meshtastic реализует mesh-топологию на базе модуляции LoRa в нелицензируемых ISM-диапазонах 433 МГц и 868 МГц с дальностью до 15 км при прямой видимости [1]. Каждый узел на базе микроконтроллера ESP32 или nRF52 с трансивером SX1262 одновременно выполняет функции клиента и ретранслятора. Платформа обеспечивает канальное шифрование AES-256 с Pre-Shared Key (PSK), дедупликацию по полю messageID и hop-by-hop подтверждения доставки [2]. Однако эти механизмы решают только задачу надежности доставки и не обеспечивают конечную аутентификацию отправителя и целостность сообщений на уровне приложения.

Отсутствие указанных гарантий составляет ключевую уязвимость протокола, так как узлы идентифицируются по NodeID, вычисляемому из MAC-адреса устройства, а не из криптографического ключа, PSK защищает трафик канала в целом, но не связывает конкретный пакет с конкретным отправителем. Любой участник в зоне действия сети способен сформировать Meshtastic.Packet с произвольным значением поля originNode, и маршрутизирующая логика ретранслирует его без проверки подлинности. Это открывает два класса атак: подмену источника – отправку ложных команд или координат от имени легитимного узла и модификацию payload в транзите, при которой получатель принимает искаженные данные за достоверные [2,3].

Среди других известных слабостей Meshtastic (Sybil-атаки через вытеснение NodeDB, отсутствие PFS, предсказуемые ключи в клонированных прошивках) проблема отсутствия конечной аутентификации выделяется возможностью локального устранения без изменения сетевой инфраструктуры. Устранение Sybil-атак требует переработки всей маршрутизации, а реализация PFS через ECDHE

добавляет дополнительный раунд обмена ключами. Поэтому уязвимость аутентификации является приоритетной для точечной модификации на уровне оконечных станций [3, 4].

Предлагаемая архитектура «Шифрующего Шлюза» представляет собой программный адаптер безопасности, встраиваемый между пользовательским приложением и драйвером радио-интерфейса. Маршрутизационные поля пакета (originNode, destinationNode, nextHop, ttl) остаются нетронутыми, модифицируется исключительно поле payload – немодифицированные узлы в сети корректно ретранслируют пакет стандартного вида, не имея возможности интерпретировать зашифрованное содержимое, что гарантирует полную совместимость с существующей инфраструктурой.

При отправке адаптер формирует блок (JSON или Protobuf) с исходным сообщением, идентификаторами отправителя и получателя и временно́й меткой, после чего применяет AEAD-шифр, следовательно, шифрование и вычисление кода аутентичности (MAC) выполняются за один проход. Временная метка блокирует replay-атаки – стандартный стек хранит сведения об обработанных пакетах около 10 минут, при этом синхронизация времени узлов доступна как по сигналу GPS с модуля на плате, так и через сопряженное мобильное устройство, после чего перехваченный пакет может быть принят повторно [4]. При приеме адаптер расшифровывает payload, верифицирует MAC и сверяет идентификатор отправителя с локальным хранилищем доверенных ключей; неудача на любом из шагов влечет отброс. Оптимальный криптографический примитив для Heltec Wireless Stick V3 (ESP32-S3FN8, Xtensa LX7, 240 МГц) – ChaCha20-Poly1305: без аппаратного AES-ускорителя алгоритм превосходит AES-GCM по пропускной способности. Базовый стек занимает 39,3 КБ ОЗУ из 512 КБ и 383,2 КБ флэш-памяти из 8 МБ при загрузке ЦПУ 1,14% [2] – ресурс для библиотеки Mbed TLS есть без замены аппаратной части.

В части управления доверием реализуется схема ручной регистрации без PKI: публичный ключ нового участника (или его SHA-256 отпечаток) передается остальным устройствам через QR-код, пакеты от незарегистрированных отправителей отклоняются без передачи в приложение. В базовой конфигурации PFS не обеспечивается, а это значит, что добавление обмена ключами X25519 (ECDHE) перед каждой сессией устранит этот пробел ценой дополнительного раунда коммуникации [3]. В текущем виде архитектура должна полностью закрывать угрозу подмены источника и модификации данных в транзите, переводя станции из режима «доверяет всем узлам канала» в режим «доверяет только зарегистрированным пользователям».

Список использованных источников:

1. Кузнецов Н. М. Использование технических возможностей сетей беспроводной связи // Динамика развития системы военного образования: материалы VII Междунар. науч.-практ. конф. – Омск: ОмГТУ, 2025. – С. 997–1000.
2. Messina F., Santoro C., Santoro F. F. Enhancing Security and Trust in Internet of Things through Meshtastic Protocol Utilising Low-Range Technology // Electronics. – 2024. – Vol. 13, No. 6. – P. 1055. – DOI: 10.3390/electronics13061055.
3. Бирюков Д. Н., Дудкин А. С., Родионов Е. С. Подход к созданию криптозащищенной mesh-сети // Труды Военно-космической академии имени А. Ф. Можайского. – 2024. – № 691. – С. 94–101.
4. Encryption // Meshtastic Official Documentation. – [б. г.]. – URL: https://meshtastic.org/docs/overview/encryption/ (дата обращения: 12.04.2026).

Kurbatov A.D.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Fatkhelislamov A.F.
Ufa University of Science and Technology, Ufa

END-TO-END AUTHENTICATION IN MESHTASTIC MESH NETWORKS: HARDWARE-SOFTWARE MODIFICATION OF TERMINAL NODES

Abstract. The paper investigates a vulnerability in the Meshtastic protocol caused by the absence of end-to-end authentication and message integrity at the application layer. Based on protocol stack analysis, the «Encrypting Gateway» architecture is proposed: a software security adapter at the terminal device level implementing AEAD encryption and manual key registration without modifying network infrastructure.

Keywords: Meshtastic, mesh network, LoRa, end-to-end authentication, AEAD, ESP32, data integrity.

УДК 004.056

Курпаченко Д.М.
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина), Санкт-Петербург

Научный руководитель:
Шульженко А.Д.
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина), Санкт-Петербург

ЦИФРОВОЙ СЛЕД СОТРУДНИКА КАК НЕРЕГЛАМЕНТИРОВАННЫЙ КАНАЛ ПЕРЕДАЧИ ИНФОРМАЦИИ: МЕТОДЫ ПРЕВЕНТИВНОГО УПРАВЛЕНИЯ

Аннотация. В докладе рассматривается проблема эксплуатации цифрового следа сотрудников как вектора атак социальной инженерии. На основе статистики 2025 года показано, что более 60% утечек данных связаны с человеческим фактором. Выявлен разрыв между традиционной моделью защиты периметра и современными векторами атак. Предложена методика превентивного управления цифровым следом, включающая мониторинг публичного контура, минимизацию разведывательной ценности данных и управление неуправляемыми устройствами.

Ключевые слова: информационная безопасность; цифровой след; социальная инженерия; депериметризация; нулевое доверие; управление рисками; человеческий фактор; защита каналов передачи данных.

В 2025 году 36% крупных инцидентов использовали социальную инженерию, при этом 60% из них привели к утечкам данных [1].

Важным активом организации с точки зрения информационной безопасности являются сотрудники – их социальные сети, блоги, аккаунты на форумах. Ключевым понятием становится цифровой след – совокупность данных, оставляемых пользователем в корпоративных и публичных сетях. Этот след представляет избыточный неконтролируемый канал связи, активно используемый злоумышленниками для повышения энтропии атак социальной инженерии.

Важно обратить особое внимание на выработку методик работы с цифровым следом, снижающих его ценность в руках злоумышленников.

Цифровой след как инструмент атаки.

Для целей защиты важнейшим аспектом является понимание принципа работы атакующего. Анализ модели использования цифрового

следа позволяет эффективнее выработать методы снижения ущерба от действий злоумышленника.

Таксономия цифрового следа. Цифровой след рационально разделить на два вида: активный и пассивный. Активный – контент, создаваемый пользователем намеренно. Пассивный – информация, появляющаяся без активного участия пользователя: техническая информация, геолокация, кросс-идентификация профилей. В руках злоумышленника оба вида образуют набор данных, открывающих новые векторы атак.

Цепочки атак с использованием цифрового следа. В 2025 году 60% подтвержденных утечек данных были связаны с человеческим фактором, из них 17% – с социальной инженерией как вектором начального доступа [2]. Злоумышленники все чаще проводят многоступенчатые атаки, где социальная инженерия служит входной точкой, за которой следуют компрометация учетных данных или развертывание вредоносного ПО. Структура таких атак описывается матрицей MITRE ATT&CK [3]. Этапы приведены в таблице 1.

Таблица 1

Этапы матрицы MITRE ATT&CK

Этап	**Характеристика**
Разведка	Сбор информации для использования в дальнейших этапах
Подготовка ресурсов	Создание ресурсов для поддержки атаки
Первоначальный доступ	Получение первоначального доступа во внутренней сети
Выполнение	Выполнение вредоносного кода
Закрепление	Удержание позиций внутри контура сети
Повышение привилегий	Попытки повышения привилегий до более высокого уровня доступа
Предотвращение обнаружения	Методы предотвращения обнаружения внутри сети
Получение учетных данных	Попытка украсть учетные данные и пароли
Изучение	Изучение окружения и устройства внутренней сети
Перемещение внутри периметра	Продвижение внутри сети
Сбор данных	Сбор данных, отвечающих целям злоумышленника
Организация управления	Попытка установить контроль над скомпрометированными данными и системами
Эксфильтрация данных	Кража данных
Деструктивное воздействие	Манипуляция данными, прерывание работы и уничтожение

Работа злоумышленника с цифровым следом соответствует первому этапу – разведке. Собранная информация повышает его осведомленность и вероятность успешности атаки.

Разрыв между системами защиты информации и личным контуром

Концепция депериметризации. В работе [4] вводится понятие депериметризации – процесса размывания четких границ корпоративной сети. Это подразумевает использование концепции нулевого доверия и означает появление нерегламентированных каналов утечки данных, не контролируемых существующими СЗИ.

Ограничения традиционных средств защиты. DLP, SIEM, IDS/IPS и системы разграничения доступа эффективны внутри периметра, но фундаментально не способны противостоять угрозам эксплуатации цифрового следа за его пределами [5]. Системы бессильны перед публикацией фото, где на заднем плане виден внутренний документ.

Разрыв доверия к доступу. Исследование [6] описывает «разрыв доверия к доступу»: 38% бывших сотрудников сохраняли доступ к данным предыдущего работодателя; 73% используют AI-инструменты без соблюдения корпоративных правил; две трети допускают небезопасные практики с паролями.

Противоречие СЗИ и современных угроз. Сравнение по трем ключевым аспектам (таблица 2) наглядно показывает пробел в обеспечении безопасности.

Таблица 2

Сравнение традиционных СЗИ и реальных векторов угроз

Аспект	**Традиционная СЗИ**	**Реальный вектор угрозы**
Контролируемая среда	Корпоративная сеть, управляемые устройства	Публичные платформы, личные устройства
Тип данных	Файлы, сетевые пакеты, логи	Метаданные, поведенческие паттерны, OSINT
Субъект защиты	Информационная система	Сотрудник как источник данных

Цифровой след формирует параллельный канал связи, по которому утекает информация, достаточная для построения успешной атаки. Существующие СЗИ не способны ни детектировать этот канал, ни контролировать передаваемую по нему информацию.

Превентивное управление цифровым следом

Ключевым принципом нового подхода должно стать нулевое доверие, расширенное на информационное поле за пределами организации – цифровой след сотрудников.

Предлагаемые методы. Мониторинг публичного контура: постоянный анализ открытых источников для понимания, какая информация доступна потенциальному нарушителю.

Минимизация разведывательной ценности: тренинги и рекомендации по работе с активным следом, а также технические средства минимизации пассивного следа.

Управление неуправляемыми устройствами: политики доступа к конфиденциальным данным с личных устройств сотрудников при соблюдении требований закона [7].

Ожидаемые эффекты. Применение методов обеспечивает: снижение успешности целевого фишинга; повышение порога входа атакующего; снижение вероятности компрометации через личные устройства; формирование культуры осведомленности о цифровом следе.

Заключение

Проведен анализ влияния цифрового следа на защищенность организации. На основе статистики 2025 года показана значимость человеческого фактора в успешности атак. Выявлен разрыв между существующими СЗИ и современными угрозами, обусловленный периметризацией. Предложен комплекс превентивных мер с ожидаемыми эффектами, свидетельствующими об их применимости в реальной практике. Дальнейшие исследования направлены на разработку конкретных реализаций предлагаемых методов.

Список использованных источников:

1. 2025 Unit 42 Global Incident Response Report: Social Engineering Edition [Электронный ресурс] // Palo Alto Networks. – 2025. – URL: https://unit42.paloaltonetworks.com/2025-unit-42-global-incident-response-report-social-engineering-edition/ (дата обращения: 09.04.2026).

2. DBIR Trends Reveal the Human Side of Data Breaches [Электронный ресурс] // PhishingBox. – 2025. – URL: https://www.phishingbox.com/news/post/dbir-trends-reveal-human-side-data-breaches (дата обращения: 11.04.2026).

3. MITRE ATT&CK® [Electronic resource] / MITRE Corporation. – URL: https://attack.mitre.org/ (дата обращения: 11.04.2026).

4. Spencer M., Pizio D. The de-perimeterisation of information security: The Jericho Forum, zero trust, and narrativity // Soc Stud Sci. 2024. Vol. 54(5). P. 655–677. DOI: 10.1177/03063127231221107.

5. Олисеенко В.Д., Абрамов М.В., Тулупьев А.Л., Иванов К.А. Прототип программного комплекса для анализа аккаунтов пользователей социальных сетей // 2022. Т. 35. № 1. С. 045–053. DOI: 10.15827/0236-235X.137.045-053.

6. Employees keep finding new ways around company access controls [Электронный ресурс] // Help Net Security. – 2025. – URL: https://www.helpnetsecurity.com/2025/11/03/1password-access-trust-gap-report/ (дата обращения: 11.04.2026).

7. Saheed M., Mafais M. Practical approach on Bring Your Own Device (BYOD) under the GDPR Regulation for SMEs. – 2025.

Kurpachenko D.M.
Saint Petersburg Electrotechnical
University «LETI», Saint-Petersburg

Scientific supervisor:
Shulzhenko A.D.
Saint Petersburg Electrotechnical
University «LETI», Saint-Petersburg

EMPLOYEE DIGITAL FOOTPRINT AS AN UNREGULATED DATA TRANSMISSION CHANNEL: PREVENTIVE MANAGEMENT METHODS

Abstract. The report examines the exploitation of employees' digital footprint as a social engineering attack vector in corporate information systems. Statistics from 2025 show that over 60% of confirmed data breaches involve the human factor. A gap between traditional perimeter protection and modern attack vectors is identified. A preventive digital footprint management methodology is proposed, encompassing public perimeter monitoring, reduction of intelligence value of data, and unmanaged device control.

Keywords: information security; digital footprint; social engineering; deperimeterization; zero trust; risk management; human factor; data transmission channel protection.

УДК 004.056.53

Мухаметьянова А.Р., Аюпова И.И.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Миронова Н.Г.
Уфимский университет науки и технологий, Уфа

МОДЕЛЬ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ СОТРУДНИКОВ В УСЛОВИЯХ РАЗМЫТИЯ ПЕРИМЕТРА: РАЗВИТИЕ КОНЦЕПЦИИ ZERO TRUST

Аннотация. Рассматривается трансформация подходов к защите персональных данных сотрудников в условиях распределенной цифровой инфраструктуры. Анализируются ограничения периметровой модели безопасности и возможности концепции Zero Trust. Предлагается развитие модели за счет учета контекста доступа и дифференциации защищаемых данных. Показано, что сочетание динамического контроля доступа и индивидуализации политики безопасности позволяет повысить устойчивость систем к современным угрозам.

Ключевые слова: персональные данные, Zero Trust, контроль доступа, информационная безопасность.

Кадровые информационные системы сегодня концентрируют наиболее чувствительные категории данных: паспортные сведения, финансовую информацию, медицинские показатели, сведения о доходах. При этом сами процессы их обработки все чаще выходят за пределы корпоративной сети – используются облачные сервисы, собственные технические средства персонала и дистанционное управление. Гибридные среды размывают границы контроля, порождая новые риски и усложняя процессы контроля и защиты данных.

Принцип модели защиты по периметру был сформирован в условиях централизованной инфраструктуры. Защита информации оказывалась привязана к инфраструктуре, не к данным. «Классический» принцип управления доступом, когда авторизованному сотруднику «по умолчанию» предоставляются права на выполнения определенных действий и подписания документов без необходимости каждый раз подтверждать свои права, приводит к захватам учетных записей или злоупотреблениею избыточными полномочиями. Ряд уязвимостей (слабый мониторинг действий сотрудников; выдача прав доступа без анализа контекста выполнения операций) порождают риск быстрого распространение атак внутри сети.

В новых обстоятельствах привычная «классическая» модель информационной безопасности (на основе разделения зон на внутреннюю – «доверенную» и внешнюю – «недоверенную» и защиты внутреннего периметра) теряет эффективность, требуя перехода от защиты физической границы – к защите данных, идентичности и рабочих нагрузок, где бы они ни находились. В более актуальной модели безопасности не предполагается автоматического доверия к пользователям или устройствам внутри периметра. Защита идентичности предполагает непрерывную проверку личности и устройства пользователя, права пользователя зависят от текущего контекста запроса и рисков при каждом запросе на доступ к защищаемым ресурсам, многофакторную идентификацию пользователя и методы поведенческого анализа, анализ состояния устройств, подключенных к корпоративной сети (на предмет актуальности обновлений, средств защиты, конфигурации устройства) [1, 3]. При этом доступ открывается каждому пользователю только к минимально необходимым для решения задачи ресурсам, а микросегментация сети делит последнюю на мелкие изолированные зоны, чтобы максимально затруднить потенциальному нарушителю продвижение внутри сети.

Более актуальная модель безопасности требует смещения акцента безопасности с субъекта на объект доступа - сами данные. Например, при работе с персональными данными сотрудников модель безопасности с акцентом на проверке пользователя или устройства явно недостаточна: различные категории персональных данных обладают неодинаковой ценностью и риском компрометации (так, данные о зарплате или медицинских показателях имеют более высокий уровень чувствительности по сравнению с общедоступными кадровыми ПДн). В отличие от стандартной схемы, добавляется этап анализ чувствительности данных, влияющий на итоговое решение о доступе (рис. 1).

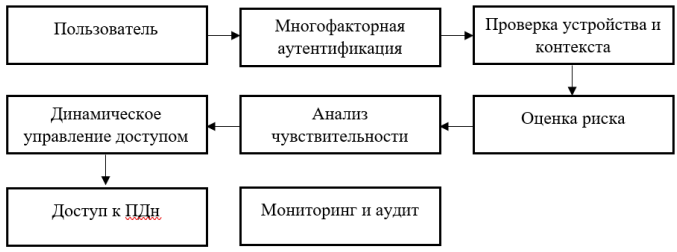


Рис. 1. Архитектура модели защиты персональных данных

Процесс обработки запроса включает несколько уровней проверки:

1. идентификация и аутентификация пользователя;
2. анализ параметров устройства и среды выполнения;
3. оценка контекста (время, местоположение, тип операции);
4. определение уровня чувствительности запрашиваемых данных;
5. формирование решения о доступе с учетом совокупного риска;
6. непрерывный контроль действий пользователя.

Традиционная модель доступа к критичным данным с предоставлением наименьших (но на весь сеанс работы с системой) привилегий дополняется в «продвинутой» архитектуре нулевого доверия принципом автоматического сброса (или ограничения) прав пользователя сразу после выполнения конкретной операции/ задачи с критичными / чувствительными данными (принципом «реверсивной привилегии»). Доступ становится динамической величиной, а не фиксированным правом. Усилить защиту помогут ограничения, связанные с идентификационными данными пользователей (запрет копирования, запись сессии и др.).

Таблица 1

Сравнение подходов

Критерий	Периметровая модель	Zero Trust	Расширенная модель
Основа доверия	Сеть	Пользователь	Пользователь + данные
Контроль доступа	Статический	Динамический	Контекстно-зависимый
Учет чувствительности данных	Отсутствует	Ограничен	Полный
Защита от инсайдеров	Низкая	Средняя	Повышенная

Описанный подход полезен в кадровых и управленческих системах [3], позволяя снизить риски утечки ПДн, последствия компрометации учетных записей, детализировать контроль доступа, обеспечить соответствие законодательству РФ в области защиты информации.

Развитие концепции Zero Trust за счет учета чувствительности данных позволяет повысить адаптивность системы защиты и приблизить ее к реальным условиям эксплуатации.

Список использованных источников:

1. Каширина Е. И., Кустов Р.А. Сравнительный анализ концепции Zero Trust и традиционной модели информационной безопасности // Электронный сетевой политематический журнал «Научные труды КубГТУ». 2025. № 6. - С. 135-149 – URL: https://ntk.kubstu.ru/data/mc/0117/5119.pdf.

2. Mandal, D., Singhal, N., Tyagi, D. Cybersecurity in the Era of Emerging Technology in Emerging Technology and Management Trends // ManglamPublications, 2023. - pp. 108-134.

3. Шахторин М.С. Анализ угроз информационной безопасности в системах цифрового управления // Вестник науки №2 (83) том 2. С. 704 - 709. 2025 г. ISSN 2712-8849 // Электронный ресурс: https://www.вестник-науки.рф/article/21423 (дата обращения: 01.04.2026).

Mukhametianova A.R., Ayupova I.I.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Mironova N.G.
Ufa University of Science and Technology, Ufa

MODEL FOR PROTECTING EMPLOYEE PERSONAL DATA IN A PERIMETERLESS ENVIRONMENT: DEVELOPMENT OF THE ZERO TRUST CONCEPT

Abstract. The article examines the transformation of approaches to protecting employees' personal data in a distributed digital environment. The limitations of perimeter-based security and the potential of Zero Trust are analyzed. An extended model is proposed that incorporates data sensitivity and contextual access control.

Keywords: personal data, Zero Trust, cybersecurity, access control.

УДК 004.75:004.021:003.26

Петренко А.С.
Санкт-Петербургский Федеральный исследовательский центр Российской академии наук, Санкт-Петербург

Научный руководитель:
Молдовян Н.А.
Санкт-Петербургский Федеральный исследовательский центр Российской академии наук, Санкт-Петербург

РАЗРАБОТКА КВАНТОВО-УСТОЙЧИВОГО АЛГОРИТМА КОНСЕНСУСА С АДАПТИВНОЙ ИЕРАРХИЧЕСКОЙ АРХИТЕКТУРОЙ

Аннотация. В работе предложена архитектура консенсуса для блокчейнов, объединяющая локальные квантовые вычисления с классическими алгоритмами согласованности. Сеть адаптивно разбивается на кластеры, в каждом из которых используются квантовые измерения для достижения консенсуса. Глобальное согласование

обеспечивается классическим алгоритмом на сжатой сетевой структуре с линейной масштабируемостью. Система обеспечивает устойчивость к квантовым атакам при сохранении экономической безопасности через механизм залогов.

Ключевые слова: квантовый консенсус, блокчейн, адаптивная кластеризация, постквантовая криптография, масштабируемость, квантовое вычисление, распределенная система, квантовая устойчивость

Развитие квантовых вычислений создает критическую угрозу для всей современной криптографии, и, в частности, криптографической безопасности блокчейн-систем. Так, алгоритм Шора демонстрирует, что асимметричная криптография на основе факторизации и дискретного логарифмирования может быть взломана за полиномиальное время квантовым компьютером. Практические системы с достаточным числом стабильных кубитов для такого взлома ожидаются в течение 15-20 лет, а первые практически релевантные для квантового криптоанализа квантовые компьютеры ожидаются уже к 2030 году, что требует немедленного перехода как к постквантовым криптографическим примитивам, так и к квантово-устойчивой архитектуре систем и приложений [1-3]. При этом реализации алгоритма консенсуса Proof-of-Stake (PoS), включая Ethereum 2.0, опираются на ECDSA и BLS подписи, которые будут полностью скомпрометированы при наличии достаточно больших квантовых ресурсов у атакующих. Выбор Proof-of-Stake в качестве базовой парадигмы для модификации обусловлен энергоэффективностью и линейной масштабируемостью по стоимости, а также изученным и проверенным механизмом экономическая безопасности.

При рассмотрении возможности использования квантовых вычислений для построения алгоритма так называемого «квантового» консенсуса было оценено несколько подходов [4-6]. Из всех типов квантовых консенсусов только гибридный квантово-классический консенсус на основе локальных измерений, сочетающий локальные квантовые операции на валидаторах с классической коммуникацией, показывает реальную применимость в ближайшие года. Этот подход использует локальные квантовые операции на каждом валидаторе при расчете один кубит на узел для генерации случайных битов или повышения энтропии, после чего результаты передаются через классические каналы, где достигается консенсус.

В ответ на существующие недостатки и ограничения существующих алгоритмов консенсуса была разработана архитектура, объединяющая локальные квантовые вычисления с классическим BFT консенсусом. Главной особенностью такой архитектуры является адаптивное разбиение

сети на K* кластеров посредством спектрального анализа матрицы Лапласиана топологии $L_G = D - A$, где D – матрица степеней вершин, а A – матрица смежности.

Коммуникационная сложность разработанной архитектуры обусловлена в первую очередь иерархической структурой, локальный консенсус требует M сообщений, глобальный BFT на метаграфе требует $O(K^2)$ *сообщений. При* $K = O(\sqrt{N})$ общая сложность составляет $O(N)$, линейная вместо $O(N^2)$ у классических BFT систем.

Временная сложность выражается в следующем, локальный консенсус сходится за $O\left(\frac{\log\left(\frac{1}{\varepsilon}\right)}{\lambda_2}\right)$ раундов, где λ_2 - спектральный промежуток графа. Глобальный консенсус требует $O(\sqrt{N})$ раундов. Для $N = 500\,000$ валидаторов с существующими современными оптимизациями задержка в худшем случае может быть снижена как минимум до 2-5 минут, что остается приемлемым для блокчейн-систем.

Общая безопасность разработанной архитектуры сочетает безопасность локального PQP (информационно-теоретическую, согласно квантовой механике) и безопасность глобального BFT (экономическую). Противник, желающий нарушить консенсус, должен единовременно взломать информационно-теоретические гарантии PQP в большинстве кластеров, или контролировать более $1/3$ stake в большинстве кластеров, или контролировать более $1/3$ кластеров на метаграфе, что требует контроля более $1/3$ залога всей сети.

Данная работа решила задачу создания алгоритма блокчейн-консенсуса, требующего одновременного достижения трех целей, которые традиционно считаются трудносовместимыми, а именно - линейной $O(N)$ коммуникационной сложности, экономической безопасности через механизм залога, и устойчивости против атак с использованием квантовых компьютеров. Решение достигнуто комбинацией трех компонентов:

1. Спектральная кластеризация сети на $K^* = O(\sqrt{N})$ кластеров на основе анализа собственных значений матрицы Лапласиана $L_G = D - A$. Это позволяет разложить полносвязную задачу $O(N^2)$ на локальные задачи $O(M)$ и глобальную задачу малого размера $O((K^*)^2) = O(N)$.

2. Локальный квантовый консенсус в каждом кластере, кодирующий состояния валидаторов на сфере Блоха и выполняющий проективные измерения. Квантовая природа гарантирует информационно-теоретическую безопасность, спектральные свойства графа определяют скорость сходимости, не зависящую от числа узлов.

3. Глобальный взвешенный BFT консенсус на метаграфе, где каждый узел представляет кластер, взвешенный пропорционально залогу

валидаторов кластера. Это сохраняет экономическую безопасность классического PoS и обеспечивает финализацию блоков.

По предварительным расчетам при наличии необходимого оборудования, не вызывающего дополнительные задержки, архитектура обеспечивает сходимость консенсуса за ~ 12 секунд эквивалентно обычному Proof-of-Stake, сохраняя линейную коммуникационную сложность $O(N)$ вместо квадратичной $O(N^2)$ классических BFT алгоритмов. Для полноценного развертывания архитектуры необходимо обеспечить каждый отдельный узел блокчейн-сети как минимум одним отдельным кубитом. В отличие от обычного PoS, который уязвим к атакам злоумышленников с использованием квантовых компьютеров и полагается на вычислительную сложность ECDSA/BLS подписей, разработанная архитектура добавляет квантовую устойчивость за счет использования локального квантового консенсуса и постквантовых криптографических элементов [7-10]. Что в совокупности обеспечивает одновременные масштабируемость и безопасность на уровне, невозможном при использовании исключительно классических или исключительно квантовых алгоритмов консенсуса.

Список использованных источников:

1. Petrenko A., Petrenko S., Gnidko K. et al. Application of quantum fourier transform in cryptology // Journal of Computer Virology and Hacking Techniques. 2025. V. 21. No. 1. Art. 26. https://doi.org/10.1007/s11416-025-00563-3.
2. Petrenko A. Applied Quantum Cryptanalysis. Aalborg: River Publishers, 2023. 222 p. https://doi.org/10.1201/9781003392873.
3. Петренко А.С., Петренко С.А. Основные алгоритмы квантового криптоанализа // Вопросы кибербезопасности. 2022. № 1(53). С. 100–115. https://doi.org/10.21681/2311-3456-2022-1-100-115.
4. Marcozzi M., Mostarda L. Quantum consensus: an overview // arXiv. 2021. arXiv:2101.04192 [quant-ph]. https://doi.org/10.48550/arXiv.2101.04192.
5. Weng C.X., Li M.Y., Yin H.L., Chen Z.B. Beating the Fault-Tolerance Bound and Security Loopholes for Byzantine Agreement with a Quantum Solution // Research. 2023. V. 6. Art. 0272. https://doi.org/10.34133/research.0272.
6. Sun X., Kulicki P., Sopek M. Multi-party quantum Byzantine agreement without entanglement // Physical Review Letters. 2020. V. 125. Art. 150501. https://doi.org/10.1103/PhysRevLett.125.150501.
7. Dinh K.L., Do T.B., Moldovyan N.A., Petrenko A.S. Typical Algebraic Signature Schemes with Two Hidden Groups // Future Data and Security Engineering. FDSE 2025: Proceedings of the 11th International

Conference / edited by T.K. Dang, J. Küng, T.M. Chung. Singapore: Springer, 2026. Communications in Computer and Information Science. V. 2709. P. 7–27. https://doi.org/10.1007/978-981-95-4724-17.

8. Петренко А.С. Метод построения постквантовых алгоритмов ЭЦП с двумя скрытыми группами // Вопросы кибербезопасности. 2025. № 2(58). С. 52–63. https://doi.org/10.21681/2311-3456-2025-2-52-63.

9. Петренко А.С. Методика построения стойких постквантовых КНАА-2-ЭЦП с малыми размерами подписи и открытого ключа // Защита информации. Инсайд. 2025. № 5(76). С. 76–83.

10. Молдовян Н.А., Петренко А.С. Алгебраический алгоритм ЭЦП с двумя скрытыми группами // Вопросы кибербезопасности. 2024. № 6. С. 98–107. https://doi.org/10.21681/2311-3456-2024-6-98-107.

Petrenko A.S.
St. Petersburg Federal Research Center
of the Russian Academy of Sciences, St. Petersburg

Scientific supervisor:
Moldovyan N.A.
St. Petersburg Federal Research Center
of the Russian Academy of Sciences, St. Petersburg

DEVELOPMENT OF A QUANTUM-STABLE CONSENSUS ALGORITHM WITH AN ADAPTIVE HIERARCHICAL ARCHITECTURE

Abstract. The paper proposes a consensus architecture for blockchains that combines local quantum computing with classical consistency algorithms. The network adaptively splits into clusters, each of which uses quantum measurements to achieve consensus. Global alignment is provided by a classical algorithm based on a compressed network structure with linear scalability. The system provides resistance to quantum attacks while maintaining economic security through a collateral mechanism.

Keywords: quantum consensus, blockchain, adaptive clustering, post-quantum cryptography, scalability, quantum computing, distributed system, quantum stability

УДК 004.056:004.89+519.83

Петренко А.С.
Санкт-Петербургский Федеральный исследовательский
центр Российской академии наук, Санкт-Петербург

Научный руководитель:
Молдовян Н.А.
Санкт-Петербургский Федеральный исследовательский
центр Российской академии наук, Санкт-Петербург

ОПТИМИЗАЦИЯ УСТОЙЧИВОСТИ НАЦИОНАЛЬНЫХ БЛОКЧЕЙН-ПЛАТФОРМ И ЭКОСИСТЕМ С ПОМОЩЬЮ КВАНТОВО-ВДОХНОВЛЕННЫХ АЛГОРИТМОВ

Аннотация. В работе предложена QUBO-постановка задачи устойчивости блокчейн-систем с вероятностями атак, ресурсными ограничениями и штрафной функцией. Адаптированы алгоритмы dSB, HdSB и разработан новый алгоритм GdSB для минимизации риска. Эксперименты на задачах до сотен переменных показывают превосходство GdSB над SB и его аналогами по точности, скорости нахождения и устойчивости решений.

Ключевые слова: блокчейн, устойчивость, квантово-вдохновленные алгоритмы, имитированная бифуркация, модель Изинга, квантовый отжиг, теория игр, оптимизация устойчивости

Блокчейн-технологии получили широкое распространение в самых разных сферах от криптовалют до государственных реестров. С ростом применения блокчейна все более актуальными становятся вопросы обеспечения его устойчивости к вредоносным воздействиям. Под устойчивостью блокчейн-системы понимается ее способность сохранять свойства безопасности (неизменяемость записей, консенсус, корректность транзакций и т.д.) при атаках на различные компоненты системы. Соответственно, под обеспечением устойчивости в данной работе понимается процесс выбора и внедрения оптимального набора защитных мер, минимизирующих вероятность успешной реализации атак. Известные основные угрозы подразделяются на атаки на консенсус, сетевую цензура и сетевые атаки, и криптографические атаки.

В перспективе появления квантовых компьютеров особую опасность представляют атаки, использующие квантовые алгоритмы для взлома криптографии (алгоритм Шора для факторизации, Гровера для перебора), т.к. подобные угрозы снижают криптостойкость электронной подписи и доказуемость работы блокчейн-системы [1-4]. Следовательно,

обеспечение устойчивости блокчейна должно носить комплексный характер, учитывая и классические, и квантовые векторы атак. Ключевой проблемой здесь является оптимальный выбор набора мер защиты и самовосстановления из большого числа возможных опций, при ограниченных ресурсах, т.к. простой полный перебор таких мер даже при умеренном числе параметров достаточно быстро становится непрактичным.

В результате были исследованы применения квантово-вдохновленных алгоритмов для оптимизации устойчивости блокчейн-систем, сформулирована QUBO-модель выбора защитных мер, минимизирующих суммарный риск успешных атак, включая атаки с использованием квантовых вычислений. Приведен обзор современных методов оптимизации от классических эвристик до специально разработанных для решения QUBO-задач квантовых и квантово-вдохновленных методов [5-12]. Отмечено, что дискретный алгоритм имитированной бифуркации (dSB) обладает наилучшим сочетанием скорости и точности для QUBO-задач на больших размерностях, что критично при анализе устойчивости сложных блокчейн-платформ и экосистем.

Было определено, как на основе вероятностной модели атак построить квадратичную целевую функцию $F(x)$, пригодную для решения методом имитированной бифуркации. Введены двоичные переменные для включения/отключения мер безопасности и различные штрафы. Такой подход позволяет учесть как одиночные уязвимости, так и их сочетания, и отдает предпочтение сбалансированным стратегиям защиты в рамках заранее определенного ресурсного бюджета.

Также было предложено сочетание квантово-вдохновленного оптимизатора с методом потенциальных игр. Дополнительная фаза игрового лучшего ответа обеспечивает достижение устойчивого решения и помогает избежать неполного учета некоторых взаимодействий между мерами. Теоретически обосновано, что игра с общим потенциалом сходится к локальному минимуму, а практические испытания показали повышение вероятности нахождения глобального минимума при нескольких запусках. Модифицированный алгоритм GdSB практически реализуем и сохраняет параллелизм вычислений.

В подтверждение указанным выше утверждениям была проведена экспериментальная апробация разработанной модификации алгоритма SB в контексте решаемой задачи. Несмотря на отсутствие практического выигрыша у dSB над SB, в силу недостаточно большого N, алгоритм GdSB дополнительно улучшал результат dSB в тех случаях, когда последний давал субоптимум, и зачастую показывал наилучший

результат. Это подтверждает целесообразность включения игрового этапа для повышения надежности оптимизации.

При этом настоящая работа исходит из модели угроз, заданной априорно вероятностями P_a . В реальных же системах оценка этих вероятностей может быть нетривиальной, и для нее может потребоваться целый ряд мер при калибровке модели на основе эмпирических данных вроде статистики атак или экспертных оценок. Кроме того, QUBO-модель может быстро расти по числу переменных, если учитывать очень много возможных мер, что может серьезно ограничить возможность реализации при существующих ресурсных ограничениях [13-15].

Также представляется перспективной интеграция предложенного подхода в системы мониторинга безопасности блокчейна. Таким образом можно построить адаптивную систему, которая периодически пересчитывает оптимальный набор защитных мер по мере появления новых уязвимостей или изменений в модели атак. Квантово-вдохновленные алгоритмы, благодаря своим качествам, могут применяться практически в режиме реального времени для подсказки операторам, какие именно меры усиления безопасности стоит внедрить в первую очередь.

Подводя итог, разработанный подход к оптимизации открывает новые возможности для анализа и обеспечения устойчивости блокчейн-систем, позволяя решать сложные задачи оптимизации, ранее считавшиеся труднореализуемыми, и тем самым обеспечивать устойчивость национальных блокчейн-платформ и экосистем перед лицом как традиционных, так и новых квантовых угроз.

Список использованных источников:

1. Петренко А.С., Петренко С.А. Метод оценивания квантовой устойчивости блокчейн платформ // Вопросы кибербезопасности. – 2022. – № 3 (49). – С. 3–22.

2. Петренко А.С. Метод анализа квантовой устойчивости национальных блокчейн экосистем и платформ // Защита информации. Инсайд. – 2025. – № 2 (122). – С. 18–27.

3. Петренко А.С. Решение оптимизационных задач обеспечения квантовой устойчивости национальных блокчейн платформ методом квантового отжига // Защита информации. Инсайд. – 2025. – № 3 (123). – С. 78–90.

4. Luke S. Essentials of Metaheuristics. – 2nd ed. – Fairfax: Lulu Press, 2013. – 242 p.

5. Johnson M.W., Amin M.H., Gilbert S., Lanting T., Hamze F., Dickson N., et al. Quantum annealing with manufactured spins // Nature. – 2011. – Vol. 473, no. 7346. – P. 194–198.

6. Hamerly R., Inagaki T., McMahon P.L., et al. Experimental investigation of performance differences between coherent Ising machines and a quantum annealer // Science Advances. – 2019. – Vol. 5, no. 5. – Art. eaau0823.

7. Inagaki T., Haribara Y., Igarashi K., Sonobe T., Tamate S., Honjo T., et al. A coherent Ising machine for 2000 node optimization problems // Science. – 2016. – Vol. 354, no. 6312. – P. 603–606.

8. Goto H., Tatsumura K., Dixon A.R. Combinatorial optimization by simulating adiabatic bifurcations in nonlinear Hamiltonian systems // Science Advances. – 2019. – Vol. 5, no. 4. – Art. eaav2372.

9. Tiunov E.S., Ulanov A.E., Lvovsky A.I. Annealing by simulating the coherent Ising machine // Optics Express. – 2019. – Vol. 27, no. 7. – P. 10288–10295.

10. Zeng Q.-G., Cui X.-P., Liu B., Wang Y., Mosharev P., Yung M.-H. Performance of quantum annealing inspired algorithms for combinatorial optimization problems // Communications Physics. – 2024. – Vol. 7. – Art. 249.

11. Goto H., Endo K., Suzuki M., Sakai Y., Kanao T., Hamakawa Y., et al. High performance combinatorial optimization based on classical mechanics // Science Advances. – 2021. – Vol. 7. – Art. eabe7953.

12. Kanao T., Goto H. Simulated bifurcation assisted by thermal fluctuation // Communications Physics. – 2022. – Vol. 5, no. 1. – Art. 153.

13. Петренко А.С. Метод построения постквантовых алгоритмов ЭЦП с двумя скрытыми группами / А.С. Петренко // Вопросы кибербезопасности. – 2025. – № 2 (58). – С. 52–63. – DOI: 10.21681/2311 3456 2025 2 52 63.

14. Молдовян Н.А., Петренко А.С. Алгебраический алгоритм ЭЦП с двумя скрытыми группами / Н.А. Молдовян, А.С. Петренко // Вопросы кибербезопасности. – 2024. – № 6. – С. 98–107. – DOI: 10.21681/2311 3456 2024 6 98 107.

15. Молдовян Н.А., Петренко А.С. Типовые уравнения верификации в алгебраических схемах ЭЦП с двумя скрытыми группами / Н.А. Молдовян, А.С. Петренко // Вопросы кибербезопасности. – 2025. – № 3 (67). – С. 8–20.

Petrenko A.S.
St. Petersburg Federal Research Center
of the Russian Academy of Sciences, St. Petersburg

Scientific supervisor:
Moldovyan N.A.
St. Petersburg Federal Research Center
of the Russian Academy of Sciences, St. Petersburg

OPTIMIZING THE SUSTAINABILITY OF NATIONAL BLOCKCHAIN PLATFORMS AND ECOSYSTEMS USING QUANTUM-INSPIRED ALGORITHMS

Abstract. The paper proposes a QUBO formulation of the problem of stability of blockchain systems with attack probabilities, resource constraints, and a penalty function. The dSB and HdSB algorithms have been adapted and a new GdSB algorithm has been developed to minimize risk. Experiments on problems with up to hundreds of variables show the superiority of GdSB over SB and its analogues in terms of accuracy, speed of finding and stability of solutions.

Keywords: blockchain, stability, quantum-inspired algorithms, simulated bifurcation, Ising model, quantum annealing, game theory, stability optimization

УДК 004.056.5:621.398

Повеликин В.Я., Машков И.А.
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина), Санкт-Петербург

Научный руководитель:
Силкин А.А.
НПКЦ «Новик-91», Егорьевск

ТЕХНОЛОГИЯ ЗАЩИТЫ ТЕЛЕМЕТРИЧЕСКОЙ ИНФОРМАЦИИ ЭЛЕМЕНТОВ МУЛЬТИАГЕНТНОЙ СИСТЕМЫ

Аннотация. В рамках проекта был разработан аппаратно-программный модуль для обеспечения конфиденциальности телеметрической информации мультиагентной системы. Работа была сосредоточена на анализе структуры телеметрии и внедрении микроконтроллеров с российскими алгоритмами шифрования, в результате чего был создан функциональный блок шифрования с новым

механизмом предотвращения потери данных при передаче большого объема данных. Успешная интеграция и тестирование подтвердили полную совместимость с программным обеспечением имеющейся системы и решение предыдущих проблем безопасности.

Ключевые слова: система, шифрование, криптография, магма, телеметрия

I. ВВЕДЕНИЕ

Задачей проекта являлось создание аппаратно-программного модуля (далее - АПМ), обеспечивающего конфиденциальность передаваемой телеметрической информации между элементами мультиагентной системы (далее - МАС).

Основной причиной создания данного блока послужила угроза несанкционированного перехвата управления МАС посредством глушения сигнала оператора и передачи команд на установку по радиоканалу для внесения изменений в систему. Ввиду отсутствия подходящих готовых решений на рынке было принято решение реализовать подобный блок, опираясь на технические требования и особенности уже существующей системы передачи информации, дополнив ее модулями шифрования.

Формально задача представляется следующим образом. Пусть дана система S вида: S=<V, H, X, Y, Z>, где V – внутренние условия функционирования, H – внешние условия функционирования, X – входной алфавит, Y – выходной алфавит, Z – функция преобразования, такая, что Z(X) = Y с соблюдением внутренних и внешний условий.

Входной алфавит может быть представлен в виде упорядоченного множества сообщений, при этом каждое сообщение представляет собой набор из N пакетов: X=(Message), Message=(Packet)^N, где N=11 либо N=14, в зависимости от внешних условий. К ним может относить активность системы позиционирования.

Каждый пакет имеет собственную строгую внутреннюю структуру, которую можно отобразить в виде упорядоченного множества элементов: Packet=(sb; id; info; sb).

При этом важно отметить, что длина поля info может варьироваться, а длина поля id строго фиксирована и составляет 1 байт – это является существенной особенностью для реализации алгоритма шифрования и представлено в виде внутренних условий функционирования.

К внутренним условиям может относиться длина информационной части пакета: len(info)∈[1;40] байт.

Общая длина пакета складывается из длины сообщения, строго определенных служебных байт и байта id в соответствии с определенной ранее структурой пакета: len(Packet)∈[5;44] байт.

Множество идентификаторов представляет собой неупорядоченное множество мощностью n, среди которых только два id строго определены и имеют важное значение для реализации последующего алгоритма шифрования: id={{id}^(n-2), id_sync, id_pp}.

Выходной алфавит представляет собой упорядоченное множество зашифрованных/расшифрованных сообщений. Структура пакета соответствует исходной структуре, но информационная часть сообщения преобразована. Важно отметить, что ее длина может не соответствовать длине исходного сообщения из-за особенностей блочного алгоритма шифрования: y=(Message_enc), Message_enc= (Packet_enc)^N, Packet_enc=(sb;id;info_enc; sb; sb), len(info_enc)∈[4; 40] байт.

Задача исследования: разработать такую функцию преобразования входного алфавита в выходной, что выполняется к ограничение сверху на время шифрования и на время расшифрования: Z: Z(X) → Y | time(Z(X) → Y) ≤ 0.1c

II. ОСНОВНАЯ ЧАСТЬ

В ходе анализа технического задания и документации было выявлено, что сообщения поступают с заданной периодичностью, состоят из структурированных пакетов с полезной нагрузкой до 40 байт и общим размером до 255 байт. При приеме наблюдалась фрагментация сообщений, что увеличивало количество входящих блоков данных.

Лимит полезной нагрузки в 40 байт и запрет на увеличение размера пакета определили выбор алгоритма «Магма» (ГОСТ Р 34.12-2015). Благодаря 8-байтному блоку данные делятся на 5 полных блоков без дополнения, тогда как шифры с 16-байтным блоком потребовали бы выравнивания, нарушающего заданный лимит. Выбор «Магмы» обоснован точным соответствием размера блока длине нагрузки, что позволяет шифровать данные целиком в штатном блочном режиме.

В связи выявленными закономерностями был составлен список алгоритмов, необходимых для реализации блока шифрования:

- Алгоритм приема информации от устройства, подключенного к интерфейсу,
- Алгоритм шифрования (расшифрования) информационной части пакета в зависимости от флага,
- Алгоритм восстановления сообщения и передачи информации, который собирает все зашифрованные или расшифрованные пакеты в структуру сообщения и передает далее по цепи передачи информации,
- Алгоритм организации очереди сообщений, который позволяет запоминать входящие сообщения в буфер в случае, если в данный момент

основная вычислительная мощность блока направленна на обработку другого входящего сообщения, что решает проблему потери сообщений.

После реализации аппаратной части решения был проведен ряд тестов. Один из которых – комплексная проверка функциональной целостности алгоритма шифрования в реальных условиях эксплуатации АПМ блока. Суть заключалась в организации замкнутого цикла обработки информации для подтверждения корректности всех этапов криптографического преобразования.

После сборки и подключения плата инициализируется. Тестовое сообщение (E) шифруется ключом в пакет (C) и выводится на выходной порт. Ретранслятор замыкает выход на вход, имитируя прием данных из внешней сети. АПМ расшифровывает полученный пакет. Полное совпадение результата с исходным сообщением (E) подтверждает корректность реализации криптоалгоритмов и работоспособность АПМ.

A. Измерение задержек

В ходе комплексного тестирования были получены временные задержки на шифрование пакетов разной длины, затем была выдвинута гипотеза о линейной зависимости времени шифрования и расшифрования пакетов, зависящей от длины входящих пакетов.

На рисунке 1 представлено наглядно, что время задержки зависит от длины сообщения, и зависимость практически линейная.

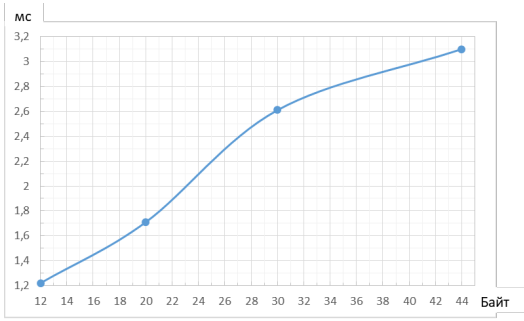


Рис. 1. Зависимость времени шифрования от длины сообщения

С использованием метода наименьших квадратов была выведена линейная аппроксимация этих значений, которая имеет вид $y \approx 0.0605x + 0.5568$.

III. ЗАКЛЮЧЕНИЕ

В ходе выполнения данной работы были проанализированы отечественные алгоритмы шифрования. Сделан выбор в пользу алгоритма шифрования «Магма» на основании особенностей передаваемой информации и технических требований заказчика.

Принято решение записывать входящую информацию в кольцевой буфер, для предотвращения потери сообщений, запись производить с помощью технологии прямого доступа к памяти (DMA), после чего последовательно производить обработку входящих сообщений и отправлять далее по цепи передачи информации.

Выполнена разводка платы и собран тестовый блок. Проведены успешные испытания тестового блока в режиме шифрования. Проведены испытания на оборудовании, замечаний и недочетов не выявлено.

Написано ПО для микроконтроллера, позволяющее получать, шифровать расшифровывать и передавать информацию.

Выполнен показатель достижения цели – среднее время шифрования 0,059с, дешифровки 0,052с, что соответствует требованиям технического задания.

Список использованных источников:

1. Kim, K., & Kang, Y. (2020). Drone security module for UAV data encryption. In 2020 International Conference on Information and Communication Technology Convergence (ICTC), pp. 1672-1674.
2. Patel, A. et al. (2025). Analysis of Light-Weight Cryptography Algorithms for UAV.
3. Secure Video and Telemetry FPGA Architecture For UAVs.
4. ГОСТ Р 34.12-2015. Информационная технология. Криптографическая защита информации. Блочные шифры.
5. STM32F401 Datasheet.
6. STM32F103C8 Datasheet.
7. Мартин Б. Чистый код: создание, анализ и рефакторинг.

Povelikin V.Y., Mashkov I.A.
Saint Petersburg Electrotechnical
University «LETI», Saint-Petersburg

Scientific supervisor:
Silkin A.A.
NPCC Novik-91, c. Yegoryevsk

TECHNOLOGY FOR PROTECTING TELEMETRY INFORMATION OF MULTI-AGENT SYSTEM ELEMENTS

Abstract. As part of this project, a hardware and software security module was developed to ensure the confidentiality of telemetry data of a multi-agent system. The work focused on analyzing the structure of telemetry and the implementation of microcontrollers with Russian encryption

algorithms, which resulted in the creation of a functional encryption unit with a new mechanism to prevent data loss when transferring large amounts of data. Successful integration and testing have confirmed full compatibility with the software of the existing system and the resolution of previous security issues.
Keywords: system, encryption, cryptography, magma, telemetry.

УДК 004.056

Ракипов Д.А.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Сенцова А.Ю.
Уфимский университет науки и технологий, Уфа

ZERO TRUST В ДЕЙСТВИИ: ПРАКТИЧЕСКИЙ ПОДХОД К ВНЕДРЕНИЮ АРХИТЕКТУРЫ НУЛЕВОГО ДОВЕРИЯ

Аннотация. В статье рассматривается практическое внедрение концепции Zero Trust. Представлена пошаговая дорожная карта: от инвентаризации активов и внедрения многофакторной аутентификации до микросегментации сети и непрерывного мониторинга. Проведен анализ эффективности на основе отчетов NIST и Gartner. Даны рекомендации по преодолению проблем интеграции с устаревшими системами.
Ключевые слова: Zero Trust, микросегментация, MFA, IAM, кибербезопасность, NIST SP 800-207.

Рост числа кибератак, направленных на обход классических средств защиты периметра, а также массовый переход на гибридные и облачные среды делают традиционную модель защиты периметра организации неэффективной. Злоумышленники все чаще получают легитимные учетные данные пользователей, что позволяет им беспрепятственно перемещаться внутри корпоративной сети. В ответ на эти вызовы архитектура Zero Trust («Никому не доверяй, всегда проверяй») перестала быть маркетинговым термином и стала обязательным элементом стратегии кибербезопасности современных организаций.

Zero Trust представляет собой не конкретный продукт, а стратегическую концепцию, основанную на принципе: **никогда не доверять, всегда проверять**. Ключевое отличие от классических моделей заключается в отказе от статичных правил доступа в пользу динамической оценки риска на основе идентификации, состояния устройства и контекста запроса. Цель данной статьи – представить

структурированное пошаговое руководство по внедрению принципов Zero Trust на практике.

1. От периметра к идентичности: смена парадигмы

Традиционная модель защиты подразумевала, что все, что находится внутри корпоративной сети (LAN), является безопасным, а все, что находится за периметром (WAN/Internet) – может быть потенциальным источником угроз. Эта модель сейчас теряет свою актуальность под влиянием следующих факторов:

1. **Удаленная работа:** Сотрудники подключаются к сети компании из дома, кафе или коворкингов, находясь вне защищенного периметра.
2. **Облачные сервисы (SaaS, IaaS):** Критичные данные могут храниться не на локальных серверах, а в AWS, Azure или Яндекс.Облаке.
3. **Атаки на цепочку поставок:** Компрометация доверенного подрядчика или обновления ПО сводит на нет защиту периметра.

Архитектура Zero Trust смещает фокус защиты с IP-адресов и подсетей на **идентичность (Identity)** и **данные**. Согласно документу NIST SP 800-207, лежащему в основе методологии, доступ предоставляется только после явной проверки и только на время, необходимое для выполнения конкретной задачи.

2. Пошаговая дорожная карта внедрения (Roadmap)

Внедрение Zero Trust – это не разовое мероприятие, а итеративный процесс. Попытка внедрить все компоненты сразу чаще всего приводит к непредсказуемым результатам. На основе анализа успешных кейсов можно выделить следующую последовательность действий.

Шаг 1: Формирование команды и инвентаризация активов. Прежде чем что-то защищать, необходимо понять, что именно необходимо защитить. На этом этапе создается рабочая группа из представителей ИБ и бизнес-отделов, а также проводится аудит всех информационных активов, пользователей, сервисных учетных записей и прав доступа к ним. Как показывает практика, до 30% учетных записей в домене могут быть неактивными или иметь избыточные права.

Шаг 2: Внедрение строгой аутентификации (MFA). Это самый быстрый и эффективный шаг. Необходимо в обязательном порядке внедрить многофакторную аутентификацию для всех критичных систем, VPN-подключений и облачных приложений. Рекомендуется отказ от SMS как второго фактора в пользу аппаратных токенов или TOTP (Google Authenticator, Яндекс.Ключ) ввиду уязвимости SIM-карт к подмене (SIM-swapping).

Шаг 3: Переход к микросегментации. Вместо плоской сети, где любой компьютер видит сервер баз данных, создаются изолированные сегменты (микропериметры). Например, бухгалтерия может работать только с сервером 1С, но не имеет доступа к серверу разработки. Для

этого используются либо межсетевые экраны нового поколения (NGFW), либо программно-определяемые решения (Software-Defined Perimeter).

Шаг 4: Обеспечение политики наименьших привилегий (PoLP). Необходимо пересмотреть права доступа к файловым ресурсам и приложениям. Внедрение Just-In-Time (JIT) доступа позволяет выдавать административные права только на время выполнения конкретной задачи с автоматическим отзывом через короткий промежуток времени.

Шаг 5: Непрерывный мониторинг и аналитика (SIEM/XDR). В модели Zero Trust недостаточно просто разрешить или запретить вход. Необходимо постоянно анализировать поведение пользователя. Если учетная запись бухгалтера в 3 часа ночи пытается скачать всю клиентскую базу – это аномалия, даже если пароль и токен были введены верно.

3. Анализ эффективности и подводные камни

Согласно отчетам аналитических компаний, организации, внедрившие принципы Zero Trust, отмечают снижение финансового ущерба от утечек данных и ускорение времени обнаружения инцидентов. Однако на пути внедрения существуют серьезные препятствия:

1. **Legacy-оборудование:** Около 66% организаций называют интеграцию с устаревшими промышленными системами (АСУ ТП) и старым ПО главной технической проблемой. Для таких систем часто приходится создавать «прокси-зоны» или виртуальные патчи.

2. **Сопротивление пользователей:** Постоянные запросы на подтверждение входа могут вызывать раздражение сотрудников, если не настроен Single Sign-On (SSO) или применены слишком жесткие политики безопасности.

3. **Отсутствие квалифицированных сотрудников:** Внедрение требует компетенций на стыке сетевой инженерии и управления доступом, которых часто не хватает в штате региональных компаний.

Заключение

Zero Trust – это не универсальный инструмент, а эволюционная стратегия снижения рисков. Начинать этот путь следует с наведения порядка в учетных записях и внедрения MFA, постепенно переходя к более сложным технологиям микросегментации. Практическая ценность подхода Zero Trust заключается в том, что он позволяет сдержать развитие атаки даже в случае компрометации одного из элементов инфраструктуры, что делает его обязательным для изучения современными специалистами по кибербезопасности.

Список использованных источников:

1. Rose S., Borchert O., Mitchell S., Connelly S. Zero Trust Architecture // NIST Special Publication 800-207. National Institute of Standards and

Technology. 2020. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf (дата обращения: 10.04.2026).

2. Multivocal literature review on zero-trust security implementation // Computers & Security. 2024. Vol. 141. URL: https://www.sciencedirect.com/science/article/abs/pii/S0167404824001287 (дата обращения: 10.04.2026).

3. Шкуропат Д. Архитектура Zero Trust в корпоративной сети: практические аспекты внедрения // IT Week. 2025. URL: https://www.itweek.ru/security/article/detail.php?ID=233733 (дата обращения: 10.04.2026).

4. Сдобникова И. Как внедрить Zero Trust: этапы, сложности и российская специфика // Anti-Malware.ru. 2025. URL: https://www.anti-malware.ru/practice/methods/How-to-implement-Zero-Trust (дата обращения: 10.04.2026).

5. Zero Trust. Защита начинается с недоверия // IT-World.ru. 2024. URL: https://www.it-world.ru/security/s4h4dwvfji80www4k8o8c4o80o8kw8w.html (дата обращения: 10.04.2026).

Rakipov D.A.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Sentsova A.Yu.
Ufa University of Science and Technology, Ufa

ZERO TRUST IN ACTION: A PRACTICAL APPROACH TO IMPLEMENTING ZERO TRUST ARCHITECTURE

Abstract. This article explores the concept of Zero Trust as an evolutionary stage in information security architecture. Unlike traditional perimeter-based models, Zero Trust assumes no implicit trust for any access subject. The focus is placed on practical implementation rather than theoretical foundations. A step-by-step roadmap is detailed, covering asset inventory, Multi-Factor Authentication (MFA) enforcement, network microsegmentation, and continuous monitoring. The paper provides a comparative analysis of Zero Trust implementation effectiveness based on open data and analytical reports. This article is aimed at students, aspiring cybersecurity specialists, and system administrators seeking to understand how to transition from slogans to actual infrastructure protection.

Keywords: Zero Trust, Microsegmentation, MFA, IAM, Cybersecurity, NIST SP 800-207.

УДК 004.94:544.42

Резбаев В.М.
Стерлитамакский филиал
Уфимского университета, Стерлитамак
Ахметов У.Р.
Российский государственный университет нефти и газа (национальный исследовательский университет) имени И.М Губкина, Москва

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

МОДЕЛИРОВАНИЕ И ПРОГНОЗИРОВАНИЕ ДИНАМИКИ ХИЩЕНИЙ ПЕРСОНАЛЬНЫХ ДАННЫХ НА ОСНОВЕ КИНЕТИЧЕСКИХ УРАВНЕНИЙ ХИМИЧЕСКИХ РЕАКЦИЙ

Аннотация. С использованием специализированного программного комплекса на базе генетических алгоритмов предложен оригинальный междисциплинарный подход. На основе анализа статистики за 2013-2025 гг. выявлена эволюция режимов компрометации данных: от линейного накопления инцидентов через диффузионные ограничения к фазе чистого автокатализа. Полученные модели позволяют перейти от статистического учета к превентивному прогнозированию рисков информационной безопасности.

Ключевые слова: информационная безопасность, утечки данных, генетический алгоритм, химическая кинетика, автокатализ.

Несмотря на интенсификацию государственного регулирования и внедрение новых механизмов защиты персональных данных (ПДн), эскалация киберугроз в российском сегменте достигла критических масштабов. По итогам 2024 года Россия закрепилась на второй позиции в глобальном антирейтинге по объему скомпрометированной информации, уступив лишь США [1].

Статистический анализ, проведенный экспертно-аналитическим центром InfoWatch, демонстрирует лавинообразный характер утечек: объем похищенных записей ПДн в 2024 году преодолел отметку в 47.24 млрд, что свидетельствует о беспрецедентном росте на 111.5% относительно показателей 2022 года.

Зафиксированное в 2025 году снижение общего числа инцидентов на 18% [2] не означает стабилизации ситуации. Напротив, характер угроз становится все более сложным и нелинейным, что указывает на качественную трансформацию методов кибератак. В этих условиях

стандартные статистические методы теряют свою прогностическую ценность. Это диктует необходимость перехода от простого количественного учета к глубокому математическому моделированию динамики киберугроз методами символьной регрессии.

Аппроксимация временного ряда выполнялась с помощью программного комплекса [3-4], использующего генетический алгоритм для подбора оптимальных кинетических уравнений. Метод позволяет сопоставлять динамику химического процесса с моделями нуклеации, диффузии и автокатализа и т.д.

Цель настоящей работы являлось применение разработанного «кинетического» подхода для мониторинга мировой ситуации в области утечек ПДн. Основной акцент сделан на выявлении скрытых динамических особенностей временного ряда похищенных записей.

Результаты аппроксимации показал следующие результаты:

Таблица 1

Результаты аппроксимации временных рядов Утекших данных ПДн

Период	R^2	F2	D3	C1	C2	F1	A2	B1	R2
2013-2016	0.88	0.98			~0	~0			
2017-2019	0.98				0.41		0.04	0.51	
2020-2023	0.63	0.90	0.09		0.01				
2023-2025	0.99			0.98				~0	~0

Анализ динамики весовых коэффициентов позволяет выделить четыре качественно различающихся этапов утечек ПДн:

Начальный этап (2013–2016 гг.) характеризуется высокой статистической значимостью функции F2. В рамках кинетического моделирования данный режим соответствует накоплению инцидентов. Практически нулевые значения автокаталитических коэффициентов свидетельствуют о том, что на данном этапе утечки носили изолированный характер: каждая компрометация данных была независимым событием, не оказывающим прямого влияния на вероятность возникновения последующих инцидентов.

Переходный период (2017-2019 гг.) отмечен качественным изменением структуры модели. Рост коэффициента C1 в сочетании с параметром B1 при высоком уровне аппроксимации указывает на возникновение центров нуклеации и разветвленных цепных реакций. Процесс хищения ПДн перестал быть линейным, демонстрируя первые признаки каскадного распространения угроз, где успешная компрометация одной системы создает условия для серии сопряженных атак.

В интервале 2020-2023 гг. наблюдается снижение точности аппроксимации при появлении значимого веса функции D3. С точки зрения математической модели, это интерпретируется как переход в диффузионную область, где скорость роста ограничивается внешними барьерами и сопротивлением среды. Динамика процесса в этот период лимитировалась не интенсивностью атак, а скоростью их «диффузии» через усложнившиеся контуры защиты информации, что приводило к временной стабилизации объемов хищений. Данный период можно охарактеризовать пандемией вызванный Covid-19, уход на дистанционную работу вынудил применять все более современные средства защиты от кибер-атак [5].

Наиболее критическая динамика зафиксирована в периоде 2023-2025 гг. Расчеты демонстрируют практически идеальную сходимость с моделью чистого автокатализа C1. Это математически подтверждает взрывной рост объема похищенных записей на 111.5% (до 47.24 млрд единиц в 2024 г.). Несмотря на локальные колебания общего числа инцидентов в 2025 году, характер угроз стал самоподдерживающимся. Современная система ИБ столкнулась с режимом, в котором каждая утечка ПДн выступает катализатором для последующих автоматизированных взломов. Таким образом, процесс перешел в фазу, где объем скомпрометированных данных является функцией от уже похищенных массивов информации.

Использование адаптированного программного комплекса [3] позволило математически подтвердить, что текущий этап (2023–2025 гг.) является наиболее критическим, так как динамика утечек приобрела характер автокаталитического процесса, требующего принципиально новых, опережающих методов защиты, отличных от мер противодействия линейным угрозам прошлых лет.

Список использованных источников:

1. Утечки информации в мире, 2022–2023 годы: отчет / Экспертно-аналитический центр InfoWatch. – 2024. – URL: infowatch.ru (дата обращения: 17.04.2025). – Текст: электронный.

2. Не победа ИБ: количество утечек персональных данных в 2025 г. снизилось, но не благодаря ИБ // ComNews: информационный портал. – 2026. – 13 марта. – URL: https://www.comnews.ru/content/244202/2026-03-13/2026-w11/1008/ne-pobeda-ib-kolichestvo-utechek-personalnykh-dannykh-2025-g-snizilos-no-ne-blagodarya-ib (дата обращения: 17.04.2025). – Текст: электронный.

3. Программный комплекс сегментированного моделирования данных по термической деструкции генетическим алгоритмом: свидетельство о государственной регистрации программы для ЭВМ №

2026616287 Рос. Федерация / Э. Р. Гиззатова, С. И. Никонова, А. А. Корнилова; заявитель и правообладатель ФГБОУ ВО «Уфимский университет науки и технологий». – № 2026615000; заявл. 03.03.2026; опубл. 05.03.2026.

4. Программа для интеллектуального анализа кинетических закономерностей полимерных систем на основе методов глобальной оптимизации: свидетельство о государственной регистрации программы для ЭВМ № 2026616598 Рос. Федерация / Э. Р. Гиззатова, С. И. Никонова, А. А. Корнилова; заявитель и правообладатель ФГБОУ ВО «Уфимский университет науки и технологий». – № 2026615500; заявл. 03.03.2026; опубл. 10.03.2026.

5. Корнилова, А. А. Обзор кибератак в период пандемии Covid-19 / А. А. Корнилова, Д. С. Юнусова // 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. 25-27. – DOI 10.33184/itokbco-2021-05-21.4.

Rezbaev V.M.
Sterlitamak Branch of Ufa University, Sterlitamak
Akhmetov U.R.
Gubkin Russian State University of Oil
and Gas (National Research University), Moscow

Scientific supervisor:
Kornilova A.A.
Ufa University of Science and Technology, Ufa

MODELING AND FORECASTING THE DYNAMICS OF PERSONAL DATA THEFT BASED ON KINETIC EQUATIONS OF CHEMICAL REACTIONS

Abstract. Using a specialized software package based on genetic algorithms, an original interdisciplinary approach is proposed. Based on the analysis of statistics for 2013–2025, the evolution of data compromise modes was identified: from linear accumulation of incidents through diffusion limitations to a phase of pure autocatalysis. The resulting models allow for a transition from statistical accounting to preventive forecasting of information security risks.

Keywords: information security, data leaks, genetic algorithm, chemical kinetics, autocatalysis.

УДК 004

Сорокин К.Д.
Уфимский университет науки и технологий, Уфа

Научный руководитель
Салов И.В.
Уфимский университет науки и технологий, Уфа

УГРОЗА АППАРАТНОГО СБРОСА ПАРОЛЯ BIOS

Аннотация. В статье рассматривается актуальная проблема информационной безопасности, связанная с возможностью аппаратного сброса пароля BIOS на современных вычислительных платформах. Анализируются технические механизмы защиты прошивок, уязвимости, возникающие при неправильной реализации систем аутентификации на уровне firmware, векторы атак через физический доступ, эксплуатацию DMA-интерфейсов и манипуляции с энергонезависимой памятью. Представлен обзор реальных инцидентов компрометации BIOS/UEFI. Особое внимание уделено российскому контексту информационной безопасности критической инфраструктуры, включая анализ отечественных решений типа «БИОС-За» и требований регуляторов.

Ключевые слова: BIOS, UEFI, firmware, аппаратный сброс пароля, информационная безопасность, критическая инфраструктура, доверенная загрузка, Intel Boot Guard, TPM.

BIOS и его современная реализация UEFI представляют собой критически важный уровень любой вычислительной системы, поскольку именно они запускаются первыми и контролируют начальные этапы загрузки [1]. Если злоумышленник получает контроль на этом уровне, он фактически обходит все механизмы защиты операционной системы. Это делает атаки на firmware особенно опасными [1].

Долгое время пароль BIOS считался простой, но эффективной мерой защиты от несанкционированного доступа. Однако практика показала, что эта мера обеспечивает лишь базовый уровень безопасности и легко обходится [2].

Исторически слабость защиты была связана с тем, что пароли хранились в CMOS-памяти, зависимой от батарейки [2]. Даже несмотря на переход к более современным способам хранения в UEFI, сама проблема не исчезла – она просто стала технически сложнее [1].

Несмотря на развитие технологий, ряд фундаментальных проблем остается актуальным. Наиболее значимыми из них являются: хранение паролей в небезопасном виде или с использованием устаревших хеш-

функций, разделение памяти прошивки и пользовательских настроек, доступность аппаратных интерфейсов (I²C, SPI), через которые можно читать и изменять данные, недостаточная защита от прямого доступа к микросхемам памяти [2].

Физический доступ остается ключевым фактором риска. В отличие от программных атак, он дает почти неограниченные возможности: от простого сброса настроек до внедрения вредоносного кода в прошивку [3]. Такой код работает в привилегированных режимах процессора (например, SMM), которые находятся вне контроля операционной системы [1]. Это означает, что даже продвинутые средства защиты не способны его обнаружить.

При этом современные атаки все чаще выходят за рамки физического доступа. Уязвимости в системах удаленного управления позволяют атаковать firmware дистанционно [1]. Компоненты вроде BMC или Intel Management Engine создают дополнительные точки входа, и при их компрометации злоумышленник получает доступ на уровень ниже ОС [1].

Основные векторы атак являются: аппаратный сброс или изменение пароля через доступ к памяти, модификация прошивки с внедрением вредоносного кода, использование уязвимостей в системах удаленного администрирования, атаки на этапе поставки оборудования (supply chain) [1].

Особую опасность представляют последние, так как пользователь получает уже скомпрометированное устройство [1].

Реальные инциденты подтверждают серьезность проблемы. Вредоносные прошивки способны сохраняться в системе годами, переживать переустановку операционной системы и использоваться для скрытого наблюдения [4]. Такие атаки применяются не только государственными структурами, но и коммерческими разработчиками spyware [1].

Для противодействия этим угрозам используются аппаратные механизмы, формирующие «цепочку доверия» при загрузке системы [1]. Их задача – гарантировать, что выполняется только проверенный код. К ключевым решениям относятся: технологии проверки целостности загрузчика (например, Boot Guard), использование доверенных модулей (TPM 2.0), изолированные процессоры безопасности (например, в архитектуре AMD), системы автоматического восстановления прошивки (PFR) [1].

Защита должна начинаться именно с уровня firmware. Средства безопасности операционной системы начинают работать слишком поздно и не способны предотвратить атаки на BIOS [1].

Отдельного внимания заслуживает использование отечественных решений в контексте критической инфраструктуры [5]. Они позволяют повысить контроль над системой и соответствовать требованиям регуляторов, однако полностью не устраняют риски, связанные с использованием зарубежной аппаратной базы.

Технические средства защиты эффективны только в сочетании с грамотной организацией процессов. На практике это означает: строгий контроль физического доступа к оборудованию, использование сложных и уникальных паролей BIOS, регулярный аудит настроек и версий прошивки, контроль источников обновлений firmware, обучение персонала и подготовку к реагированию на инциденты [3].

При подозрении на компрометацию важно понимать, что обычные меры вроде переустановки операционной системы не помогают. Единственным надежным способом восстановления является полная перепрошивка BIOS с использованием доверенного источника [1].

Аппаратный сброс пароля BIOS – это не просто частная уязвимость, а показатель более глубокой проблемы: недостаточной защищенности уровня firmware. Современные атаки показывают, что этот уровень становится одной из главных целей злоумышленников.

Эффективная защита возможна только при комплексном подходе, который включает: аппаратные механизмы контроля целостности, организационные меры, контроль физического доступа, и постоянный аудит состояния системы.

Именно firmware сегодня становится критической точкой доверия всей информационной инфраструктуры.

Список использованных источников:

1. Shade BIOS 2025: анализ угроз UEFI и многоуровневая защита критической инфраструктуры [Электронный ресурс]. URL: https://codeby.net/threads/shade-bios-2025-analiz-ugroz-uefi-i-mnogourovnevaya-zashchita-kriticheskoi-infrastruktury.89849/ (дата обращения: 02.04.2026).

2. Аппаратный взлом для обхода паролей BIOS [Электронный ресурс]. URL: https://habr.com/ru/articles/741992/ (дата обращения: 02.04.2026).

3. Protection Against Physical Attacks [Электронный ресурс]. URL: https://mail.whonix.org/wiki/Protection_Against_Physical_Attacks/ (дата обращения: 09.04.2026).

4. Найдены уязвимые BIOS на ноутбуках Clevo и Gigabyte [Электронный ресурс]. URL: https://www.itsec.ru/news/naydeno-uyazvimoye-bios-na-noutbukah-clevo-i-gigabyte/ (дата обращения: 05.04.2026).

5. Суверенный BIOS – новая ниша для отечественных разработчиков [Электронный ресурс]. URL: https://www.comnews.ru/content/238568/2025-04-01/2025-w14/1008/suverennyy-bios-novaya-nisha-dlya-otechestvennykh-razrabotchikov/ (дата обращения: 13.04.2026).

Sorokin K.D.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Salov I.V.
Ufa University of Science and Technology, Ufa

THREAT OF BIOS PASSWORD RESET

Abstract. The article discusses the current problem of information security related to the possibility of hardware resetting the BIOS password on modern computing platforms. It analyzes the technical mechanisms of firmware protection, vulnerabilities that arise from improper implementation of firmware-level authentication systems, and attack vectors through physical access, exploitation of DMA interfaces, and manipulation of non-volatile memory. The article provides an overview of real-world incidents of BIOS/UEFI compromise. Special attention is given to the Russian context of information security in critical infrastructure, including an analysis of domestic solutions such as BIOS-Za and regulatory requirements.

Keywords: BIOS, UEFI, firmware, hardware password reset, information security, critical infrastructure, trusted boot, Intel Boot Guard, TPM, SMM mode.

УДК 004.056

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

Научный руководитель:
Сенцова А.Ю.
Уфимский университет науки и технологий, Уфа

АТАКИ НА СЕТИ КОМПАНИЙ: АНАЛИЗ, ЭКСПЛУАТАЦИЯ И ЗАЩИТА ОТ SSRF-УЯЗВИМОСТЕЙ НА ПРИМЕРЕ МИКРОСЕРВИСНОЙ АРХИТЕКТУРЫ

Аннотация Данная статья рассматривает популярные для веб-приложений SSRF-уязвимости. Приведен пример эксплуатации

уязвимости в локальной микросервисной архитектуре, описаны способы защиты от данного вида атак.

Ключевые слова: SSRF-уязвимость, защита данных, микросервисная архитектура, веб-приложения.

С развитием микросервисной архитектуры и бессерверных вычислений, периметр корпоративной сети размывается [1]. Уязвимости SSRF возникают, когда приложение доверяет входным данным пользователя и позволяет им влиять на запросы к удаленным ресурсам, таким как базы данных, веб-серверы и API. Если злоумышленник получит контроль над этими запросами, это может привести к серьезным последствиям для безопасности. Классическая SQL-инъекция позволяет украсть базу данных, в то время как SSRF часто открывает путь ко всей внутренней инфраструктуре, минуя межсетевые экраны и системы сетевой сегментации.

В статье рассмотрена SSRF-уязвимость, ее типы, цели эксплуатации и развернут локальный стенд, для демонстрации того, как уязвимость может превратить легитимный функционал приложения в брешь для доступа к внутренним метаданным.

Типы SSRF:

- Blind SSRF. Сервер отправляет запрос, но не возвращает его тело в ответе пользователю. Тем не менее, факт запроса можно отследить по задержкам, DNS-логам или ошибкам подключения.
- Semi-Blind SSRF. Злоумышленник видит лишь часть ответа или ограниченные данные, такие как: уведомления об ошибках, статус-код, фрагменты содержимого ответа. Для проведения атак ему понадобится дальнейшее изучение системы.
- Full-Read SSRF. Атакующий получает содержимое ответа от целевого внутреннего ресурса (самый опасный тип уязвимости).

Целями для атак через уязвимость являются Cloud Metadata API (эндпоинты вроде 169.254.169.254 (AWS, GCP, Azure, Yandex Cloud), где хранятся секреты, IAM-роли и ключи доступа), внутренние сервисы (Redis, Elasticsearch, Docker API, базы данных, не имеющие публичного доступа), внутренние панели администрирования. Злоумышленники могут использовать SSRF для сканирования внутренних сетей. При этом традиционные механизмы защиты (межсетевые экраны, системы обнаружения вторжений) бессильны, ведь запросы выполняются от имени сервера.

Для демонстрации возможностей уязвимости, был развернут локальный стенд, с помощью Python созданы файлы, имитирующие внутренний микросервис (содержит несколько эндпоинтов, порт 5000) и уязвимое веб-приложение (сервис проверки URL, который принимает от

пользователя произвольный адрес, выполняет HTTP-запрос и возвращает ответ, порт 8080) с отсутствием валидации пользовательского ввода. Структура стенда представлена на рис. 1.



Рис.1. Структура локального стенда

При тестировании через браузер, на странице уязвимого веб-приложения (http://127.0.0.1:8080) в поле ввода вводится URL (например, http://127.0.0.1:5000/health) и нажимается кнопка «Проверить». Уязвимое приложение выполняет запрос к внутреннему API и возвращает его ответ. SSRF-атака успешно проведена. Так, потенциальный злоумышленник вводит различные URL и получает необходимые данные – тестовые AWS-ключи, пароль базы данных, информацию о здоровье внутреннего API, список пользователей, конфигурацию системы или, как видно на рис. 2, API-ключи.

Для автоматизации атаки могут создаваться полноценные эксплойты, которые перебирают все эндпоинты внутреннего API через уязвимое приложение и выводят полученную информацию в отформатированном виде, без постоянного участия злоумышленника. Уязвимость также позволяет провести сканирование портов и обнаружить открытые порты на локальном хосте [2].

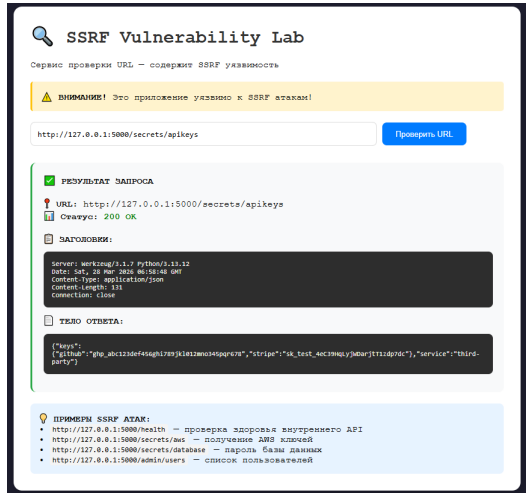


Рис. 2. Получение API-ключей с помощью уязвимости SSRF

Для защиты от SSRF-уязвимости в веб-приложении необходимо реализовать следующие меры: разрешить только протоколы HTTP и HTTPS; запретить адреса localhost (127.0.0.1), loopback; запретить приватные IP-диапазоны, использовать белый список разрешенных доменов. Защищенное приложение (порт 8081) при попытке ввода некорректного URL выводит сообщение о блокировке доступа (см. рис. 3).

Валидация ввода в защищенном приложение позволяет обеспечить безопасность метаданных от атак с помощью уязвимости SSRF.

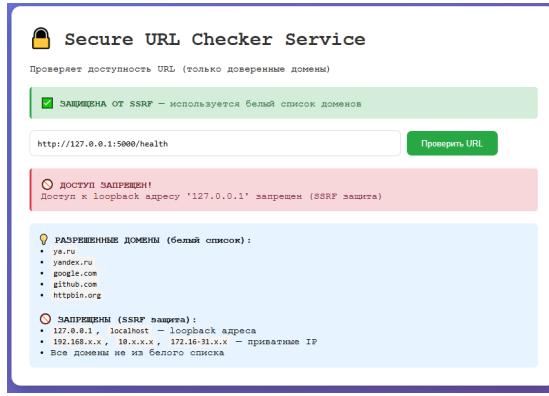


Рис. 3. Сообщение о запрете доступа в защищенном приложении

Таким образом, защита от SSRF-уязвимости является важным аспектом безопасности для современных распределенных сетей в условиях размытия сетевого периметра. Основные принципы безопасности веб-приложений включают защиту на этапе ввода и вывода данных, валидацию входящей информации, ограничение доступа к ресурсам и использование шифрования [3]. Следует на этапе разработки обращать внимание на встраиваемые возможности и верную настройку сервисов, чтобы исключить возможность исследования и атаки на инфраструктуру [4].

Список использованных источников:

1. Меметов, М. Р. Будущее корпоративной безопасности: Zero Trust и Защита данных в распределенных системах / М. Р. Меметов // Информационно-компьютерные технологии в экономике, образовании и социальной сфере. – 2025. – № 4(50). – С. 121-128.

2. Ильин, Р. А. Server-Side Request Forgery: Угрозы и методы защиты / Р. А. Ильин // Научный Альманах ассоциации France-Kazakhstan. – 2024. – № 4. – С. 282-288.

3. Алисултанова, И. А. Безопасность веб-приложений и методы предотвращения хакерских атак / И. А. Алисултанова, Д. Х. Джабраилов // Экономика и управление: проблемы, решения. – 2025. – Т. 3, № 3(156). – С. 35-42. – DOI 10.36871/ek.up.p.r.2025.03.03.005.

4. Где и как искать этот ваш SSRF: первые шаги в багхантинге // Habr [Электронный ресурс] - URL: https://habr.com/ru/companies/pt/articles/842598/ (дата обращения: 15.03.2026).

Fayzullina A.S.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Sentsova A.U.
Ufa University of Science and Technology, Ufa

ATTACKS ON COMPANY NETWORKS: ANALYSIS, OPERATION, AND PROTECTION AGAINST SSRF VULNERABILITIES USING MICROSERVICE ARCHITECTURE AS AN EXAMPLE

Abstract. This article discusses SSRF vulnerabilities that are popular for web applications. It provides an example of exploiting a vulnerability in a local microservice architecture and describes how to protect against this type of attack.

Keywords: SSRF vulnerability, data protection, microservice architecture, and web applications.

УДК 004.056.5

Фатеев Р.Р.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Сенцова А.Ю.
Уфимский университет науки и технологий, Уфа

ПРОГРАММНЫЙ КОМПЛЕКС «ROUTERSENTRY» ДЛЯ АУТЕНТИФИКАЦИИ ДОМАШНИХ WI-FI МАРШРУТИЗАТОРОВ НА ОСНОВЕ АППАРАТНЫХ ХАРАКТЕРИСТИК

Аннотация. В статье представлен программный комплекс «RouterSentry», предназначенный для защиты домашних и малых офисных сетей от атак типа «злой двойник» (Rogue AP). Комплекс реализует механизм аутентификации «Свой/Чужой», основанный на анализе уникальных аппаратных параметров маршрутизатора – дрейфа тактовой частоты (Clock Skew) и его беспроводного окружения. Описаны архитектура программы, алгоритмы сбора эталонных данных и процедура верификации, обеспечивающие высокую надежность обнаружения подменных устройств без использования специализированного оборудования.

Ключевые слова: Кибербезопасность, Wi-Fi, аутентификация, дрейф тактовой частоты, Rogue Access Point, аппаратный отпечаток.

Распространенность атак с использованием подставных точек доступа делает уязвимыми домашние сети рядовых пользователей. Стандартные методы защиты не эффективны против спуфинга MAC-адресов и SSID. В данной работе предлагается программное решение, переносящее принцип биометрической аутентификации на сетевые устройства. Программа не требует установки специализированного ПО на маршрутизатор, что делает решение универсальным.

1. Архитектура программного комплекса

Программный комплекс «RouterSentry» состоит из двух основных модулей, реализованных в виде десктопного приложения для ОС Windows/Linux/macOS:

1. Модуль Профилирования (The Profiler). Ответственен за первичный сбор эталонных данных о легитимном маршрутизаторе.

2. Модуль Верификации (The Verifier). Выполняет текущую проверку активного сетевого шлюза, сравнивая его характеристики с эталоном.

Оба модуля взаимодействуют с сетевым интерфейсом компьютера и используют библиотеки для низкоуровневого анализа сетевых пакетов (например, libpcap).

2. Алгоритм работы программы

2.1. Фаза инициализации и сбора эталона

Пользователь запускает Модуль Профилирования и указывает IP-адрес своего домашнего маршрутизатора. Программа последовательно выполняет два типа активных и пассивных зондирований.

2.1.1. Измерение дрейфа тактовой частоты (Clock Skew):

Метод: Программа отправляет на маршрутизатор серию из нескольких сотен ICMP-запросов (ping) или TCP-SYN пакетов с фиксированным интервалом.

Обработка данных: Каждый ответный пакет от маршрутизатора содержит временную метку (TCP- timestamp) или время приема фиксируется на стороне программы с использованием системных высокоточных часов.

Вычисление отпечатка: Алгоритм строит график временных задержек ответов. Из-за несовершенства кварцевого резонатора маршрутизатора, его внутренние часы идут с уникальной микроскопической погрешностью. Эта погрешность не случайна, а имеет стабильный характер. Для ее вычисления программа применяет линейную регрессию к полученным временным меткам, определяя угол наклона (skew) результирующей прямой. Именно этот наклон, измеряемый в миллионных долях секунды (ppm), является уникальным **аппаратным отпечатком** (Clock Skew) конкретного экземпляра маршрутизатора [2].

Физическая основа: Данный параметр обусловлен технологическими вариациями при производстве кварцевых резонаторов и является стабильным на протяжении всего срока службы устройства, а также слабо зависит от температуры и нагрузки. Подделать его дистанционно невозможно.

2.1.2. Сканирование и анализ беспроводного окружения:

Метод: Программа переводит Wi-Fi-адаптер компьютера в режим мониторинга (monitor mode) и в течение 2-3 минут passively («прослушивает») эфир на всех каналах.

Обработка данных: Собираются все кадры управления и контроля от всех видимых точек доступа. Для каждой уникальной сети извлекается ее BSSID (реальный MAC-адрес) и средняя мощность принимаемого сигнала (RSSI).

Формирование эталона: На основе собранных данных создается «цифровой слепок» (Radio Frequency Fingerprint) окружения. Эталоном является упорядоченный список пар [BSSID, RSSI], отсортированный по мощности сигнала. Данная картина уникальна для местоположения маршрутизатора в пространстве.

Полученные эталонные значения (Clock Skew и список окружения) шифруются и сохраняются в локальной базе данных программы.

2.2. Фаза активной верификации

Обнаружение шлюза: Программа определяет текущий IP-адрес сетевого шлюза (маршрутизатора) через системную таблицу маршрутизации.

Повторное измерение: Модуль Верификации повторяет процедуры, описанные в п. 2.1.1 и 2.1.2: отправляет серию пакетов для вычисления, текущего Clock Skew и сканирует эфир для получения актуальной карты окружения.

Сравнение Clock Skew: рассчитывается разница между текущим измеренным skew и эталонным. Если отклонение превышает экспериментально установленный порог (например, 0.1 ppm), маршрутизатор считается подозрительным.

Сравнение окружения: Текущий список BSSID и RSSI сравнивается с эталонным с помощью алгоритма взвешенного сходства.

Вынесение вердикта: на основе комбинации двух факторов программа присваивает соединению статус: **LEGITIMATE» (Свой):** Оба параметра в пределах нормы; **«SUSPICIOUS» (Подозрительный):** Незначительные отклонения; **«ROGUE» (Чужой):** Обнаружено значительное несовпадение Clock Skew.

При обнаружении статуса «ROGUE» программа блокирует трафик через данный шлюз средствами межсетевого экрана и уведомляет пользователя.

Обоснование эффективности и практическая реализация

Устойчивость к спуфингу: Злоумышленник может скопировать MAC-адрес и SSID, но не может изменить физические свойства кварцевого резонатора атакуемого маршрутизатора. Измерение Clock Skew проводится активно, с рабочей станции пользователя, что делает атаку невидимой для злоумышленника.

Пространственная привязка: Проверка окружения обеспечивает дополнительный контекст. Для успешной атаки злоумышленнику необходимо разместить подставной маршрутизатор в непосредственной близости от жертвы, чтобы воспроизвести идентичную картину сигналов, что резко повышает риск его обнаружения.

Ресурсоемкость: Алгоритмы не требуют значительных вычислительных мощностей. Основные операции – отправка сетевых

пакетов и статистическая обработка временных рядов, что по силам любому современному ПК или ноутбуку.

Программный комплекс «RouterSentry» обеспечивает надежную аутентификацию сетевых устройств для массового пользователя на основе неуязвимых для удаленного спуфинга аппаратных характеристик, что делает его высокоэффективным средством против атак «злой двойник». Развертывание не требует модификации маршрутизатора или дополнительного оборудования, позволяя широко применять его для защиты домашних и малых офисных сетей.

Список использованных источников:

1) Kohno T., Broido A., Claffy K.C. Remote physical device fingerprinting // IEEE Symposium on Security and Privacy. 2005. URL: https://ieeexplore.ieee.org/document/1425124 (дата обращения: 01.02.2026).

2) Jana S., Kasera S.K. On Fast and Accurate Detection of Unauthorized Wireless Access Points Using Clock Skews // IEEE Transactions on Mobile Computing. 2010. Vol. 9, no. 6. URL: https://ieeexplore.ieee.org/document/5404349 (дата обращения: 01.02.2026).

3) Corbett C., Beyah R., Copeland J. Passive Classification of Wireless NICs during Active Scanning // International Journal of Digital Crime and Forensics. 2010. Vol. 2, no. 3. URL: https://www.igi-global.com/article/passive-classification-wireless-nics-during/51588 (дата обращения: 01.02.2026).

Fateev R.R.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Sentsova A.Yu.
Ufa University of Science and Technology, Ufa

ROUTERSENTRY SOFTWARE PACKAGE FOR AUTHENTICATION OF HOME WI-FI ROUTERS BASED ON HARDWARE CHARACTERISTICS

Abstract. The article presents the RouterSentry software package designed to protect home and small office networks from Rogue AP attacks. The complex implements a "Friend/Foe" authentication mechanism based on the analysis of the router's unique hardware parameters – clock drift (Clock Skew) and its wireless environment. The architecture of the program, algorithms for collecting reference data and the verification procedure are

described, ensuring high reliability of detection of replacement devices without the use of specialized equipment.

Keywords: cybersecurity, Wi-Fi, authentication, clock frequency drift, Rogue Access Point, hardware fingerprint.

УДК 004.056.53

Фесько Н.В.
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина), Санкт-Петербург

Научный руководитель:
Шульженко А.Д.
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина), Санкт-Петербург

ПРОБЛЕМЫ РЕФЛЕКТОМЕТРИИ И ПРЕДЛОЖЕНИЕ ПО ПОИСКУ ВЕЙВЛЕТОВ ДЛЯ АВТОМАТИЗАЦИИ АНАЛИЗА

Аннотация. В статье рассмотрены проблемы рефлектометрии: слепая зона, погрешности, чувствительность к шумам. Выявлено отсутствие механизма автоматического выявления подключений и дефектов в российских рефлектометров, что приводит к субъективности оператора и погрешности до 50%. Предложен подход на основе Python-скрипта для автоматического наложения рефлектограмм и выявления отклонений, позволяющий исключить человеческий фактор, сократить время анализа и повысить точность обнаружения подключений и дефектов.

Ключевые слова: рефлектометрия, информационная безопасность, выявление подключений, незадекларированные подключения

Рефлектометрия является одним из основных методов поиска несанкционированных подключений и повреждений в металлических кабельных линиях. Однако при работе с рефлектометрами может возникнуть ряд проблем: наличие слепой зоны, чувствительность к шумам, погрешность, а также субъективность анализа рефлектограмм. Особенно остро стоит проблема отсутствия в большинстве российских рефлектометров формального механизма сравнения текущих рефлектограмм с эталонной базовой линией. Как показал анализ 9 приборов (Программно-аппаратный комплекс «СИРИУС-МК», Рефлектометр «ИРК-ПРО Гамма Е», РЕЙС-45, РЕЙС-50, РЕЙС-100, РЕЙС-105М1, РЕЙС-205, РЕЙС-305, РЕЙС-405), ни один из них не имеет полностью автоматизированного сравнения рефлектограмм. Оператор

вынужден вручную проводить анализ и субъективно оценивать отклонения, из-за этого увеличивается время принятия решения, существуют расхождения в результатах, принятых разными операторами, и погрешность измерения может достигать 50% у отдельных устройств [1]. В работе предлагается подход к автоматизации анализа рефлектограмм с использованием кода на Python, реализующего наложение текущей рефлектограммы на эталонную базовую линию для визуализации различий.

На основе сравнения семи методов рефлектометрии (TDR, ARM, ICE/Decay, WTDR, FDR, STDR, SSTDR) выявлены следующие ограничения:

- Слепая зона из-за наложения отраженного сигнала на падающий [2];
- Погрешность измерения расстояния в зависимости от прибора;
- Чувствительность к шумам;
- Отсутствие механизма автоматического выявления подключений и дефектов в большинстве российских рефлектометров (см. табл. 1).

Таблица 1

Анализ наличия механизма сравнения текущей рефлектограммы с базовой линией в российских рефлектометрах

Название прибора	Функция сохранения снятой рефлектограммы	Механизм сравнения рефлектограммы с базовой линией
Программно-аппаратный комплекс «СИРИУС-МК»	Есть	Отсутствует
Рефлектометр «ИРК-ПРО Гамма Е»	Есть	Есть, требует работа оператора для выявления дефектов и подключений
РЕЙС-45	Есть	Есть, нужна работа оператора для выявления дефектов и подключений
РЕЙС-50	Есть (до 20 рефлектограмм)	Есть (режим наложения), требуется работа оператора для выявления дефектов и подключений
РЕЙС-100	Отсутствует	Отсутствует
РЕЙС-105М1	Есть (более 200 рефлектограмм)	Есть (сравнение/вычитание), требуется оператор для выявления дефектов и подключений
РЕЙС-205	Есть	Есть, требуется оператор для выявления дефектов и подключений
РЕЙС-305	Есть	Есть (режим наложения), требуется работа оператора для выявления дефектов и подключений
РЕЙС-405	Есть (более 1000 рефлектограмм)	Есть (режим наложения/разности сигналов), требуется оператор для выявления дефектов и подключений

Даже при наличии функции сравнения оператор вынужден самостоятельно выявлять отклонения, что вносит субъективность и увеличивает время диагностики.

Для устранения указанных недостатков предлагается автоматизированное наложение рефлектограмм с использованием скрипта на Python. Алгоритм работы следующий: загрузка эталонной и текущей рефлектограмм, построение двух графиков на одной координатной плоскости с разными цветами и автоматическое выделение отклонений. Предложенный подход позволяет исключить субъективность, связанную с человеческим фактором, поскольку сравнение графиков выполняется программой автоматически. Время анализа сокращается, так как оператору не нужно искать отклонения рефлектограмм самостоятельно. Повышается точность обнаружения изменений состояния линии, особенно при слабых отражениях, которые на глаз заметить сложно. Обеспечивается полная воспроизводимость результатов – при повторном анализе тех же данных вывод будет идентичным. Кроме того, реализация не требует сложного математического аппарата или дорогостоящего дополнительного оборудования, достаточно любого компьютера с установленным Python.

Для апробации методики сконструирован стенд, позволяющий имитировать: короткое замыкание, обрыв линии, отсутствие заземления и подключение устройств в розетки. Стенд обеспечивает получение рефлектограмм для каждого типа неоднородности, которые затем используются для последующего автоматического сравнения.

Таким образом, основной проблемой рефлектометрии является отсутствие автоматизированного механизма сравнения рефлектограмм, что приводит к субъективности оператора. Предложенный подход позволяет:

- автоматически накладывать текущую рефлектограмму на эталонную базовую линию;
- выделять места отклонений (потенциальные дефекты или подключения);
- снизить время принятия решений;
- исключить человеческий фактор.

Дальнейшее развитие работы – интеграция скрипта непосредственно в программное обеспечение рефлектометров и расширение библиотеки эталонных рефлектограмм для различных типов кабелей.

Список использованных источников:

1. Авдеюк Д.Н. Информационно-измерительная система определения места повреждения магистральных линий электропередач:

дис. канд. тех. наук: 2.2.11 / Шилин Александр Николаевич – Волгоград, 2023. – 121 с.

2. Furse C., Chung Y.C., Lo C., Pendayala P. A critical comparison of reflectometry methods for location of wiring faults. Smart Structures and Systems. 2006;2(1). URL: https://www.livewireinnovation.com/wp-content/uploads/2016/03/A-Critical-Comparison-of-different-wire-fault-location-methods.-A-Critical-Comparison-of-different-wire-fault-location-methods..pdf.

Fesko N.V.
Saint Petersburg Electrotechnical
University «LETI», Saint-Petersburg

Scientific supervisor:
Shulzhenko A.D.
Saint Petersburg Electrotechnical
University «LETI», Saint-Petersburg

REFLECTOMETRY PROBLEMS AND A PROPOSAL FOR SEARCHING WAVELETS TO AUTOMATE ANALYSIS

Abstract. The article discusses the problems of reflectometry: blind zone, errors, and sensitivity to noise. It reveals the lack of an automatic mechanism for detecting connections and defects in Russian reflectometers, which leads to operator subjectivity and errors of up to 50%. The article proposes a Python-based approach for automatically overlaying reflectograms and detecting deviations, which eliminates the human factor, reduces analysis time, and improves the accuracy of detecting connections and defects.

Keywords: reflectometry, information security, detection of connections, undeclared connections

УДК 004.056

Хайсаров Р.И., Шабрин А.Ю.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Байрушин Ф.Т.
Уфимский университет науки и технологий, Уфа

МЕССЕНДЖЕРЫ И СОЦИАЛЬНЫЕ СЕТИ КАК СРЕДА РЕАЛИЗАЦИИ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ: СМИШИНГ, ПРЕТЕКСТИНГ И ИСПОЛЬЗОВАНИЕ ГОЛОСОВЫХ ДИПФЕЙКОВ

Аннотация. В статье рассматриваются современные методы социальной инженерии, реализуемые через мессенджеры и социальные сети, включая смишинг, претекстинг и использование голосовых дипфейков. Особое внимание уделено схемам мошенничества, связанным с имитацией голоса близких людей и руководителей организаций. Проанализированы причины высокой эффективности данных атак, их эволюция в условиях цифровизации, а также предложены организационные и технические меры противодействия.

Ключевые слова: социальная инженерия, смишинг, претекстинг, дипфейк, голосовой синтез, информационная безопасность, мошенничество.

На сегодняшний день мессенджеры и социальные сети стали не только средством коммуникации, но и одной из основных площадок для реализации атак социальной инженерии. Это обусловлено высокой степенью доверия пользователей к таким каналам связи, а также их повсеместной интеграцией в повседневную и профессиональную деятельность. Распространение технологий искусственного интеллекта значительно упростило создание правдоподобных сценариев обмана, что привело к появлению новых угроз, в частности – атак с использованием голосовых дипфейков.

Дополнительным фактором риска является рост объема персональных данных, публикуемых пользователями в открытом доступе. Фото, видео, аудиозаписи, информация о месте работы и круге общения формируют цифровой профиль человека, который злоумышленники могут использовать для подготовки целенаправленных атак. Таким образом, современные атаки социальной инженерии все чаще носят персонализированный характер (targeted attacks), что существенно повышает их эффективность.

Одним из наиболее распространенных методов является смишинг – разновидность фишинга, реализуемая через SMS и мессенджеры. В рамках данного подхода злоумышленники рассылают сообщения, побуждающие пользователя перейти по вредоносной ссылке, ввести учетные данные или совершить финансовую операцию. Часто такие сообщения маскируются под уведомления от банков, государственных сервисов или служб доставки. Однако в последнее время наблюдается усложнение подобных атак за счет внедрения элементов претекстинга – создания заранее продуманного сценария взаимодействия с жертвой.

Претекстинг основывается на формировании доверительного контекста, в котором злоумышленник выдает себя за другого человека. В условиях цифрового общества такими «ролями» чаще всего становятся родственники, сотрудники банков, представители государственных органов или руководители организаций. Использование эмоционального давления, срочности и авторитета позволяет значительно повысить вероятность успешной атаки. При этом злоумышленники могут вести длительное общение с жертвой, постепенно укрепляя доверие, что отличает данный метод от классического фишинга.

Особую опасность представляет схема, получившая условное название «Мама, это я, дай денег». В рамках данной атаки злоумышленники используют технологии синтеза речи для имитации голоса близкого человека. Аудиозапись создается на основе открытых источников, таких как видеоролики из социальных сетей (например, TikTok или Instagram), где пользователь ранее публиковал собственную речь. Современные нейросетевые модели позволяют воспроизводить не только тембр голоса, но и интонацию, эмоциональную окраску и индивидуальные речевые особенности.

В результате родитель получает звонок с якобы знакомым голосом, находящимся в стрессовой ситуации (например, после ДТП или задержания правоохранительными органами), и под влиянием паники переводит денежные средства. В некоторых случаях злоумышленники комбинируют голосовой дипфейк с текстовыми сообщениями, создавая более убедительный многоканальный сценарий атаки.

Эффективность данной схемы обусловлена сразу несколькими факторами. Во-первых, голос воспринимается человеком как один из наиболее надежных способов идентификации личности. Во-вторых, ситуация искусственно создается как срочная и критическая, что снижает уровень рационального мышления и активирует эмоциональные реакции. В-третьих, технологии генерации речи на сегодняшний день стали доступными и не требуют значительных технических навыков, что снижает порог входа для злоумышленников.

Не менее опасной является схема «Звонок от руководителя», направленная на сотрудников организаций. В данном случае злоумышленники либо используют взломанные аккаунты в мессенджерах, либо применяют голосовые дипфейки для имитации речи руководителя. Сотруднику (например, бухгалтеру или менеджеру) поступает срочное указание перевести денежные средства на указанный счет под предлогом важной сделки или конфиденциальной операции. Дополнительно может использоваться обещание оформить документы «задним числом» или ссылка на срочные внешние обстоятельства.

Данная атака особенно эффективна из-за психологических факторов. Сотрудники нередко боятся перепроверять распоряжения руководства, опасаясь показаться некомпетентными или нарушить субординацию. Кроме того, в условиях высокой рабочей нагрузки и ограниченного времени вероятность критического анализа информации снижается. В сочетании с реалистичной имитацией голоса это приводит к принятию необдуманных решений и значительным финансовым потерям для организации.

Анализ рассмотренных схем показывает, что ключевым элементом успешной атаки является не техническая сложность, а грамотное использование человеческого фактора. Современные технологии лишь усиливают эффект социальной инженерии, делая обман более убедительным, масштабируемым и труднораспознаваемым.

Для противодействия подобным угрозам необходимо применять комплекс мер. Во-первых, следует ограничивать публикацию аудио- и видеоконтента с собственным голосом в открытых источниках либо использовать настройки приватности. Во-вторых, в организациях должны внедряться процедуры многоуровневой проверки финансовых операций (принцип «двух ключей»), особенно при получении срочных указаний. В-третьих, необходимо развивать программы обучения сотрудников и пользователей, направленные на повышение осведомленности о методах социальной инженерии.

Дополнительно целесообразно внедрение технических средств защиты, таких как системы анализа аномалий в коммуникациях, биометрическая аутентификация и инструменты выявления дипфейков. Перспективным направлением является разработка алгоритмов, способных обнаруживать синтетическую речь по характерным артефактам генерации.

Таким образом, развитие технологий искусственного интеллекта привело к появлению новых форм мошенничества, основанных на синтезе речи и имитации личности. Голосовые дипфейки значительно повышают эффективность атак, особенно в сочетании с методами смишинга и претекстинга. В этих условиях ключевым направлением

защиты становится не только техническое обеспечение безопасности, но и формирование критического мышления у пользователей, а также развитие культуры кибербезопасности в обществе.

Список использованных источников:

1. Как избежать атаки с использованием социальной инженерии // Kaspersky Lab. URL: https://www.kaspersky.ru/resource-center/threats/how-toavoid-social-engineering-attacks.Назаров А.В.

2. Петрова А.С. Социальная инженерия: методы и способы защиты. СПб.: Экономика, 2022.

3. Тарасова Ю.А. Анализ проблемы фишинга в цифровом пространстве // Международный журнал прикладных и фундаментальных исследований.2023. № 11. С. 56–60. URL: https://applied-research.ru/ru/article/.

4. Механизм распознавания фишинговых сайтов по косвенным признакам // Молодой ученый. URL: https://moluch.ru/archive/318/72550/.

Khaisarov R.I., Shabrin A.Yu.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Bayrushin F.T.
Ufa University of Science and Technology, Ufa

MESSENGERS AND SOCIAL NETWORKS AS A PLATFORM FOR SOCIAL ENGINEERING: SMISHING, PRETEXTING AND DEEPFAKE AUDIO ATTACKS

Abstract. The article examines modern social engineering methods implemented through messengers and social networks, including smishing, pretexting, and the use of deepfake audio. Special attention is paid to fraud schemes involving voice imitation of relatives and company executives. The reasons for the high effectiveness of such attacks are analyzed and countermeasures are proposed.

Keywords: social engineering, smishing, pretexting, deepfake, voice synthesis, information security, fraud.

УДК 004

Яикбаев А.А., Бадамшин И.В.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Миронова Н.Г.
Уфимский университет науки и технологий, Уфа

ПРОБЛЕМЫ БЕЗОПАСНОСТИ ИНТЕРНЕТА ВЕЩЕЙ: ТЕХНОЛОГИИ, ПЕРСПЕКТИВЫ, РИСКИ

Аннотация. Рассмотрены вопросы безопасности IoT-устройств, проанализированы актуальные риски технологии и пути их снижения.

Ключевые слова: интернет вещей, кибербезопасность.

В последние годы активно развивается такая сфера мобильных информационных технологий, как Интернет вещей (IoT) (разнообразная «умная» бытовая и медицинская техника, гаджеты, системы транспортного контроля и беспилотные объекты, промышленное оборудование). Согласно ежегодным отчетам Zscaler ThreatLabz [1], особенно активно атакуются IoT-устройства в таких отраслях как транспортная (рост числа атак за 2025 – на 382%, последствия – нарушение логистики и операционной деятельности, компрометация систем безопасности транспортных средств, утечка конфиденциальных данных), энергетика (рост за 2025 на 387%), здравоохранение (на 224%), строительство (более чем на 410% [2]) и т.д. По оценкам аналитиков Росатома [3], к 2027 году количество подключенных устройств в России вырастет до 140 млн, т. о. ландшафт подобных угроз существенно расширится.

Стандартная архитектура IoT-системы состоит из пяти функциональных слоев [4], и для каждого киберпреступники могут использовать определенные вектора атаки:

- Устройства (датчики, приводы) зачастую обладают ограниченной вычислительной мощностью, что затрудняет применение криптозащиты.
- Транспортный уровень. Передача данных реализуется с использованием беспроводных протоколов (Zigbee, LoRaWAN, NB-IoT), уязвимости которых позволяют проводить MitM-атаки и перехват данных.
- Уровень обработки. Облачные сервисы и серверы аналитики становятся объектом атак на целостность информации и несанкционированный доступ к агрегированным данным.

- Прикладной уровень – из-за уязвимостей в коде web-приложений становятся возможны межсайтовый скриптинг, SQL-инъекции и т.п.
- Бизнес-уровень. Управление бизнес-процессами и транзакциями требует защиты от изменений в правах доступа и подделки логов действий.

Кроме того, типовыми уязвимостями IoT, эксплуатируемыми злоумышленниками, являются: слабые пароли и пароли по умолчанию (от производителя), передача информации от IoT без шифрования, отсутствие механизмов безопасного обновления прошивок (OTA) от разработчика, отсутствие проверки соответствия устройств требованиям кибербезопасности. Реализуемые через указанные выше уязвимости IoT угрозы: НСД к управлению устройством; атаки на протоколы взаимодействия между устройствами (M2M), позволяющие внедрять ложные команды в промышленные процессы, а также модификация прошивки, использование некачественных или контрафактных компонентов в цепочке поставок. Атакующие применяют мишинг, вирусы трояны и шифровальщики, эксплуатируют уязвимости неправильно настроенных устройств IoT и маршрутизаторов (75% всех кибератак на IoT были направлены на маршрутизаторы в 2025 г.), интегрируя зараженные устройства в свои ботнеты (типа Mirai) для последующих DDoS-атак на другие объекты [5].

Безопасность устройств интернета вещей включает в себя не только защиту личной информации, но и обеспечение физической безопасности пользователей, а также устойчивость критически важных инфраструктур, поскольку мобильные и IoT-устройства используют часто как основную точку входа в сеть (корпоративную, домашнюю) для развития атаки. Для безопасности экосистем интернета вещей требуется комплексный подход. Актуальные технические меры защиты IoT-устройств: использовать более надежные пароли или средства многофакторной аутентификации, регулярное обновление ПО (если позволяет IoT-устройство); для обеспечения более защищенной связи с IoT применять какие-либо легкие криптографические алгоритмы (совместимые с их микроконтроллерами). При использовании в корпоративной инфраструктуре IoT-устройств выделять их в отдельный сегмент/микросегмент сети (придерживаясь принципов Zero Trust), применять в этом сегменте для защиты системы обнаружения аномалий на основе машинного обучения для оперативного выявления признаков атак. Среди организационных мер можно рекомендовать периодические проверки безопасности (с тестированием на проникновение); обучение сотрудников безопасным регламентам работы с IoT и гаджетами в корпоративной инфраструктуре…

Развитие кибербезопасности интернета вещей обусловлено внедрением искусственного интеллекта для опережающего обнаружения

угроз [6], адаптацией защитных решений под условия 5G и edge-вычислений, а также переходом на постквантовую криптографию. Обеспечение масштабируемости IoT-сред требует применения подхода «безопасность на стадии проектирования», обеспечивающего синтез функциональности, экономической эффективности и защищенности, что возможно только при слаженной работе производителей, регуляторов и конечных пользователей. Важнейшее значение имеет правовое регулирование отрасли разработки IoT-устройств; актуальные такие направления безопасности, как:

- приведение национальных стандартов в соответствие с международными практиками (например, ETSI EN 303 645, ISO/IEC 27001);
- поощрение производителей в части реализации принципа «безопасности по умолчанию» (security by design) за счет условий госзакупок и требований к сертификации;
- определение четкой ответственности поставщиков за уязвимости в устройствах на всех этапах их эксплуатации.

Список использованных источников:

1. Industry Report «Zscaler ThreatLabz 2025 Mobile, IoT, & OT Threat Report» - URL: https://www.zscaler.com/campaign/threatlabz-mobile-iot-ot-report (доступ по запросу).
2. Рост кибератак на интернет вещей охватывает новые отрасли / infowatch.ru – URL: https://www.infowatch.ru/analytics/daydzhesty-i-obzory/rost-kiberatak-na-internet-veschey-okhvatyvayet-novyye-otrasli (Дата публикации: 24 ноября 2025).
3. Исследование «Росатома»: в России всплеск спроса на технологии интернета вещей // Росатом URL: https://www.rusatom-utilities.ru/media-center/news/issledovanie-rosatoma-v-rossii-vsplesk-sprosa-na-tekhnologii-interneta-veshchey/ (дата публикации: 21.11.2024).
4. 5 уровней архитектуры IoT, которые наделяют его сверхвозможностями // Вестник ГЛОНАСС URL: http://vestnik-glonass.ru/news/intro/5-urovney-arkhitektury-iot-kotorye-nadelyayut-ego-sverkhvozmozhnostyami/ (Дата публикации: 10 Января 2023).
5. Ситон У., Ганди В., Шарма Х., Барахас Й. Рост числа атак на отраслевые платформы, распространение мобильного вредоносного ПО: отчет ThretalLabz 2025 по мобильным устройствам, IoT и операционным технологиям / zscaler.com: сайт – URL: https://www.zscaler.com/blogs/security-research/industry-attacks-surge-mobile-malware-spreads-threatlabz-2025-mobile-iot-ot.
6. Кобозева Е. М., Берсенева Д. В. Будущее интернета вещей: угрозы, проблемы и перспективы // Вестник Астраханского

государственного технического университета. Серия: Экономика. 2025. - № 2. - URL: https://cyberleninka.ru/article/n/buduschee-interneta-vesche y-ugrozy-problemy-i-perspektivy/viewer (дата обращения: 30.03.2026).

Yaikbaev A.A., Badamshin I.V.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Mironova N.G.
Ufa University of Science and Technology, Ufa

INTERNET OF THINGS SECURITY ISSUES: TECHNOLOGIES, PROSPECTS, AND RISKS

Abstract. The security issues of IoT devices are considered, current risks of the technology and ways to mitigate them are analyzed

Keywords: Internet of Things, cybersecurity.

При подготовке электронного издания использовались следующие программные средства:

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

Все права защищены. Книга или любая ее часть не может быть скопирована, воспроизведена в электронной или механической форме, в виде фотокопии, записи в память ЭВМ, репродукции или каким-либо иным способом, а также использована в любой информационной системе без получения разрешения от издателя. Копирование, воспроизведение и иное использование книги или ее части без согласия издателя является незаконным и влечет уголовную, административную и гражданскую ответственность.

Научное издание

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ ОБЕСПЕЧЕНИЯ КОМПЛЕКСНОЙ БЕЗОПАСНОСТИ В ЦИФРОВОМ ОБЩЕСТВЕ

Материалы
IX Всероссийской молодежной научно-практической конференции с международным участием
(г. Уфа, 22–23 мая 2026 г.)

Научное электронное издание сетевого доступа

За достоверность информации, изложенной в статьях, ответственность несут авторы.
Статьи публикуются в авторской редакции

Подписано к использованию 02.10.2026 г.
Гарнитура «Times New Roman». Объем 6,17 Мб.
Заказ 222.

ФГБОУ ВО «Уфимский университет науки и технологий»
450008, Башкортостан, г. Уфа, ул. Карла Маркса, 12.

Тел.: +7-908-35-05-007
e-mail: red@uust.ru