

Актуальные проблемы кибербезопасности Противодействие экстремизму и терроризму в информационной молодежной среде

**Сборник докладов I межрегиональной
научно-практической конференции**



**Брянск
БГТУ
2025**

Министерство науки и высшего образования Российской Федерации
Брянский государственный технический университет

**«АКТУАЛЬНЫЕ ПРОБЛЕМЫ КИБЕРБЕЗОПАСНОСТИ.
ПРОТИВОДЕЙСТВИЕ ЭКСТРЕМИЗМУ И ТЕРРОРИЗМУ
В ИНФОРМАЦИОННОЙ МОЛОДЕЖНОЙ СРЕДЕ»**

I межрегиональная научно-практическая конференция
(Брянск, 29 апреля 2025 г.)

Сборник докладов

Под общей редакцией М. Ю. Рытова, О. М. Голембиовской

Текстовое электронное издание



Брянск
БГТУ
2025

© Брянский государственный
технический университет, 2025
ISBN 978-5-907570-98-6

УДК 004.056

ББК 32.97

А 74

Утверждено редакционно-издательским советом БГТУ

А74 Актуальные проблемы кибербезопасности. Противодействие экстремизму и терроризму в информационной молодежной среде : сборник докладов I межрегиональной научно-практической конференции [Электронный ресурс] / под общей редакцией М. Ю. Рытова, О. М. Голембиовской. – Брянск : БГТУ, 2025. – 409 с. – Режим доступа: <https://www.tu-bryansk.ru/mainpage/nauka/konferentsii/sborniki-trudov-konferentsiy-provodimyykh-bgtu>. – Загл. с экрана.

Сборник подготовлен по материалам I межрегиональной научно-практической конференции «Актуальные проблемы кибербезопасности. Противодействие экстремизму и терроризму в информационной молодежной среде», прошедшей 29 апреля 2025 года в ФГБОУ ВО «Брянский государственный технический университет».

Для студентов и аспирантов, занимающихся научно-исследовательской работой.

Текстовое электронное издание

Минимальные системные требования

- Браузеры: Google Chrome, Microsoft Edge, Mozilla Firefox, Opera
- Скорость подключения к информационно-телекоммуникационным сетям 1 Мбит/с
- Дополнительные настройки для чтения PDF в браузере: Google Chrome (требуется), Microsoft Edge (требуется), Mozilla Firefox (требуется), Opera (требуется)

Материалы публикуются с сохранением авторской орфографии и пунктуации

УДК 004.056

ББК 32.97

ISBN 978-5-907570-98-6

© Брянский государственный
технический университет, 2025

Научное издание

**«АКТУАЛЬНЫЕ ПРОБЛЕМЫ КИБЕРБЕЗОПАСНОСТИ.
ПРОТИВОДЕЙСТВИЕ ЭКСТРЕМИЗМУ И ТЕРРОРИЗМУ
В ИНФОРМАЦИОННОЙ МОЛОДЕЖНОЙ СРЕДЕ»**

I межрегиональная научно-практическая конференция
(Брянск, 29 апреля 2025 г.)

Сборник докладов

Под общей редакцией М. Ю. Рытова, О. М. Голембиовской

Текстовое электронное издание

Сборник разработан с помощью программного
обеспечения Microsoft Office Word, Adobe Acrobat Pro

Подписано к использованию
Объем издания – 7,39 Мб.
Гарнитура Times

Организационный комитет

- Сканцев В. М. – первый проректор, председатель оргкомитета;
- Шкаберин В. А. – проректор по учебной работе и цифровизации, заместитель председателя оргкомитета;
- Рытов М. Ю. – заведующий кафедрой «Системы информационной безопасности», заместитель председателя оргкомитета;
- Еременко В. Т. – профессор кафедры «Информационная безопасность» Орловского государственного университета им. И. С. Тургенева (по согласованию);
- Громов Ю. Ю. – директор института автоматизации и информационных технологий Тамбовского государственного технического университета;
- Афанасьев А. Ю. – начальник кафедры криминалистики Нижегородской академии МВД России, майор полиции;
- Голембиовская О. М. – доцент кафедры «Системы информационной безопасности»;
- Горлов А. П. – доцент кафедры «Системы информационной безопасности»;
- Шпичак С. А. – доцент кафедры «Системы информационной безопасности»;
- Шинаков К. Е. – доцент кафедры «Системы информационной безопасности»;
- Лексиков Е. В. – старший преподаватель кафедры «Системы информационной безопасности»;
- Лысов Д.А. - старший преподаватель кафедры «Системы информационной безопасности»;
- Захарова Л. И. – доцент кафедры «Гуманитарные и социальные дисциплины», ответственный секретарь конференции.

СОДЕРЖАНИЕ

СЕКЦИЯ 1. АКТУАЛЬНЫЕ ПРОБЛЕМЫ КИБЕРБЕЗОПАСНОСТИ И РЕШЕНИЯ.....	ИХ 9
Алексеев В.В., Анисимов А.Д., Брюханов А.А. Задача прогнозирования развития атак на сетевую структуру организации и ее решение	9
Алексеев В.В., Вислобоков Д.А., Шишкин И.С., Маленков Е.С. Применение технологии киберобмана для защиты баз данных	16
Анисимов А.Д., Брюханов А.А., Воскобойников О.А. Усовершенствованная система депонирования ключей шифрования в условиях проведения специальной военной операции с применением средств радиоэлектронной борьбы	22
Анищенков К.А., Березкин Ф.Е., Евдокимов А.В. Киберугрозы и оборона: как современные конфликты меняют подходы к информационной безопасности в армии	30
Березкин Ф.Е., Бобков К.В., Шапенская А.М., Голембиовский М.М. Оптимизация маршрутов снабжения с учётом киберрисков и геополитических угроз.....	35
Березкин Ф.Е., Бобков К.В., Шапенская А.М., Банников А.И. Telegram-каналы в распространении деструктивных идеологий: методы блокировки и альтернативы.....	39
Березкин Ф.Е., Шапенская А.М., Евдокимов А.В., Шинаков К.Е. Эволюция атак программ-вымогателей (Ransomware): от превентивных мер к стратегиям киберустойчивости и восстановления	43
Бузылев А.А., Киселёв В.П., Лысов Д.А., Горлов А.П. Исследование применения модели Cyber-Kill Chain	48
Бузылев А.А., Киселёв В.П., Лысов Д.А., Горлов А.П. Управление рисками безопасности при реализации аутентификации и авторизации в Application Programming Interface	52
Воробьёв Д.Д., Шапенская А.М. Обнаружение OSINT: современные методы выявления и защиты от разведки по открытым источникам.....	57
Грива М.Д., Коновалов С.И., Аверин П.А. Обнаружение атак на офисную Wi-Fi-инфраструктуру: анализ угроз и защитных решений	60
Гулак М.Л. О применении стеганографии в различных сферах.....	64
Евдокимов А.В., Березкин Ф.Е., Анищенков К.А. Проактивный поиск сложных киберугроз (threat hunting)	69
Киселев В.П., Бузылев А.А., Лысов Д.А., Горлов А.П. Анализ нормативных основ, регламентирующих безопасность интернета вещей в России и мире.....	72
Козлова О.С. Оценка уязвимости объектов: подход к определению вероятного внутреннего нарушителя.....	76
Коновалов С.И., Аверин П.А., Логинов К.В. Обзор средств защиты и мониторинга информационных систем	81
Коновалов С.И., Аверин П.А., Лактюшин Д.А. Оценка соответствия требованиям приказа ФСТЭК России № 31	85
Коновалов С.И., Аверин П.А., Лысов Д.А. Основные методы взлома паролей и способы противодействия им	89
Коновалов С.И., Аверин П.А., Лысов Д.А. Применение утилиты Hashcat в аудите безопасности паролей.....	92
Коновалов С.И., Аверин П.А., Седаков К.А. Технология Secure Enclave как основа аппаратной безопасности в iOS-устройствах: архитектура и принципы защиты данных.....	95
Куцева Е.С., Евдокимов А.В. Оценка соответствия требованиям приказа ФСТЭК России № 237	98
Лукутина М.С., Денисеня Д.И., Лысов Д.А. Исследование методов защиты пользователей от агрессивного поведения в игровых сообществах и чатах	102

Лысов Д.А., Березкин Ф.Е. Сравнительный анализ эффективности технических средств защиты от различных векторов атак социальной инженерии.....	105
Лысов Д.А., Березкин Ф.Е. Человеческий фактор как ключевая уязвимость: анализ эффективности комплексных мер защиты от социальной инженерии в корпоративной среде	111
Мамичев Р.А., Коновалов С.И., Аверин П.А. Идентификация и эксплуатация уязвимостей в информационных системах	117
Морозова К.В., Горелов П.Д., Денисеня Д.И., Лысов Д.А. Анализ актуальности разработки платформ для работы с нормативно-правовыми актами как инструмента для комплексного подхода к соблюдению отраслевых требований в вопросах защиты информации.....	121
Морозова К.В., Шапенская А.М. Анализ процессов и компонентов внутри SOC: ключевые аспекты работы	125
Мурьян В.С., Евдокимов А.В. Методика противодействия повышению привилегий... через известные уязвимости Windows.....	129
Пантюхина М.С., Голембиовская О.М. Разграничение доступа пользователей в системе Linux.....	132
Плиско Н.О., Березкин Ф.Е., Шапенская А.М. Анализ горизонтального перемещения в информационной безопасности.....	136
Родин А.А., Шапенская А.М. Применение утечек хэша NTLM Windows при реализации..... фишинговых атак.....	140
Руденко Н.А., Березкин Ф.Е. Управление киберрисками в экосистеме цифровых цепочек поставок: уязвимости, последствия и стратегии повышения защищенности	145
Руденко Н.А., Евдокимов А.В. Анализ методик идентификации и эксплуатации уязвимостей	151
Рытов М.Ю., Шкаберин В.А. Актуальность высококачественной обработки информации . в регионах Российской Федерации	154
Таран Д.Г., Мартынов А.С., Шабардин А.С. Методы обеспечения безопасности информации при передаче данных	158
Устюшенков Д.В., Шапенская А.М. Исследование средств взлома паролей Hashcat и Patator	165
Шабардин А.С., Мартынов А.С., Таран Д.Г. Исследование возможности модуляции хаотического колебания информационным сигналом для повышения информационной безопасности	169
Шауло А.А., Родин А.А. Исследование видов атак на Wi-Fi, осуществляемых при помощи MitM и DoS/DDoS, и способы противодействия им	176
Шишкин И.С., Вислобоков Д.А., Маленков Е.С. Анализ уязвимостей Docker-образов с использованием инструмента Trivy	179
СЕКЦИЯ 2. КОМПЬЮТЕРНАЯ КРИМИНАЛИСТИКА.....	184
Голембиовский М.М., Васина Т.В. Внедрение предмета «Компьютерная криминалистика» в образовательную программу студентов направления «Информационная безопасность»..	184
СЕКЦИЯ 3. ИНЦИДЕНТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.....	187
Морозова К.В., Горелов П.Д., Денисеня Д.И., Лысов Д.А. Исследование важности роли метаданных в инцидентах информационной безопасности	187
Родин А.А., Березкин Ф.Е. Атака хакерами IronHusky государственных информационных систем..... России и Монголии	193
Родин А.А., Березкин Ф.Е. Атака хакерами SideWinder информационных систем стран Африки и Южной Азии.....	197
Родин А.А., Шапенская А.М. Использование Microsoft Trusted Signing злоумышленниками	202

Сычев Д.А. Анализ крупных утечек данных 2023–2024 годов: причины, последствия и уроки для организаций.....	205
Сычев Д.А. Роль человеческого фактора в инцидентах информационной безопасности ..	209
Терехова Д.А., Козлова О.С. Анализ актуальных угроз информационной безопасности ..	212
Урецкий А.М., Голембиовская О.М. OSINT как инструмент предотвращения мошенничества	215
Фурсова А.В., Яковлев А.В. Анализ актуальных угроз ситуационного центра регионального уровня	220
СЕКЦИЯ 4. АУДИТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, УПРАВЛЕНИЕ РИСКАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.....	225
Банний П.В., Петроченко Н.В., Седаков К.А. Основные особенности оценки уровня остаточного риска информационной безопасности	225
Иваничкин В.В., Шинаков К.Е., Волков В.И. Алгоритм определения актуальных угроз согласно методическим рекомендациям ФСТЭК России	231
Козлова О.С., Горбачев Е.П., Кондрашова Е.В. Особенности построения политики защищенной обработки персональных данных.....	236
Козлова О.С., Сафоненко С.В., Голембиовская О.М. Особенности построения модели угроз по методическим рекомендациям ФСБ России.....	240
Матюхина Г.Д., Седаков К.А. Анализ основных видов уязвимостей информационной безопасности учреждений сферы здравоохранения.....	247
Седаков К.А., Рытов М.Ю. Основные показатели защищенности при проведении оценки..... эффективности системы защиты персональных данных в медицинских учреждениях	251
Янченко Е.Н. Сканирование сетей в информационной безопасности	255
СЕКЦИЯ 5. ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ.....	259
Белоусов А.Г. Шифрование изображений: особенности и рекомендации	259
Грива М.Д., Рытов М.Ю. Особенности IP-камер и перспективы их развития.....	266
Грива М.Д., Рытов М.Ю. Принцип слежения, используемый IP-камерами	269
Грива М.Д., Шапенская А.М. Перспективы развития систем видеонаблюдения.....	273
Колесников М.В. Разработка систем защиты персональных данных	277
Матюхина Г.Д., Воронин В.А. Сравнительный анализ технологий двухфакторной аутентификации для физических лиц.....	283
Матюхина Г.Д., Ковалев М.В. Преимущества и риски использования биометрии для защиты данных физических лиц	287
СЕКЦИЯ 6. ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ КАК ИНСТРУМЕНТ ПОМОЩИ СПЕЦИАЛИСТУ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	291
Аверин П.А., Коновалов С.И., Лысов Д.А. OSINT: виды разведки, инструменты и правовые ограничения в практике анализа открытых данных.....	291
Аверин П.А., Коновалов С.И., Лысов Д.А. Разведка по открытым источникам (OSINT): сущность, цели и место в современной информационной экосистеме.....	295
Аверин П.А., Коновалов С.И., Седаков К.А. Оценка результативности современных методов обеспечения информационной безопасности с применением межсетевых экранов	298
Брюханов А.А., Куликов Д.А., Чернов В.Н., Шишов В.Р. Искусственный интеллект в биометрии: новые решения для обеспечения безопасности доступа.....	303
Грива М.Д., Шапенская А.М. Использование искусственного интеллекта в системах видеонаблюдения.....	308
Медведева И.Ю., Седаков К.А. Искусственный интеллект как помощник в информационной безопасности в медицинских учреждениях	311
СЕКЦИЯ 7. ПРОТИВОДЕЙСТВИЕ ЭКСТРЕМИЗМУ И ТЕРРОРИЗМУ В ИНФОРМАЦИОННОЙ МОЛОДЕЖНОЙ СРЕДЕ	316
Аверин П.А., Бутузова Д.Д., Коновалов С.И., Шапенская А.М. Поиск и эксплуатация уязвимостей с использованием Metasploit Framework.....	316

Аверин П.А., Диво А.А., Коновалов С.И., Шапенская А.М. Анализ процесса постэксплуатации в Linux.....	321
Аверин П.А., Коновалов С.И., Шапенская А.М. Анализ атак на беспроводные сети Wi-Fi с применением техник MitM и DoS/DDoS.....	325
Аверин П.А., Коновалов С.И., Шапенская А.М. Применение программного обеспечения Wireshark для анализа сетевого трафика.....	330
Аверин П.А., Коновалов С.И., Шапенская А.М. Современные методы компрометации паролей и средства их нейтрализации.....	334
Аверин П.А., Староверов Д.В., Коновалов С.И., Шапенская А.М. Постэксплуатация в Windows.....	338
Аверин П.А., Терехова Д.А., Коновалов С.И., Шапенская А.М. Оценка соответствия требованиям приказа ФСТЭК России № 21.....	342
Анищенко Е.В. Кибербезопасность и молодежь: противодействие цифровому экстремизму и террористическому влиянию в Интернете.....	346
Денисеня Д.И., Лысов Д.А., Горелов П.Д., Морозова К.В. Автоматизированный анализ текстов в социальных сетях для выявления признаков вербовки в экстремистские организации.....	349
Киселев В.П., Бузылев А.А., Лысов Д.А., Горлов А.П. Социально-культурные аспекты противодействия экстремизму и терроризму в молодежной среде.....	352
Сычев Д.А. Влияние экстремистских ценностей на подростков через социальные сети: анализ и последствия.....	355
СЕКЦИЯ 8. БЕСПИЛОТНЫЕ ЛЕТАТЕЛЬНЫЕ АППАРАТЫ*	359
Аненков О.А. Роль искусственного интеллекта в оснащении беспилотных..... летательных аппаратов.....	359
Анищенков К.А., Березкин Ф.Е. БПЛА в виртуальной реальности: ITGS-исследование симуляторов полета.....	364
Анищенков К.А., Березкин Ф.Е. БПЛА в математическом моделировании: оптимизация маршрутов как задача для IA по Math AA AI.....	367
Анищенков К.А., Березкин Ф.Е. Микро- и наноБПЛА как невидимая угроза будущих войн.....	370
Анищенков К.А., Березкин Ф.Е. Обзор перспектив развития БПЛА-такси.....	376
Капустин В.В., Кирюпина В.В. Анализ технических требований современных БПЛА и их роль в современных операциях.....	379
Марченко А.Р., Медведев И.И. Использование систем радиоэлектронного подавления для противодействия беспилотным летательным аппаратам.....	384
Родин А.А., Березкин Ф.Е., Шапенская А.М. Использование БПЛА в кибератаках: уязвимости инфраструктуры и риски.....	387
Родин А.А., Березкин Ф.Е., Шапенская А.М. Роевые технологии в военном применении БПЛА: тактика, разработки и вызовы.....	391
Романенко И.Г., Медведев И.И. Современные системы борьбы с БПЛА.....	395
Руденко Н.А., Березкин Ф.Е. Защита беспилотных систем от кибератак.....	398
Шведчиков И.А. Методы выявления и классификации беспилотных летательных аппаратов с использованием искусственного интеллекта.....	403
Шведчиков И.А. Рой БПЛА: координация и управление группой дронов.....	406

СЕКЦИЯ 1. АКТУАЛЬНЫЕ ПРОБЛЕМЫ КИБЕРБЕЗОПАСНОСТИ И ИХ РЕШЕНИЯ

Научная статья

УДК 004.056

Задача прогнозирования развития атак на сетевую структуру организации и ее решение

Владимир Витальевич Алексеев¹, Артем Дмитриевич Анисимов²✉,
Александр Александрович Брюханов³

¹ Тамбовский государственный технический университет, Тамбов, Россия

^{2,3} Межвидовой центр подготовки и боевого применения (учебный и испытательный), Тамбов, Россия

¹vvaalex1961@mail.ru

^{2,3}nauchnajarota@yandex.ru ✉

Аннотация. Целью работы является решение задачи прогнозирования развития кибератак на сетевую инфраструктуру при помощи автоматизации построения сценариев. В работе существующие методы решения задачи прогнозирования атак, а также предложено новое программное решение, использующее базу знаний MITRE ATT&CK и SIEM-систему Wazuh. Результатом работы разработанной системы является сценарий реагирования, что позволяет своевременно предотвратить развитие атаки и минимизировать возможный ущерб для информационной безопасности.

Ключевые слова: информационная безопасность, прогнозирование, сетевая безопасность.

Для цитирования: Алексеев В.В., Анисимов А.Д., Брюханов А.А. Задача прогнозирования развития атак на сетевую структуру организации и ее решение // Актуальные проблемы кибербезопасности. Противодействие экстремизму и терроризму в информационной молодежной среде: сборник докладов I межрегиональной научно-практической конференции. – Брянск: БГТУ, 2025. – С. 9 – 15.

Кибератаки в наше время приобретают всё более сложный, многослойный и изменчивый характер. Злоумышленники активно применяют современные технологии, такие как искусственный интеллект, машинное обучение и автоматизированные средства взлома, что значительно снижает эффективность традиционных методов защиты. В связи с этим одной из важнейших задач в области кибербезопасности становится возможность предугадывания направления развития атак и их предотвращения до того, как будет нанесён ущерб.

Эта задача особенно важна как для бизнеса, так и для государственных структур, поскольку отсутствие эффективного прогнозирования может привести к серьёзным последствиям – от утечек конфиденциальной информации и финансовых потерь до нарушений работы критически важных инфраструктур.

1. Задача прогнозирования развития кибератак

Прогнозирование развития кибератак – это процесс предугадывания возможных угроз на основе исторических данных, анализа поведения пользователей и потенциальных уязвимостей в информационных системах. Однако этот процесс сталкивается с рядом сложностей:

- быстрое развитие киберугроз: злоумышленники постоянно совершенствуют свои методы, используя новые технологии и тактики. Каждый год появляются новые виды атак, что делает их предсказание затруднительным;
- большие объемы данных: современные системы генерируют огромные объемы информации, в которых сложно обнаружить потенциальные угрозы без применения продвинутой аналитики;
- человеческий фактор: ошибки пользователей и сотрудников компаний часто являются причиной успешных атак, например, фишинговые атаки, в которых злоумышленники получают доступ к системам через социальную инженерию;
- недостаток координации и обмена информацией: многие компании не делятся сведениями о кибератаках, что затрудняет создание глобальных баз данных угроз и их анализ.

2. Методы решения задачи прогнозирования атак

Чтобы минимизировать риски кибератак, необходимо применять комплексный подход, включающий технологии искусственного интеллекта, автоматизацию и активный обмен информацией между организациями:

- использование искусственного интеллекта и машинного обучения: современные системы кибербезопасности могут анализировать огромные массивы данных и выявлять подозрительное поведение на ранних стадиях атаки. Например, SIEM-системы (Security Information and Event Management) помогают автоматически выявлять аномалии в трафике и потенциальные угрозы;
- моделирование атак: организации должны регулярно тестировать свои системы безопасности, имитируя атаки (Red Teaming) и анализируя возможные уязвимости. Использование баз данных угроз (например, MITRE ATT&CK) позволяет системам безопасности предугадывать новые типы атак;
- обучение сотрудников и пользователей: около 90% атак происходят из-за ошибок людей, поэтому обучение персонала основам кибергигиены (например, выявлению фишинговых писем) является критически важным;
- обмен информацией о кибератаках: для эффективного прогнозирования атак необходимо сотрудничество между государственными органами, частными компаниями и международными организациями. Создание глобальных платформ обмена информацией о киберугрозах поможет быстрее реагировать на новые атаки.

3. Система прогнозирования развития атак на корпоративную инфраструктуру с генерацией сценария

В основе системы, предназначенной для прогнозирования развития атак на корпоративную ИТ-инфраструктуру и генерации сценариев реагирования, лежит база знаний MITRE ATT&CK. Эта база описывает поведение злоумышленников через 14 тактик, каждая из которых включает набор конкретных техник. Тактики

отражают последовательные этапы атаки на информационные системы и представлены в промышленной матрице Enterprise MITRE ATT&CK в логической последовательности **[Ошибка! Источник ссылки не найден.]**.

Формирование прогноза развития атаки и построение сценария реагирования осуществляется на основе сведений о конфигурации корпоративной инфраструктуры и особенностях используемых техник. Именно техники содержат данные о возможных действиях противника, способах их выявления, а также о мерах реагирования. Зная, какая техника применяется в данный момент, можно определить текущую фазу атаки и спрогнозировать, какие методы и действия злоумышленник может использовать далее, опираясь на логику перехода между тактиками в MITRE ATT&CK.

Разрабатываемая система включает в себя SIEM-платформу (систему управления событиями информационной безопасности), которая фиксирует и анализирует события, потенциально свидетельствующие о применении определённых техник. Также она содержит базу данных, в которой хранятся сведения о компонентах корпоративной инфраструктуры организации и информация о техниках из матрицы MITRE ATT&CK **[Ошибка! Источник ссылки не найден.]**.

Для обнаружения событий информационной безопасности, указывающих на потенциальные действия злоумышленников, была выбрана платформа SIEM Wazuh. Wazuh представляет собой централизованную систему мониторинга и анализа событий в реальном времени, предназначенную для выявления угроз и контроля соответствия требованиям безопасности. Эта платформа способна собирать информацию из различных источников, включая конечные устройства, сетевое оборудование и программное обеспечение **[Ошибка! Источник ссылки не найден.]**.

Важным компонентом является модуль Wazuh MITRE ATT&CK, обеспечивающий интеграцию с одноимённой базой знаний. С его помощью события, зафиксированные системой Wazuh, могут быть сопоставлены с конкретными техниками и тактиками MITRE ATT&CK, что позволяет точнее интерпретировать действия злоумышленника.

Для реализации механизма сценарного реагирования и учета архитектуры корпоративной ИТ-среды используется база данных, содержащая сведения как о корпоративной инфраструктуре, так и о техниках из MITRE ATT&CK. Эти данные представлены в формате JSON. Файл, описывающий инфраструктуру, содержит список рабочих станций организации с указанием установленных на них операционных платформ и сервисов. Описание техник соответствует структуре карточек, представленных в официальной базе MITRE ATT&CK

Elasticsearch – это распределённая поисково-аналитическая система RESTful, которая централизованно хранит данные для поиска, индексирования и анализа данных всех форм и размеров.

Elasticsearch представляет собой NoSQL базу данных, специализирующуюся на документах, и использует полнотекстовую поисковую систему в своей архитектуре. Основанная на библиотеке Apache Lucene, она хранит данные в формате JSON, предоставляет RESTful API и обеспечивает эффективный меха-

низм аналитики для быстрого извлечения информации. Elasticsearch доступен в двух версиях: бесплатной (открытый исходный код) и коммерческой [**Ошибка! Источник ссылки не найден.**].

Результатом работы системы является сформированный сценарий реагирования, включающий необходимые сведения из описаний техник в базе данных. Этот сценарий предоставляет рекомендации и информацию, которые позволяют своевременно предотвратить развитие атаки и минимизировать возможный ущерб для информационной безопасности.

Общая схема разрабатываемой системы представлена на рис. 1.

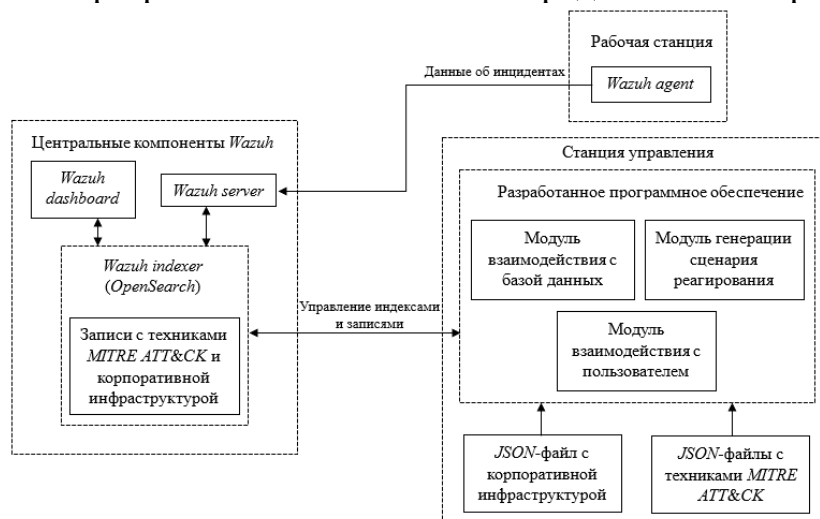


Рис. 1. Общая схема работы системы прогнозирования развития атак на корпоративную инфраструктуру с генерацией сценария

Разработанное программное решение ADPS (Attack Development Prediction System) доступно в двух форматах: с графическим пользовательским интерфейсом (GUI) и в консольном исполнении. Вариант с графическим интерфейсом ориентирован на пользователей, не обладающих глубокими техническими навыками. Он обеспечивает наглядное представление данных, упрощает анализ информации и делает процесс взаимодействия с системой более доступным.

Консольная версия, в свою очередь, отличается высокой скоростью запуска и низким потреблением ресурсов за счёт отсутствия визуальной оболочки. Этот формат удобен для интеграции с другими программными средствами и автоматизированными сценариями, а также обеспечивает расширенные возможности конфигурации, что делает его предпочтительным выбором для системных администраторов и продвинутых пользователей. Кроме того, консольный вариант возможно легко развернуть в различных операционных средах, обеспечивая максимальную гибкость в эксплуатации.

Графический интерфейс ADPS включает следующие функциональные элементы (рис. 2):

- добавление корпоративной инфраструктуры – предназначено для ввода и визуализации данных о корпоративной ИТ-среде организации;
- добавление техник – используется для внесения информации о техниках MITRE ATT&CK и их отображения;

- журнал событий Wazuh – отображает зафиксированные системой события информационной безопасности с привязкой к соответствующим техникам MITRE ATT&CK. Это позволяет анализировать происхождение событий и их возможное влияние на защищаемую инфраструктуру;
- сценарии – модуль генерации сценариев реагирования, основанных на идентификаторе техники и номере станции, на которой обнаружено подозрительное событие;
- вывод – обеспечивает получение информации из базы данных OpenSearch, включая результаты анализа и рекомендации по реагированию.



Рис. 2. Графический интерфейс ADPS

Для добавления информации о корпоративной инфраструктуре пользователь должен выбрать соответствующий текстовый файл формата .txt с помощью кнопки «Указать файл». Содержимое этого файла должно строго соответствовать структуре JSON-документа, описанной ранее, что необходимо для корректной интерпретации и обработки данных системой.

При успешной загрузке и соответствии структуры файла требованиям, система отобразит уведомление о создании или обновлении записи. Это сообщение служит подтверждением того, что данные были успешно внесены в базу и готовы к дальнейшему использованию в рамках функционирования программного обеспечения.

```
Вывод
=====INFRASTRUCTURE=====
{
  "_index": "corporate_infrastructure",
  "_id": "1",
  "_version": 6,
  "_seq_no": 5,
  "_primary_term": 1,
  "found": true,
  "source": {
    "properties": [
      {
        "station number": "1",
        "name": "w",
        "ip": "w",
        "platform": "Windows",
        "service": [
          "VPN",
          "Telnet",
          "Containers"
        ]
      }
    ]
  }
}
```

Рис. 3. Вывод записи с информацией о корпоративной инфраструктуре

В поле «Сценарии» при вводе идентификатора техники MITRE ATT&CK и указания номера рабочей станции, информацию о которой мы берем из записи с корпоративной инфраструктурой, выводятся записи техник, которые может реализовать злоумышленник, с указанием вероятных станций (рис. 4).

Добавление корпоративной инфраструктуры

Указать файл

Отобразить инфраструктуру

Добавление техники

Идентификатор техники

Указать файл

Отобразить технику

Журнал событий Wazuh

Дата журнала

Отобразить журнал

Отобразить с полем MITRE

Сценарии

Идентификатор техники 1078

Номер станции 1

Сгенерировать сценарий

Вывод

```
{
  "name tactics": [
    "Предотвращение обнаружения"
  ],
  "platforms": [
    "Linux",
    "Windows",
    "macOS"
  ],
  "service": [
    "IaaS",
    "Containers"
  ],
  "description": "Злоумышленники могут модифицировать и/или отключать инструменты безопасности, что",
  "mitigations": [
    {
      "idm": "M1038",
      "mitigation": "Предотвращение выполнения",
      "description": "Используйте контроль приложений, где это необходимо, особенно в отношении выполне"
    }
  ],
  "detection": [
    {
      "id": "DS0029",
      "data source": "Команда",
      "data component": "Выполнение команд",
      "detects": "Отслеживайте выполнение команд и аргументов, связанных с отключением или модифика"
    }
  ]
}
```

Вероятные станции для развития атаки: 2 3
PDF документ успешно создан и сохранен по пути: C:\Users\anidm\source\repos\VKR\VKR\bin\Debug\1 1078.pdf

Рис. 4. Вывод записи техник, которые может реализовать злоумышленник

Итогом операции является файла в формате PDF с сценарием реагирования.

Кибератаки становятся всё сложнее, а традиционные методы защиты не всегда способны вовремя выявить новые угрозы. Прогнозирование атак — одна из ключевых задач в сфере кибербезопасности, и её решение требует комплексного подхода. Использование искусственного интеллекта, автоматизация процессов, моделирование атак и активное сотрудничество между организациями помогут создать более защищенные цифровые системы.

Компании, которые внедряют проактивные меры киберзащиты, получают конкурентное преимущество, снижая риски утечек данных, финансовых потерь

и репутационного ущерба. В условиях стремительного развития технологий только инновационные методы защиты позволят эффективно противостоять угрозам.

Разработанная система учитывает корпоративную инфраструктуру в виде платформ (Windows, macOS, Linux) и работающих на них сервисов. Данные о корпоративной инфраструктуре и техниках злоумышленников хранятся в JSON-файлах. Сценарий реагирования на инциденты содержит структурированную информацию в формате PDF.

Список источников

1. MITRE ATT&CK. URL: <https://at-tack.mitre.org/> (дата обращения: 10.04.2025).
2. Что такое SIEM? | Microsoft Security. URL: <https://www.microsoft.com/ru-ru/security/business/security-101/what-is-siem> (дата обращения: 10.04.2025).
3. SIEM | Wazuh. URL: <https://wazuh.com/platform/siem/> (дата обращения: 10.04.2025).
4. Elasticsearch features list | Elastic. URL: <https://www.elastic.co/elasticsearch/features> (дата обращения: 10.04.2025).

Статья поступила в редакцию 19.04.2025; принята к публикации 10.05.2025

Информация об авторах

Алексеев В.В. - профессор кафедры «Информационные системы и защита информации» ТГТУ, доктор технических наук.

Анисимов А.Д. - старший оператор научной роты войск РЭБ.

Брюханов А.А. - старший оператор научной роты войск РЭБ.

Вклад авторов

Алексеев В.В. - идея, научное редактирование текста (25%).

Анисимов А.Д. - написание статьи, сбор материала, обработка материала (40%).

Брюханов А.А. - написание статьи, сбор материала (35%).

Конфликт интересов отсутствует.

Научная статья
УДК 004.056.53

Применение технологии киберобмана для защиты баз данных

Владимир Витальевич Алексеев¹, Денис Александрович Вислобоков^{2✉},
Илья Сергеевич Шишкин³, Евгений Сергеевич Маленков⁴

^{1, 2, 3}Тамбовский государственный технический университет, Тамбов, Россия

⁴Российская академия народного хозяйства и государственной службы
при Президенте Российской Федерации, Москва, Россия

¹vvalex1961@mail.ru , <https://orcid.org/0000-0002-0398-4426>

²denis.vislobokov@mail.ru ✉ , <https://orcid.org/0009-0006-6986-4132>

³ilya.shis@yandex.ru , <https://orcid.org/0009-0004-6413-8364>

⁴z.malenkov@yandex.ru , <https://orcid.org/0009-0005-9416-1167>

Аннотация. В статье рассматривается применение технологии киберобмана для защиты баз данных за счёт использования ложных экземпляров популярных СУБД (MySQL, Redis и др.). Проведён обзор существующих ловушек с открытым исходным кодом, таких как mysql-honeypotd и RedisHoneyPot, и выполнено их тестирование в изолированной среде. Результаты показали, что такие ловушки фиксируют попытки подключения и выполняемые команды, позволяя выявлять подозрительную активность. Это подтверждает целесообразность использования ложных баз данных как средства повышения проактивной защиты.

Ключевые слова: информационная безопасность, кибербезопасность, honeypot, deception technology, база данных.

Для цитирования: Алексеев В.В., Вислобоков Д.А., Шишкин И.С., Маленков Е.С. Применение технологии киберобмана для защиты баз данных // Актуальные проблемы кибербезопасности. Противодействие экстремизму и терроризму в информационной молодежной среде: сборник докладов I межрегиональной научно-практической конференции. – Брянск: БГТУ, 2025. – С. 16 – 21.

Базы данных (БД) играют ключевую роль в современных информационных системах, обеспечивая централизованное хранение, обработку и доступ к критически важной информации. Они лежат в основе множества бизнес-процессов, включая управление пользователями, финансовыми транзакциями, логистикой и внутренней аналитикой. Именно благодаря высокой концентрации ценных данных – таких как персональная информация, учетные записи, коммерческая тайна и финансовые отчёты – базы данных становятся одной из главных целей для злоумышленников при совершении кибератак [1*Ошибка! Источник ссылки не найден.*].

Нарушение конфиденциальности или целостности баз данных может привести к серьёзным последствиям: утечке чувствительной информации, репутационным потерям, финансовому ущербу и нарушению правовых требований. В связи с этим злоумышленники активно применяют разнообразные техники для получения несанкционированного доступа к базам данных – от эксплуатации

уязвимостей SQL-инъекций до использования украденных учётных данных **[Ошибка! Источник ссылки не найден.]**.

На этом фоне актуальной задачей становится не только защита реальных баз данных, но и создание систем активной защиты, способных выявлять злоумышленников на ранних этапах проникновения. Одним из подобных подходов в рамках технологии киберобмана (Deception technology) является размещение ложных (имитированных) баз данных – ловушек, предназначенных для привлечения и отслеживания действий нарушителей. Такие ловушки создают убедительную иллюзию ценных целей, атаки на которые не представляют реальной угрозы для бизнеса, и при этом позволяют фиксировать аномальные действия, анализировать поведение злоумышленников и выстраивать более точные механизмы реагирования. Использование имитированных баз данных значительно снижает вероятность ложных срабатываний и усиливает систему защиты, особенно в условиях недостаточной эффективности традиционных методов мониторинга.

Защита баз данных в технологии киберобмана

Применение технологии киберобмана для защиты баз данных подразумевает размещение в информационной системе наряду с реально используемыми базами их ложных копий, не содержащих конфиденциальной информации. Для обеспечения реалистичности такой ложной инфраструктуры в целом и повышения вероятности атаки именно на ложные цели, следует использовать в качестве имитируемых баз данных именно те виды, которые реально используются (MySQL, PostgreSQL, Redis, MongoDB) **[Ошибка! Источник ссылки не найден.]**. Для обеспечения такой возможности, система защиты на основе технологии киберобмана должна быть способна обнаруживать существующие в системе базы данных и создавать их ложные аналоги, для чего необходимо наличие соответствующей ловушки под каждую базу данных.

Ловушки для имитации баз данных уже существуют в виде открытого программного обеспечения и находятся в свободном доступе **[Ошибка! Источник ссылки не найден.]**. Среди них стоит отметить pg-server, mysql-honeypotd, RedisHoneyPot и MongoDB-HoneyProxy для, соответственно, баз данных PostgreSQL, MySQL, Redis и MongoDB.

Ловушка pg-server – это эмулятор сервера PostgreSQL, который можно использовать в качестве прокси, ловушки или для фильтрации запросов. Он позволяет перехватывать и модифицировать SQL-запросы, передаваемые между клиентом и реальным сервером. С помощью него можно, например, ограничить доступ к определённым таблицам или запретить выполнение сложных запросов, таких как JOIN. Также он может имитировать PostgreSQL сервер, создавая ловушку для злоумышленников **[Ошибка! Источник ссылки не найден.]**.

Ловушка mysql-honeypotd – это низкоинтерактивная ловушка MySQL, написанная на C, которая имитирует работу MySQL сервера. Она записывает все попытки подключения и неудачные попытки авторизации, предоставляя ценную информацию о возможных атаках на сервер. Ловушка имеет настраиваемые па-

раметры, такие как IP-адрес, порт, задержки между попытками входа и возможность работы в фоновом режиме. Она используется для привлечения злоумышленников, которые пытаются получить несанкционированный доступ к базе данных MySQL **[Ошибка! Источник ссылки не найден.]**.

Ловушка RedisHoneyPot – это высокоинтерактивная ловушка, поддерживающая Redis-протокол, разработанная на языке программирования Go (Golang). Основная функция RedisHoneyPot – эмуляция поведения Redis-сервера, что позволяет специалистам по безопасности обеспечивать мониторинг и изучать возможные злонамеренные взаимодействия, нацеленные на базы данных Redis. Поддерживаемые команды: ping, info, set, get, del, exists, keys, flushall, flushdb, save, select, dbsize, config, slaveof **[Ошибка! Источник ссылки не найден.]**.

Ловушка MongoDB-HoneyProxu – это проект, разработанный в ответ на проблему «MongoDB Apocalypse», когда незащищённые MongoDB-серверы стали уязвимыми для атак **[Ошибка! Источник ссылки не найден.]**. Этот инструмент действует как прокси-сервер для MongoDB, который логирует все запросы, проходящие через него, что позволяет отслеживать подозрительную активность и повысить безопасность базы данных. MongoDB-HoneyProxu предоставляет возможность создания фальшивых данных, которые могут использоваться для ловли и анализа атакующих, при этом скрывая реальную информацию базы данных **[Ошибка! Источник ссылки не найден.]**.

Тестирование ложных баз данных

Для подтверждения возможности использования технологии киберобмана для защиты баз данных, необходимо провести тестирование работоспособности некоторых из представленных выше ловушек. Для этого требуется осуществить их установку на условный узел, попытаться подключиться к базе данных и оценить реакцию ловушки на это. В качестве условного узла будет использоваться виртуальная машина с операционной системой (ОС) Ubuntu Server 24.04.2. Подключение будет осуществляться с другой виртуальной машины с ОС Kali Linux.

В качестве ложной БД MySQL используется ловушка mysql-honeypotd. Для её установки требуется выполнить следующую последовательность команд:

1. Установка необходимых зависимостей:

```
sudo apt update
```

```
sudo apt install git build-essential libev-dev -y .
```

2. Клонирование репозитория:

```
git clone https://github.com/sjinks/mysql-honeypotd.git
```

```
cd mysql-honeypotd .
```

3. Сборка приложения:

```
make .
```

4. Запуск ловушки с выводом в консоль и прослушкой порта 3306 (стандартный порт MySQL):

```
sudo ./mysql-honeypotd -f -p 3306 .
```

Ловушка успешно запущена и готова принимать подключения. Для тестирования требуется подключиться к серверу с помощью команды:

```
mysql -h 192.168.186.128 -P 3306 -u test -p
```

В итоге, ловушка обнаружила подключение и в консоли появился соответствующий вывод:

```
mysql-honeypotd [7881]: New connection from 192.168.186.129:54282  
[192.168.186.129] to 192.168.186.128:3306
```

```
mysql-honeypotd [7881]: Access denied for user 'test' from  
192.168.186.129:54282 to 192.168.186.128:3306 (using password: NO; authentication  
plugin: mysql_native_password) mysql-honeypotd [7881]: Closing connection for  
192.168.186.129:54282
```

На основе этой информации уже можно определить адрес подключения, время подключения и имя пользователя. Вывод этих данных в какую-либо систему мониторинга позволит вовремя обнаружить злоумышленника и предпринять необходимые меры.

Следующая ловушка для тестирования – RedisHoneyPot. Для начала необходимо установить Go:

```
sudo apt install golang-go
```

Далее клонируется репозиторий:

```
git clone https://github.com/сypwnpwnsocute/RedisHoneyPot.git
```

```
cd RedisHoneyPot
```

Сборка проекта:

```
go build
```

Запуск ловушки в фоне с выводом данных в журнал:

```
nohup ./RedisHoneyPot -addr 0.0.0.0:6379 -proto tcp -num 1 > redis.log &
```

Ловушка успешно запущена и ожидает подключений. Для тестирования требуется подключиться к серверу с ловушкой, используя его адрес и стандартный порт Redis, а также выполнить несколько тестовых команд:

```
redis-cli -h 192.168.186.128 -p 6379
```

```
ping
```

```
set key "test"
```

```
get key
```

Для проверки журнала используется следующая команда:

```
tail -f redis.log
```

В итоге, ловушка записала следующую информацию:

```
{"action": "NewConnect", "addr":"192.168.186.129:34756","level": "info",  
"msg": , "time":"2025-04-09 09:43:25"}
```

```
 {"action": "COMMAND DOCS", "addr":"192.168.186.129:34756","level":  
"info", "msg": , "time":"2025-04-09 09:43:25"}
```

```
 {"action": "COMMAND", "addr":"192.168.186.129:34756","level": "info",  
"msg": "time":"2025-04-09 09:43:25"}
```

```
 {"action": "ping", "addr":"192.168.186.129:34756","level": "info", "msg":  
,"time": "2025-04-09 09:43:47"}
```

```
 {"action": "set key test", "addr":"192.168.186.129:34756","level": "info",  
"msg": "", "time": "2025-04-09 09:44:04"}
```

```
 {"action": "get key", "addr":"192.168.186.129:34756", "level": "info", "msg":  
,"time": "2025-04-09 09:44:08"}
```

По этим данным можно определить адрес и время подключения, а также действия потенциального злоумышленника. Информация представлена в стандартном для журналов событий виде и может быть легко экспортирована в системы мониторинга для своевременного обнаружения нежелательной активности и принятия соответствующих мер.

В условиях роста количества и сложности киберугроз защита баз данных требует применения не только пассивных, но и активных методов безопасности. Одним из наиболее перспективных подходов является использование технологии киберобмана, в частности – размещение ложных баз данных, имитирующих реальные цели. Такие ловушки позволяют не только выявлять попытки несанкционированного доступа, но и собирать информацию о поведении потенциальных злоумышленников, что особенно важно для своевременного реагирования на инциденты.

Рассмотренные решения – mysql-honeypotd, RedisHoneyPot, pg-server и MongoDB-HoneyProху – подтверждают техническую возможность развертывания имитированных баз данных с использованием открытого программного обеспечения. Результаты тестирования показывают, что даже при минимальной конфигурации ловушки способны эффективно фиксировать подключения и команды, отправленные нарушителями, тем самым повышая уровень информированности о попытках атак.

Интеграция подобных систем в инфраструктуру корпоративной безопасности позволяет повысить устойчивость к атакам, снизить вероятность ложных срабатываний и обеспечить дополнительный уровень защиты наиболее критичных ресурсов. В совокупности с системами мониторинга и реагирования, ловушки на основе киберобмана становятся мощным инструментом проактивной защиты, особенно актуальным в условиях постоянно эволюционирующих угроз.

Список источников

1. Россия заняла первое место в мире по количеству слитых в даркнет баз данных. URL: <https://www.vedomosti.ru/technology/articles/2024/07/30/1052737-rossiya-zanyala-pervoe-mesto-v-mire-po-kolichestvu-slitih-v-darknet-dannih>.
2. Защита базы данных. URL: https://rt-solar.ru/products/solar_dozor/blog/2719/.
3. Виды баз данных. Большой обзор типов СУБД. URL: <https://habr.com/ru/companies/amvera/articles/754702/>.
4. 70+ бесплатных приманок для ловли хакеров. URL: <https://habr.com/ru/companies/bastion/articles/731172/>.
5. Pg-server. URL: <https://github.com/oguimbal/pg-server>.
6. mysql-honeypotd. URL: <https://github.com/sjinks/mysql-honeypotd>.
7. RedisHoneyPot. URL: <https://github.com/cypwnpwnsocute/RedisHoneyPot>.

8. MongoDB Apocalypse Is Here as Ransom Attacks Hit 10,000 Servers.
URL: <https://www.bleepingcomputer.com/news/security/mongodb-apocalypse-is-here-as-ransom-attacks-hit-10-000-servers/>.
9. MongoDB-HoneyProxy. URL: <https://github.com/Plazmaz/MongoDB-HoneyProxy>.

Статья поступила в редакцию 11.04.2025; принята к публикации 10.05.2025

Информация об авторах

Алексеев В.В. – д.т.н., профессор, профессор кафедры «Информационные системы и защита информации» ФГБОУ ВО «ТГТУ».

Вислобоков Д.А. – аспирант кафедры «Информационные системы и защита информации», направление подготовки 2.3.6 – Методы и системы защиты информации, информационная безопасность ФГБОУ ВО «ТГТУ».

Шишкин И.С. – аспирант кафедры «Информационные системы и защита информации», направление подготовки 2.3.6 – Методы и системы защиты информации, информационная безопасность ФГБОУ ВО «ТГТУ».

Маленков Е.С. – магистрант кафедры «Государственное и муниципальное управление», направление подготовки 38.04.04 – Государственное управление социально-экономическим развитием ФГБОУ ВО «РАНХиГС».

Вклад авторов

Все авторы внесли эквивалентный вклад в подготовку публикации.

Конфликт интересов отсутствует.

Научная статья
УДК 004.056

Усовершенствованная система депонирования ключей шифрования в условиях проведения специальной военной операции с применением средств радиоэлектронной борьбы

**Артем Дмитриевич Анисимов^{1✉}, Александр Александрович Брюханов²,
Олег Алексеевич Воскобойников³**

^{1,2,3} Межвидовой центр подготовки и боевого применения (учебный и испытательный),
Тамбов, Россия

^{1,2,3}nauchnajarota@yandex.ru✉

Аннотация. Современные военные конфликты, включая формат специальной военной операции (СВО), сопровождаются активным применением средств радиоэлектронной борьбы (РЭБ), что существенно осложняет передачу, хранение и защиту криптографических данных. В таких условиях возрастает необходимость создания устойчивой и адаптивной системы депонирования ключей шифрования, обеспечивающей информационную безопасность и сохранность каналов управления войсками. В данной статье рассматривается концепция усовершенствованной системы депонирования ключей, соответствующей условиям применения средств РЭБ и особенностям оперативной обстановки.

Ключевые слова: усовершенствованная система депонирования ключей, утечка данных, криптографический протокол, закрытый ключ, открытый ключ, разделение секрета.

Для цитирования: Анисимов А.Д., Брюханов А.А., Воскобойников О.А. Усовершенствованная система депонирования ключей шифрования в условиях проведения специальной военной операции с применением средств радиоэлектронной борьбы // Актуальные проблемы кибербезопасности. Противодействие экстремизму и терроризму в информационной молодежной среде: сборник докладов I межрегиональной научно-практической конференции. – Брянск: БГТУ, 2025. – С. 22 – 29.

Появление и интенсивное развитие средств радиоэлектронного подавления в корне меняет условия применения традиционных криптографических механизмов. С развитием криптографических атак и появлением новых угроз цифровой безопасности стало очевидно, что необходимы новые, более надежные подходы к управлению ключами. Подразделения, действующие в зонах активной РЭБ, сталкиваются с невозможностью своевременного получения или обновления ключей, высоким риском их перехвата, а также угрозами физического захвата криптографических носителей. Обычные централизованные подходы к управлению ключами становятся уязвимыми, что требует перехода к более гибкой, распределённой и устойчивой архитектуре. В соответствии с этим были предложены усовершенствованные системы депонирования ключей, представляющие собой инновационный подход к обеспечению безопасности данных.

Усовершенствованная система депонирования ключей представляет собой метод хранения и управления ключами шифрования, который обеспечивает до-

полнительные уровни безопасности и контроля доступа по сравнению с традиционными методами. Основная идея заключается в том, чтобы разделить ключ на несколько частей и передать их различным доверенным сторонам, чтобы ни одна из них не имела полного доступа к ключу [**Ошибка! Источник ссылки не найден.**].

1. Особенности условий проведения СВО

Специфика проведения СВО заключается в высокой плотности средств РЭБ, которые создают постоянное давление на радиочастотные и спутниковые каналы связи, подавляя их работу, а также в высокой мобильности и рассредоточенности войск, часто действующих в автономном режиме. Временные окна связи могут быть крайне ограничены, а физическая передача ключевых данных сопряжена с рисками. В этих условиях необходимо обеспечить не только криптостойкость алгоритмов, но и возможность быстрого, надёжного и безопасного получения ключей при минимальной зависимости от централизованных систем.

В условиях боевых действий система депонирования должна быть интегрирована в общий цикл планирования и командования. Ключи готовятся заранее, распределяются по подразделениям согласно оперативным задачам и активируются в чётко определённое время. Командиры на местах получают ограниченный доступ, а ввод ключей осуществляется при участии нескольких уполномоченных лиц. После завершения задачи ключи автоматически деактивируются или уничтожаются [**Ошибка! Источник ссылки не найден.**].

Такой подход позволяет снизить нагрузку на операционные службы, исключить утечку информации при захвате оборудования и обеспечить стабильную работу даже в условиях полного радиомолчания. При этом предусмотрены процедуры экстренного восстановления доступа и протоколы обработки нестандартных ситуаций.

2. Концепция усовершенствованной системы

В условиях СВО система депонирования ключей должна строиться по принципу децентрализации, с возможностью автономной работы на уровне тактического звена. Центральный орган криптографического управления обеспечивает предварительное планирование и формирование ключевого материала на определённые временные интервалы. Этот материал доставляется в войска заранее, упакованный в защищённые криптоконтейнеры, которые активируются строго по времени или по сигналу. Такой подход исключает необходимость постоянного обмена ключами в реальном времени и снижает уязвимость к РЭБ.

Передача ключей осуществляется по заранее определённым маршрутам с использованием защищённых каналов, устойчивых к радиоподавлению, в том числе на основе перестройки частот и временных интервалов связи. При невозможности использования связи допускается физическая передача криптоконтейнеров курьером или через вспомогательные носители, снабжённые механизмами автоматического уничтожения в случае угрозы захвата. Ключи при этом являются одноразовыми и ограничены по сроку действия, что минимизирует ущерб даже в случае их компрометации.

Криптографические модули, находящиеся в распоряжении подразделений, способны работать без подключения к сети, содержат изолированную среду выполнения и защищены от физического взлома. В случае чрезвычайной ситуации может быть запущена процедура самоуничтожения или блокировки ключевого материала.

Одной из ключевых проблем являются уязвимости и риски, связанные с хранением шифровальных ключей. Их компрометация может привести к серьезным последствиям, таким как утечка конфиденциальной информации и нарушение приватности пользователей. Кроме того, существует угроза атак на системы хранения ключей. Злоумышленники могут применять различные методы для доступа к зашифрованным данным, включая перехват трафика и эксплуатацию уязвимостей в программном обеспечении. Поэтому необходимо создать систему, которая надежно защитит шифровальные ключи и обеспечит высокий уровень безопасности [Ошибка! Источник ссылки не найден.].

Рассмотрев процесс создания и распределения ключей в описанной криптографической системе, следует перейти к анализу самого протокола и процесса взаимодействия его участников, а также к диаграмме последовательностей (рис. 1).

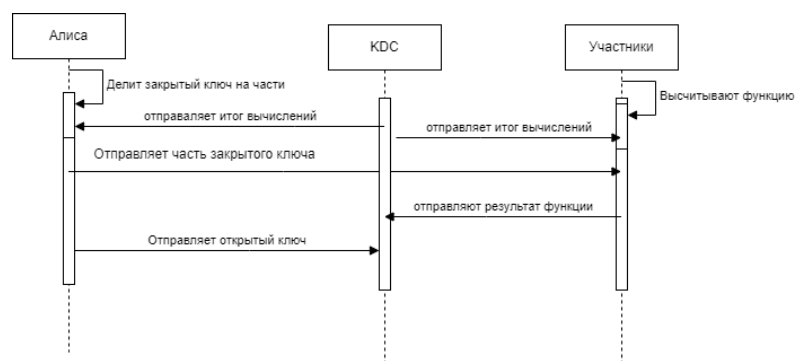


Рис. 1. Диаграмма последовательностей протокола

Представлю разработанную программу демонстрирующую усовершенствованную систему депонирования ключей.

Разработка ПО проводилась на языке C#. C# – объектно-ориентированный язык программирования общего назначения. Однако, как и у любого языка, у него есть свои преимущества и недостатки, которые следует учитывать при выборе для конкретного проекта [Ошибка! Источник ссылки не найден.].

На рисунке 2 представлен стартовый интерфейс программы, состоящий из таких управляющих элементов, как кнопки «Разделить секрет» и «Восстановить секрет», полей, выводящих исходное уравнение, номера и значения теней, восстановленное значение секрета и результат валидности теней.

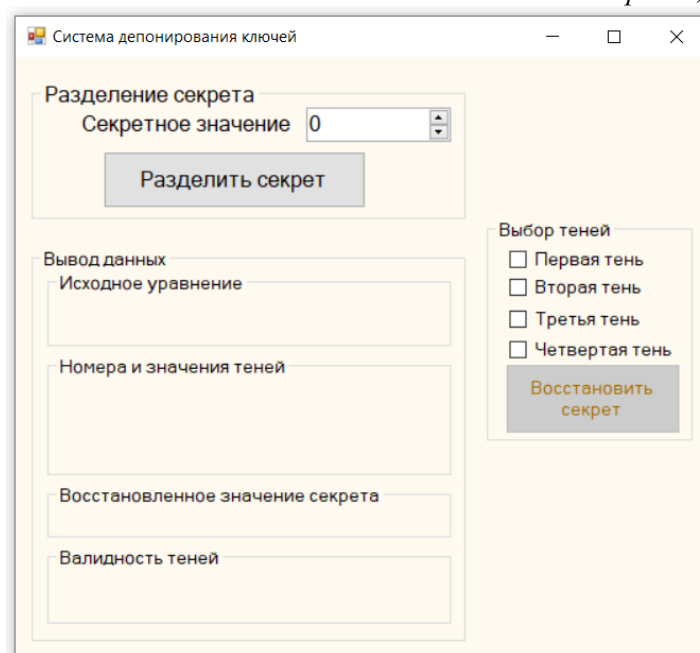


Рис. 2. Главный интерфейс ПО

В данном окне необходимо выбрать секретное значение, которое впоследствии будет разделяться, и нажать кнопку «Разделить секрет». Для ввода секрета можно как ввести значение в поле «Секретное значение» вручную с клавиатуры, так и воспользоваться ползунком для выбора значения (рис. 3).

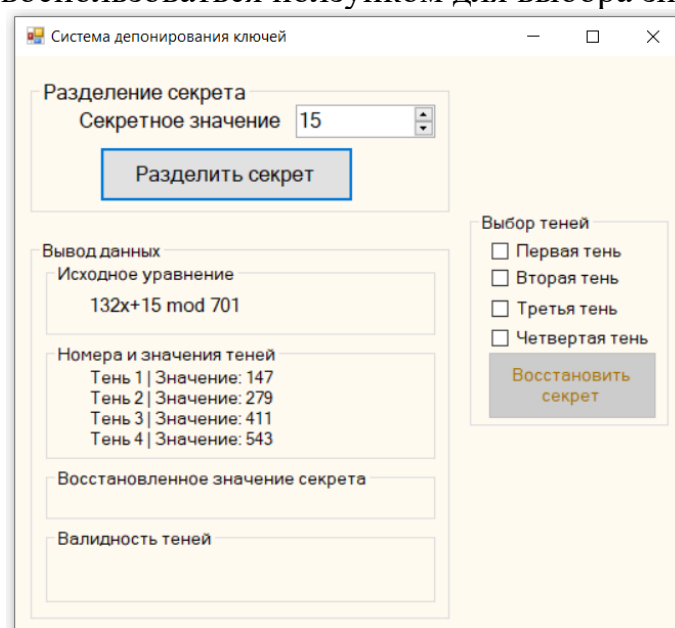


Рис. 3. Выбор секретного значения

Секретное значение делится на четыре тени, формируется исходное уравнение, включающее случайные коэффициенты, значение секрета и простое число, а также генерируются закрытые, открытые ключи и подписи для проверки подлинности теней (рис. 4).

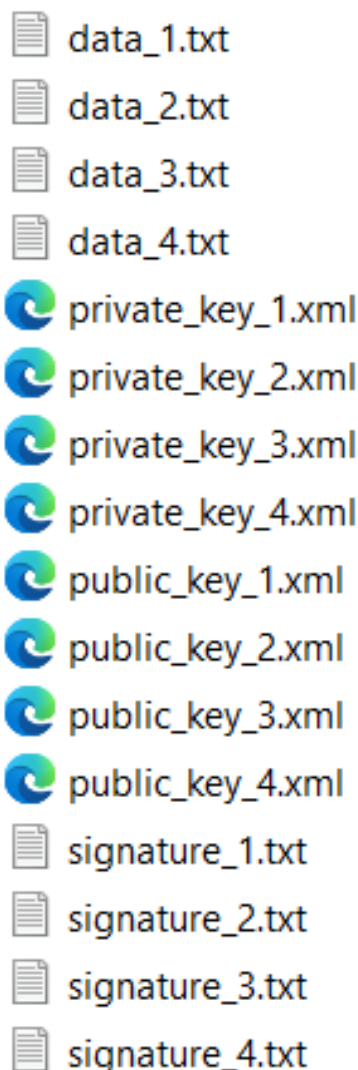


Рис. 4. Формирование значения секрета, закрытых, открытых ключей, а также подписи

Закрытые ключи записываются в файлы формата XML (рис. 5).

```
<RSAKeyValue>
  <Modulus>tV/8earsq/q45erHDHwivKl+P+SQm+T34UUoItfneSHmVi+hpGw2ZfgGjc5RkpIlj60FhUssApgeaV0mnanPd2QXGxVQcHHp9MmI7biJ
  </Modulus>
  <Exponent>AQAB</Exponent>
</RSAKeyValue>
```

Рис. 5. Закрытый ключ для первой тени

Открытые ключи также записываются в файлы формата XML (рис. 6).

```
<RSAKeyValue>
  <Modulus>tV/8earsq/q45erHDHwivKl+P+SQm+T34UUoItfneSHmVi+hpGw2ZfgGjc5RkpIlj60FhUssApgeaV0mnanPd2QXGxVQcHHp9MmI7biJ
  </Modulus>
  <Exponent>AQAB</Exponent>
</RSAKeyValue>
```

Рис. 6. Открытый ключ для первой тени

Затем необходимо выбрать нужное количество теней для восстановления, установив галочку напротив тени в поле «Выбор теней», и нажать кнопку «Восстановить секрет» (рис. 7).

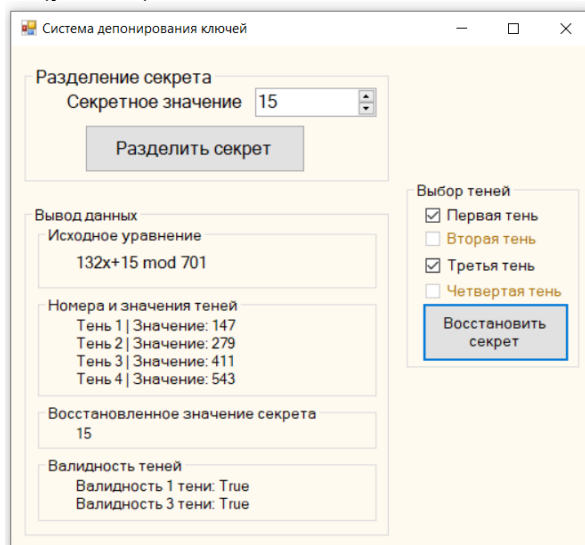


Рис. 7. Восстановление секрета

В случае, если значение тени будет подменено, то секрет восстановится неверным, а также будет показано какая тень не является подлинной, что поможет быстро обнаружить злоумышленника (рис. 8).

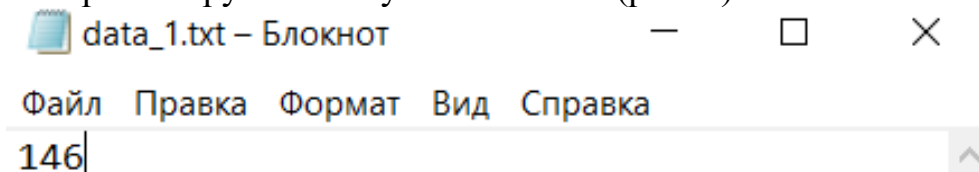


Рис. 8. Изменение первой тени

В поле «Валидность теней» напротив подмененной тени установится значение «False» вместо «True» (рис. 9).

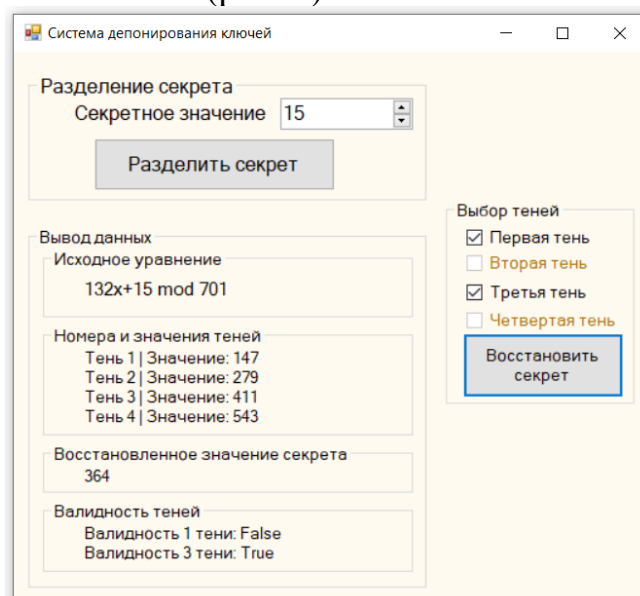


Рис. 9. Интерфейс неверного восстановления секрета и нарушения целостности первой тени

Таким образом, ПО, реализующее усовершенствованную систему депонирования ключей, помимо разделения и восстановления секрета, информирует о нарушении целостности конкретной тени, что позволяет быстро обнаружить злоумышленника.

Для реализации ПО использован язык программирования C#, поскольку он является кроссплатформенным, объектно-ориентированным, взаимодействующим с экосистемой Windows и постоянно развивающимся.

Переход к усовершенствованной системе депонирования ключей шифрования является объективной необходимостью в условиях современной СВО с активным применением средств РЭБ. За счёт распределённой архитектуры, автономной работы и высокой устойчивости к внешним воздействиям, такая система обеспечивает надёжную защиту критически важной информации, сохраняя управляемость войсками и их боеспособность в сложнейших условиях радиоэлектронного подавления. Основная идея усовершенствованных систем депонирования ключей заключается в том, чтобы обеспечить безопасное хранение ключей, предотвратить их утрату, кражу или несанкционированный доступ, а также обеспечить возможность доступа к ним только авторизованным лицам. Такие системы могут включать в себя механизмы шифрования, многофакторную аутентификацию, а также физические меры безопасности [**Ошибка! Источник ссылки не найден.**].

Внедрение подобных решений требует не только технической, но и организационной подготовки, включая переобучение личного состава и интеграцию криптографической защиты в общее планирование операций.

Список источников

1. Рубин Ф. Криптография с секретным ключом. М.: ДМК Пресс, 2023. - 386 с.
2. Гриднев В. А. Правовой подход к построению системы защиты информации в организации / В. А. Гриднев, В. В. Алексеев, Е. В. Емельянов, А. Д. Кастерин // Правовая информатика. 2020. № 2. С. 54 – 61.
3. Шнайер Б. Прикладная криптография. - М.: Триумф, 2003. - 806 с.
4. Алексеев В. В. Программное обеспечение, реализующее алгоритм Шамира в стойких частных криптосистемах / В. В. Алексеев В. А. Гриднев, А. Ю. Селиванов // Правовая информатика. 2021. № 3. С. 50 – 59.
5. Гриднев В. А. Организационно-правовые вопросы внедрения стойких частных криптосистем / В. А. Гриднев, И. С. Володин, А. М. Желудкова // Правовая информатика. 2021. № 1. С. 51 – 60.

Статья поступила в редакцию 19.04.2025; принята к публикации 10.05.2025

Информация об авторах

Анисимов А.Д. - старший оператор научной роты войск РЭБ.

Брюханов А.А. - старший оператор научной роты войск РЭБ.

Воскобойников О.А. - оператор научной роты войск РЭБ.

Вклад авторов

Анисимов А.Д. - подбор литературных источников, частичное написание статьи (20%).

Брюханов А.А. - редактирование визуальной части (рисунков), разработка программного обеспечения, частичное написание статьи (60%).

Воскобойников О.А. - научное редактирование текста, частичное написание статьи (20%).

Конфликт интересов отсутствует.

Научная статья

УДК 004.056

Киберугрозы и оборона: как современные конфликты меняют подходы к информационной безопасности в армии

Кирилл Александрович Анищенков¹, Федор Евгеньевич Березкин^{2✉},
Алексей Владимирович Евдокимов³

^{1, 2, 3}Брянский государственный технический университет, Брянск, Россия

¹kirill.anishenkov@gmail.com, <https://orcid.org/0009-0000-9011-2804>

²fedor.berezkin32@yandex.ru[✉], <https://orcid.org/0009-0002-0105-7335>

³alekseievdokimov05@gmail.com, <https://orcid.org/0009-0004-4331-1279>

Аннотация. В данной статье исследуется трансформация подходов к обеспечению информационной безопасности в вооруженных силах, обусловленная возрастающей ролью киберпространства в современных конфликтах.

Ключевые слова: киберугрозы, информационная безопасность, военные конфликты, искусственный интеллект, кибероборона.

Для цитирования: Анищенков К.А., Березкин Ф.Е., Евдокимов А.В. Киберугрозы и оборона: как современные конфликты меняют подходы к информационной безопасности в армии // Актуальные проблемы кибербезопасности и их решения. Противодействие экстремизму и терроризму в информационной молодежной среде: сборник докладов I межрегиональной научно-практической конференции. – Брянск: БГТУ, 2025. – С. 30 – 34.

Современные военные конфликты перешли в эру, где Современная эпоха характеризуется стремительной цифровизацией всех сфер жизни, и военная область не является исключением. Глубокое проникновение информационно-коммуникационных технологий в системы управления войсками, разведку, логистику и даже в функционирование отдельных образцов вооружения и военной техники привело к формированию новой среды противоборства – киберпространства. Сегодня вооруженные конфликты все чаще приобретают гибридный характер, где наряду с традиционными военными действиями активно применяются методы информационного и кибернетического воздействия. Это обстоятельство заставляет пересматривать устоявшиеся подходы к обеспечению информационной безопасности в вооруженных силах, выдвигая новые, более сложные задачи перед системами киберобороны. Киберугрозы становятся не просто дополнением к конвенциональным средствам поражения, а самостоятельным и зачастую более эффективным инструментом достижения военно-политических целей, способным нанести ущерб не только военным объектам, но и критически важной инфраструктуре государства, а также повлиять на морально-психологическое состояние населения и личного состава армии [1].

Трансформация характера угроз в киберпространстве является ключевым фактором, определяющим изменения в военных доктринах и стратегиях инфор-

мационной безопасности. Если ранее основное внимание уделялось защите закрытых военных сетей от несанкционированного доступа и шпионажа, то современные конфликты демонстрируют гораздо более широкий спектр кибератак. Противник стремится не только получить доступ к секретной информации, но и нарушить или полностью парализовать работу систем боевого управления, связи, навигации и целеуказания. Атаки типа "отказ в обслуживании" (DDoS), внедрение вредоносного программного обеспечения, способного вывести из строя оборудование или исказить передаваемые данные, становятся рутинными элементами противоборства. Примером могут служить целенаправленные атаки на системы C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance), нарушение функционирования которых может дезорганизовать управление войсками и лишит командование оперативной информации о действиях противника и обстановке на поле боя [2]. Особую опасность представляют атаки на системы управления высокоточным оружием и беспилотными летательными аппаратами, способные привести к непредсказуемым последствиям, включая потерю контроля над боевыми средствами.

Более того, киберпространство активно используется для ведения информационно-психологической войны. Современные конфликты наглядно показывают, как социальные медиа и интернет-ресурсы превращаются в поле боя за умы и настроения людей [3]. Целенаправленные кампании по дезинформации, распространение фейковых новостей, пропаганда, направленная на дискредитацию военно-политического руководства страны и командования вооруженных сил, деморализацию личного состава и населения – все это стало неотъемлемой частью гибридных войн. Противник активно использует методы социальной инженерии, фишинговые атаки и эксплуатирует уязвимости, связанные с человеческим фактором, для проникновения в системы и получения информации, в том числе через личные аккаунты военнослужащих в социальных сетях. Неосторожное поведение военнослужащих в киберпространстве, публикация фотографий, видеоматериалов, геолокационных данных или служебной информации может привести к утечке критически важных сведений и создать угрозу безопасности как для отдельных лиц, так и для целых подразделений [4]. Это требует не только технических мер защиты, но и повышения уровня цифровой грамотности и информационной культуры всего личного состава.

В ответ на эти вызовы вооруженные силы вынуждены кардинально менять свои подходы к организации киберобороны. Происходит переход от пассивной защиты периметра сетей к проактивной стратегии, включающей непрерывный мониторинг киберпространства, выявление угроз на ранних стадиях, анализ тактик и инструментов потенциального противника, а также разработку мер по активному противодействию. Создаются специализированные кибервойска или киберкомандования, наделенные широкими полномочиями и ресурсами для ведения операций в киберпространстве как оборонительного, так и наступательного характера [5]. Оборонительные задачи включают защиту собственных информационных систем, сетей и баз данных от несанкционированного доступа, атак и вредоносного воздействия. Это предполагает внедрение многоуровневых

систем защиты (defense-in-depth), использование современных средств криптографии, систем обнаружения и предотвращения вторжений, а также регулярное проведение аудитов безопасности и тестирование на проникновение [1]. Важной составляющей становится обеспечение устойчивости и живучести информационных систем, способности быстро восстанавливать работоспособность после кибератак.

Наступательные кибероперации, в свою очередь, могут рассматриваться как средство сдерживания потенциального агрессора, а также как инструмент для получения разведывательной информации, нарушения работы вражеских систем управления и связи, проведения информационно-психологических акций. Развитие таких возможностей требует не только высокотехнологичных программно-аппаратных комплексов, но и наличия высококвалифицированных специалистов – "кибербойцов", способных разрабатывать и применять сложные инструменты кибервоздействия [2]. Подготовка таких кадров становится одним из приоритетных направлений развития современных армий. Требуются специалисты не только в области программирования и сетевых технологий, но и в криптографии, анализе данных, психологии, лингвистике. Привлечение и удержание таких экспертов в военной сфере является отдельной сложной задачей, учитывая высокую конкуренцию с коммерческим сектором [3].

Современные конфликты также подчеркивают важность защиты не только сугубо военных информационных систем, но и объектов критической информационной инфраструктуры (КИИ) государства, таких как энергетические сети, транспортные узлы, финансовые системы, системы здравоохранения и государственного управления. Атаки на КИИ могут иметь катастрофические последствия, сравнимые с применением традиционных видов оружия, и зачастую используются как элемент гибридной войны для дестабилизации обстановки в стране и подрыва ее обороноспособности [4]. Это требует тесного взаимодействия между военными структурами, отвечающими за кибероборону, и гражданскими ведомствами, ответственными за безопасность КИИ. Необходимо создание единых национальных систем обнаружения, предупреждения и ликвидации последствий компьютерных атак, обмен информацией об угрозах и инцидентах, координация действий при реагировании на киберкризисы.

Особое внимание в современных условиях уделяется обеспечению информационной безопасности на тактическом уровне. С развитием концепции сетцентрической войны, предполагающей объединение всех участников боевых действий – от штабов до отдельных солдат и единиц боевой техники – в единую информационную сеть, возрастает количество потенциальных точек входа для кибератак [5]. Планшеты командиров, наשלменные дисплеи, системы связи и навигации, датчики на боевой технике – все это становится потенциальными целями для противника. Защита этих распределенных и зачастую мобильных систем требует новых подходов, включая использование защищенных протоколов связи, шифрование данных "на лету", разработку встроенных средств безопасности для тактических устройств и постоянное обновление программного обеспечения для устранения уязвимостей.

Еще одним аспектом, меняющим подходы к информационной безопасности, является все более широкое применение технологий искусственного интеллекта (ИИ) и машинного обучения как в средствах нападения, так и в системах защиты. ИИ может использоваться для автоматизации разведки уязвимостей, создания самоадаптирующихся вредоносных программ, проведения сложных фишинговых кампаний и управления ботнетами [1]. С другой стороны, ИИ и машинное обучение становятся незаменимыми инструментами для анализа больших объемов данных о сетевом трафике, выявления аномалий, указывающих на кибератаку, прогнозирования угроз и автоматизации процессов реагирования. Внедрение ИИ в системы киберобороны позволяет значительно повысить скорость и эффективность обнаружения и нейтрализации атак, что критически важно в условиях постоянно возрастающей сложности и интенсивности киберпротивоборства [2]. Однако использование ИИ также порождает новые вызовы, связанные с безопасностью самих ИИ-систем, их уязвимостью к атакам (например, атакам на обучающие данные) и необходимостью обеспечения доверия к принимаемым ими решениям.

Таким образом, опыт современных конфликтов демонстрирует, что киберпространство стало полноценной сферой военного противоборства, а киберугрозы – одним из ключевых факторов, влияющих на национальную безопасность и обороноспособность государства. Это требует от вооруженных сил непрерывной адаптации и совершенствования подходов к обеспечению информационной безопасности. Недостаточно просто защищать существующие сети и системы; необходимо выстраивать комплексную, эшелонированную и проактивную систему киберобороны, охватывающую все уровни управления – от стратегического до тактического.

Список источников

1. Зеленков М. Ю., Ахмадулина Э. Р. Основы информационной безопасности Вооруженных сил Российской Федерации в социальных медиаресурсах // Вестник Московского государственного лингвистического университета. Общественные науки. 2020. № 2 (839). С. 148–163. URL: <https://cyberleninka.ru/article/n/osnovy-informatsionnoy-bezopasnosti-vooruzhennyh-sil-rossiyskoy-federatsii-v-sotsialnyh-media-resursah/viewer> (дата обращения: 14.04.2025).
2. Кибервойны: новая реальность современных конфликтов // IT-портал Дзен. 2024. URL: <https://dzen.ru/a/Z4e1SPqH6ms9siQZ> (дата обращения: 14.04.2025).
3. Информационная война и роль IT-экспертов: защита от киберугроз в военной сфере // Блог Astana Hub. 2023. URL: <https://astanahub.com/ru/blog/informatsionnaia-voina-i-rol-it-ekspertov-zashchita-ot-kiberugroz-v-voennoi-sfere> (дата обращения: 14.04.2025).

4. Абрамов Е. С., Кулдошин А. И. Сетецентрические войны в аспекте информационного противоборства // Вестник компьютерных и информационных технологий. 2008. № 12. С. 38–42. URL: <https://vestnik-tekh.ru/files/6005b4ccad0d20.30400936.24.pdf> (дата обращения: 14.04.2025).

5. Военная IT-оборона: стратегии, вызовы и будущие тенденции // Информационный портал Ярцевский.рф. 2024. URL: <https://ярцевский.рф/press-czentr/voennaya-it-oborona-strategii-vyzovy-i-budushhie-tendenczii> (дата обращения: 14.04.2025).

Статья поступила в редакцию 22.04.2025 принята к публикации 10.05.2025

Информация об авторах

Анищенков К.А. – студент кафедры «Системы информационной безопасности», направление подготовки 10.05.03 – Информационная безопасность автоматизированных систем ФГБОУ ВО «БГТУ».

Березкин Ф.Е. – студент кафедры «Системы информационной безопасности», направление подготовки 10.05.03 – Информационная безопасность автоматизированных систем ФГБОУ ВО «БГТУ».

Евдокимов А.В. – студент кафедры «Системы информационной безопасности», направление подготовки 10.05.03 – Информационная безопасность автоматизированных систем ФГБОУ ВО «БГТУ».

Вклад авторов

Анищенков К.А. – идея, сбор материала, обработка материала, частичное написание статьи (33%).

Березкин Ф.Е. – идея, сбор материала, обработка материала, частичное написание статьи (33%).

Евдокимов А.В. – идея, сбор материала, обработка материала, частичное написание статьи (34%).

Научный руководитель

Шапенская А.М. – ассистент кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Конфликт интересов отсутствует.

Научная статья

УДК 656.025.4:004.056

Оптимизация маршрутов снабжения с учётом киберрисков и геополитических угроз

Федор Евгеньевич Березкин ^{1✉}, Кирилл Викторович Бобков ²,
Алина Михайловна Шапенская ³, Максим Михайлович Голембиовский⁴

^{1, 2, 3, 4}Брянский государственный технический университет, Брянск, Россия

¹fedor.berezkin32@yandex.ru[✉], <https://orcid.org/0009-0002-0105-7335>

²kirillbobbkof2004@yandex.ru, <https://orcid.org/0009-0000-6467-1514>

^{3, 4}alinashapenskaya@yandex.ru, <https://orcid.org/0009-0007-8434-5848>

Аннотация. В данной статье исследуется проблема оптимизации логистических маршрутов в условиях возрастающих кибернетических и геополитических рисков. Анализируется, как цифровая трансформация логистики создает новые уязвимости, а геополитическая нестабильность нарушает традиционные цепочки поставок. Обосновывается необходимость перехода от классических методов оптимизации, сфокусированных на затратах, к риск-ориентированным подходам, интегрирующим оценку и управление современными угрозами для повышения устойчивости снабжения.

Ключевые слова: логистика, цепочки поставок, оптимизация маршрутов, кибербезопасность, геополитические риски.

Для цитирования: Березкин Ф.Е., Бобков К.В., Шапенская А.М., Голембиовский М.М. Оптимизация маршрутов снабжения с учётом киберрисков и геополитических угроз // Актуальные проблемы кибербезопасности и их решения. Противодействие экстремизму и терроризму в информационной молодежной среде: сборник докладов I межрегиональной научно-практической конференции. – Брянск: БГТУ, 2025. – С. 35 – 38.

Современная мировая экономика строится на сложных, разветвленных цепочках поставок. Для любой компании, стремящейся к успеху и стабильности, крайне важно обеспечить, чтобы ее логистика работала без сбоев и эффективно. Однако привычные способы планирования маршрутов, где главной целью было сэкономить время и деньги, сегодня уже не справляются со всеми вызовами. Дело в том, что к обычным проблемам вроде плохой погоды или поломки машины добавились новые, куда более серьезные угрозы – кибератаки и геополитическая нестабильность. Игнорировать их нельзя, ведь они могут привести к катастрофическим последствиям. Поэтому сейчас перед логистами стоит задача научиться учитывать эти новые риски при планировании маршрутов, чтобы сделать цепочки поставок по-настоящему надежными.

Цифровые технологии прочно вошли в логистику. Системы управления транспортом и складами, интернет вещей для отслеживания грузов, облачные сервисы для обмена документами – все это сильно ускорило и упростило работу, сделало ее прозрачнее [1]. Но у этой медали есть и обратная сторона: чем больше процессов уходит в онлайн, тем больше появляется лазеек для хакеров. Логистические компании хранят и обрабатывают массу ценной информации: о грузах, клиентах, маршрутах, финансах, сотрудниках. Если эта информация попадет не

в те руки или если злоумышленники нарушат работу управляющих систем, последствия могут быть очень тяжелыми – от денежных потерь и удара по репутации до полной остановки перевозок [2]. Киберугрозы для логистики разнообразны. Это и программы-вымогатели, блокирующие доступ к важным данным, и фишинговые письма для кражи паролей, и атаки, выводящие из строя сайты и онлайн-сервисы, и даже целенаправленные взломы систем управления транспортом [3]. Проблема усугубляется тем, что логистические цепочки – это целые экосистемы, где множество участников зависят друг от друга: производители, поставщики, перевозчики, склады, таможня, IT-компании. Достаточно одному звену в этой цепи оказаться слабо защищенным, как под угрозой оказываются все остальные [4]. Например, если хакеры взломают систему небольшой транспортной фирмы, они могут узнать графики движения ценных грузов и использовать это для кражи. А атака на провайдера облачной логистической платформы может парализовать работу сразу множества его клиентов [5]. Поэтому компаниям нужно заботиться не только о собственной киберзащите, но и внимательно проверять своих партнеров, прописывать требования безопасности в договорах и регулярно проводить проверки [1]. Одновременно с ростом киберугроз мир сталкивается с серьезной геополитической нестабильностью. Конфликты, торговые споры, санкции, политические кризисы в разных регионах напрямую влияют на международные перевозки, причем часто непредсказуемо [2]. Закрытие границ, воздушного пространства или морских путей, новые ограничения на ввоз или вывоз товаров, усложнение таможни, пиратство – все это может сорвать поставки, увеличить сроки и стоимость доставки. Компаниям приходится срочно искать обходные пути, которые могут быть дороже или дольше, но зато надежнее в текущей ситуации [3]. Например, недавние события в Красном море заставили многие судоходные линии пускать корабли вокруг Африки, что резко увеличило время и стоимость перевозок.

Самое сложное в том, что киберугрозы и геополитические проблемы часто идут рука об руку и усиливают друг друга. Когда отношения между странами накаляются, нередко учащаются и кибератаки, в том числе спонсируемые государствами. Их целью может стать критическая инфраструктура противника, включая транспорт и логистику [4]. Такие атаки могут быть направлены не просто на кражу данных или денег, а на то, чтобы навредить экономике, нарушить поставки важных товаров, посеять хаос. С другой стороны, если хакеры атакуют крупный порт или аэропорт в и без того нестабильном регионе, последствия будут куда серьезнее, чем в спокойной обстановке. Это может усугубить уже существующие проблемы с движением транспорта и безопасностью коридоров.

В таких условиях старые методы оптимизации маршрутов, ориентированные только на стоимость и время, больше не работают. Они не учитывают непредсказуемый характер кибернетических и геополитических рисков – событий, которые случаются не так часто, но если случаются, то приводят к огромному ущербу. Маршрут, который казался оптимальным по старым меркам, может оказаться совершенно незащищенным перед новыми угрозами. Значит, нужен новый подход – риск-ориентированная оптимизация. Выбирать маршрут нужно не только исходя из того, насколько он дешев и быстр, но и оценивая, насколько он подвержен разным опасностям и насколько вся цепочка поставок будет устойчива, если что-то пойдет не так. Создать такие модели непросто. Во-первых,

нужно как-то измерить кибернетические и геополитические риски для разных участков маршрута. Это может означать анализ уязвимостей IT-систем по пути следования, проверку киберзащиты партнеров, отслеживание новостей о ситуации в регионах транзита, изучение прошлых инцидентов [1, 2]. Оценивать риски можно по-разному: с помощью экспертов, проигрывая разные сценарии, разрабатывая специальные индексы опасности. Во-вторых, эти оценки риска нужно встроить в программы, которые рассчитывают маршруты. Можно, например, добавить в расчет штрафы за выбор опасного участка или использовать методы, которые помогают найти баланс между ценой, скоростью и безопасностью.

Технологии здесь играют важную роль. Системы, которые в реальном времени следят за обстановкой в мире и киберугрозами, анализируя новости, отчеты и данные с датчиков, могут давать актуальную информацию для оценки рисков [3]. Аналитические программы с использованием машинного обучения могут предсказывать вероятность тех или иных проблем на разных участках пути. Современные системы управления транспортом должны уметь быстро перестраивать маршрут, если где-то резко возрастает опасность. Рассматриваются и такие технологии, как блокчейн – он может помочь сделать обмен данными в цепи поставок более прозрачным и защищенным от подделки [4].

Но одних технологий мало. Чтобы оптимизация маршрутов с учетом новых угроз работала, нужны изменения в самой компании. Логисты, IT-безопасники, риск-менеджеры, аналитики – все должны работать вместе, обмениваться информацией. Очень важно иметь четкие планы на случай чрезвычайных ситуаций: что делать, если основной маршрут перекрыт, как быстро перейти на запасной вариант [5]. Нельзя забывать и о людях: обучение сотрудников правилам кибербезопасности по-прежнему остается одним из лучших способов снизить риски [1]. Наконец, стратегия диверсификации – когда компания не складывает все яйца в одну корзину, а использует несколько разных маршрутов и работает с несколькими перевозчиками – помогает легче пережить локальные сбои **[Ошибка! Источник ссылки не найден.]**.

Таким образом, оптимизация маршрутов сегодня – это уже не просто расчет самой дешевой дороги. Это сложный процесс управления рисками в мире, полном неопределенности. Учет киберугроз и геополитики при планировании перевозок – это не прихоть, а жизненная необходимость для любой компании, которая хочет, чтобы ее поставки были надежными, а бизнес – устойчивым. Для этого нужны новые методы оценки рисков, умные аналитические инструменты, гибкие технологии для контроля и реагирования, а также серьезные изменения в том, как организована работа и как сотрудники относятся к вопросам безопасности. Те компании, которые смогут перестроить свою логистику под новую реальность, не только избегут больших потерь, но и получат преимущество перед конкурентами за счет большей надежности и предсказуемости поставок. Нужно продолжать искать более точные способы измерения этих сложных рисков и разрабатывать умные алгоритмы, которые помогут находить лучшие маршруты в этом непростом и постоянно меняющемся мире.

Список источников

1. Кибербезопасность в логистике: защита цифровых процессов от современных угроз // Verum Logistics. 2023. URL:

<https://verumlogistics.ru/novosti/kiberbezopasnost-v-logistike-zawita-cifrovyyh-processov-ot-sovremennyh-ugroz/> (дата обращения: 16.04.2025).

2. Обеспечение кибербезопасности поддержки жизненного цикла изделий на транспорте // Данные экономики транспорта. URL: <https://data.tedo.ru/technology/cybersecurity-support.pdf> (дата обращения: 16.04.2025).

3. Как управлять киберрисками в цепочке поставок // Alibaba Reads RU. 2023. URL: <https://reads.alibaba.com/ru/how-to-manage-cyber-risks-in-the-supply-chain/> (дата обращения: 16.04.2025).

4. Кибербезопасность в логистике: как защитить данные // Logistic Tools. 2024. URL: <https://logistic.tools/ru/blog/kiberbezopasnost-v-logistike-kak-zashitit-dannie> (дата обращения: 16.04.2025).

5. Влияние геополитической ситуации на логистические цепочки международных грузоперевозок // D2D Logistics. 2023. URL: <https://d2d-l.com/vliyanie-geopoliticheskoy-situacii-na-logisticheskie-cepochki-mezhdunarodnyh-gruzoperevozok/> (дата обращения: 16.04.2025).

Статья поступила в редакцию 22.04.2025; принята к публикации 10.05.2025

Информация об авторах

Березкин Ф.Е. – студент кафедры «Системы информационной безопасности», направление подготовки 10.05.03 – Информационная безопасность автоматизированных систем ФГБОУ ВО «БГТУ».

Бобков К.В. – студент кафедры «Системы информационной безопасности», направление подготовки 10.05.03 – Информационная безопасность автоматизированных систем ФГБОУ ВО «БГТУ».

Шапенская А.М. – ассистент кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Голембиовский М.М. – ассистент кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Вклад авторов

Березкин Ф.Е. – идея, сбор материала, обработка материала, частичное написание статьи (25%).

Бобков К.В. – идея, сбор материала, обработка материала, частичное написание статьи (25%).

Шапенская А.М. – написание статьи, научное редактирование текста (25%).

Голембиовский М.М. – сбор материала, написание статьи (25%).

Конфликт интересов отсутствует.

Научная статья

УДК 004.056:316.77

Telegram-каналы в распространении деструктивных идеологий: методы блокировки и альтернативы

Федор Евгеньевич Березкин ^{1✉}, Кирилл Викторович Бобков ²,
Алина Михайловна Шапенская ³, Артур Игоревич Банников ⁴

^{1, 2, 3, 4}Брянский государственный технический университет, Брянск, Россия

¹fedor.berezkin32@yandex.ru [✉], <https://orcid.org/0009-0002-0105-7335>

²kirillbobjkof2004@yandex.ru, <https://orcid.org/0009-0000-6467-1514>

^{3, 4}alinashapenskaya@yandex.ru, <https://orcid.org/0009-0007-8434-5848>

Аннотация. В данной статье рассматривается масштабная проблема использования Telegram-каналов как платформы для распространения деструктивных идеологий и экстремистских взглядов, особенно среди молодежи. Анализируются ключевые механизмы функционирования таких каналов, методы блокировки деструктивного контента, правовые и технические трудности при реализации ограничительных мер. Особое внимание уделяется разработке альтернативных, превентивных мер, включающих цифровую гигиену, развитие критического мышления и институциональное сотрудничество. Отмечается необходимость интеграции технических, нормативных и просветительских подходов для эффективного противодействия данной угрозе.

Ключевые слова: Telegram, деструктивные идеологии, цифровая безопасность, блокировка каналов, медиаграмотность, молодежь, экстремизм.

Для цитирования: Березкин Ф.Е., Бобков К.В., Шапенская А.М., Банников А.И. Telegram-каналы в распространении деструктивных идеологий: методы блокировки и альтернативы // Актуальные проблемы кибербезопасности и их решения. Противодействие экстремизму и терроризму в информационной молодежной среде: сборник докладов I межрегиональной научно-практической конференции. – Брянск: БГТУ, 2025. – С. 39 – 42.

Сегодняшний мир тесно связан с интернетом, где мессенджеры вроде Telegram играют огромную роль в общении и распространении информации. Популярность Telegram обусловлена его удобством, возможностью создавать большие публичные каналы и группы, а также функциями, обеспечивающими приватность, такими как секретные чаты и определенная анонимность [1]. Однако эти же черты делают платформу привлекательной для распространения опасных идей, включая экстремизм, ненависть и призывы к незаконным действиям [2]. Использование Telegram-каналов в таких целях создает серьезную проблему, требующую анализа методов распространения вредного контента и поиска эффективных способов противодействия, которые бы не нарушали права пользователей на частную жизнь и свободу слова.

Привлекательность Telegram для распространителей деструктивного контента объясняется его функционалом и репутацией. Каналы позволяют вещать на огромную аудиторию без прямого контакта [3], а большие группы служат площадкой для обсуждений и вербовки. Сложившееся мнение о том, что Telegram

менее подвержен цензуре по сравнению с другими крупными соцсетями, также играет роль [4]. Хотя платформа заявляет о борьбе с незаконными материалами, на практике модерация часто не успевает за потоком информации или оказывается менее строгой. Возможность анонимной регистрации и использование шифрования в личной переписке [5] дополнительно снижают риски для тех, кто занимается противоправной деятельностью.

Распространение вредоносных идеологий в Telegram происходит через различные механизмы. Каналы публикуют пропагандистские материалы, часто рассчитанные на эмоциональный отклик и вирусное распространение. Информация расходуется через репосты, обмен ссылками и целые сети связанных каналов и групп, создавая информационные пузыри. Вербовка и координация действий, вплоть до планирования насилия, могут происходить в закрытых группах или зашифрованных чатах, что затрудняет их обнаружение [6]. При этом заблокированные каналы легко возрождаются под новыми именами, быстро восстанавливая аудиторию, что делает борьбу с ними похожей на битву с гидрой.

Основным методом противодействия является блокировка каналов и групп, нарушающих правила или законы, часто по жалобам пользователей или запросам властей [1]. Однако эффективность таких мер ограничена. Заблокированные сообщества быстро появляются снова, выявить весь деструктивный контент сложно из-за его объемов и маскировки, а международный статус Telegram создает юридические трудности из-за различий в законодательствах стран [2]. Локальные меры, вроде запрета стикеров [3], носят скорее символический характер. Помимо блокировок, могут применяться и другие ограничения, но их применение не всегда прозрачно. Ключевой проблемой остается конфликт между необходимостью контроля контента и защитой приватности пользователей, особенно в свете использования шифрования [4, 5] и давления со стороны правительств, на которое Telegram традиционно отвечает защитой данных пользователей [6].

Ограниченность существующих методов требует поиска дополнительных решений. Развитие искусственного интеллекта для выявления опасного контента перспективно, но сталкивается с техническими сложностями, вопросами точности и проблемой шифрования. Важным направлением является усиление сотрудничества между платформой, правоохранительными органами и исследователями для обмена информацией и выработки общих стратегий, но это требует четких правовых рамок. Не менее значима работа с самими пользователями: повышение медиаграмотности помогает людям распознавать манипуляции и пропаганду, а создание и продвижение позитивных контрнарративов может предложить альтернативу деструктивным идеям. Формирование общественного иммунитета к таким идеологиям – долгосрочная, но потенциально более устойчивая стратегия.

Рассмотрение альтернативных платформ, таких как Signal, показывает, что они также делают упор на безопасность и шифрование [1, 2], но их структура часто больше ориентирована на личное общение, чем на массовое вещание. Это

может делать их менее удобными для широкой пропаганды, но не исключает использования для координации в закрытых группах. Проблема использования коммуникационных технологий во вред не привязана к одной платформе, а скорее отражает общие возможности и риски современных сетей, позволяющих быстро и анонимно распространять информацию. Каждая платформа ищет свой баланс между функциональностью, приватностью и безопасностью [3, 4].

Таким образом, использование Telegram для распространения деструктивных идей – сложная проблема, связанная с особенностями самой платформы. Стандартные методы блокировки эффективны лишь отчасти, сталкиваясь с техническими и юридическими трудностями, а также фундаментальным противоречием между безопасностью и правами пользователей. Решение требует комплексного подхода, включающего технологические улучшения, сотрудничество различных структур, образовательные меры для повышения медиаграмотности и активное продвижение альтернативного контента. Простое удаление контента не искореняет проблему, а лишь может загнать ее глубже. Поиск рабочего баланса между контролем, свободой и приватностью остается ключевой задачей для Telegram и всего цифрового общества в борьбе с онлайн-угрозами.

Список источников

1. Альтернативы Signal и Telegram: какой безопасный мессенджер использовать? // Hi-Tech Mail.ru. URL: <https://hi-tech.mail.ru/review/114266-alternativy-signal-i-telegram-kakoj-bezopasnyj-messendzher-ispolzovat/> (дата обращения: 10.04.2025).
2. Альтернативы Signal и Telegram: какой безопасный мессенджер использовать? // Hi-Tech Mail.ru. URL: <https://hi-tech.mail.ru/review/114266-alternativy-signal-i-telegram-kakoj-bezopasnyj-messendzher-ispolzovat/> (дата обращения: 10.04.2025).
3. Telegram начал блокировать каналы, связанные с ЧВК «Вагнер» // SecurityLab.ru. 24.06.2023. URL: <https://www.securitylab.ru/news/554869.php> (дата обращения: 10.04.2025).
4. Why Extremists, Criminal Activity Thrive on Telegram Chat App // Bloomberg (via Translated.turbopages.org). August 26, 2024. URL: https://translated.turbopages.org/proxy_u/en-ru.ru.964c12f7-68015233-5fa73f08-74722d776562/https://www.bloomberg.com/news/articles/2024-08-26/telegram-why-extremists-criminal-activity-thrive-on-chat-app (дата обращения: 10.04.2025).
5. Новые ограничения в Telegram: в России запрещены некоторые стикеры // VC.ru. 14.06.2024. URL: <https://vc.ru/id4221622/1865333-novye-ogranicheniya-v-telegram-v-rossii-zapresheny-nekotorye-stikery> (дата обращения: 10.04.2025).
6. Telegram каналы. Самый подробный разбор // Dzen.ru. 21.02.2024. URL: <https://dzen.ru/a/ZebTAOkqLBLUsiws> (дата обращения: 10.04.2025).

Статья поступила в редакцию 22.04.2025; принята к публикации 10.05.2025

Информация об авторах

Березкин Ф.Е. – студент кафедры «Системы информационной безопасности», направление подготовки 10.05.03 – Информационная безопасность автоматизированных систем ФГБОУ ВО «БГТУ».

Бобков К.В. – студент кафедры «Системы информационной безопасности», направление подготовки 10.05.03 – Информационная безопасность автоматизированных систем» ФГБОУ ВО «БГТУ».

Шапенская А.М. – ассистент кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Банников А.И. – ассистент кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Вклад авторов

Березкин Ф.Е. – идея, аналитика, доработка, структурирование и редактирование текста статьи (25%).

Бобков К.В. – идея, сбор материала, аналитическая часть, написание чернового варианта статьи (25%).

Шапенская А.М. – написание статьи, научное редактирование текста (25%).

Банников А.И. - сбор материала, написание статьи (25%).

Конфликт интересов отсутствует.

Научная статья

УДК 004.056

Эволюция атак программ-вымогателей (Ransomware): от превентивных мер к стратегиям киберустойчивости и восстановления

Федор Евгеньевич Березкин ^{1✉}, Алина Михайловна Шапенская ²,
Алексей Владимирович Евдокимов ³, Кирилл Евгеньевич Шинаков ⁴

^{1, 2, 3}Брянский государственный технический университет, Брянск, Россия

¹fedor.berezkin32@yandex.ru [✉], <https://orcid.org/0009-0002-0105-7335>

²alinashapenskaya@yandex.ru, <https://orcid.org/0009-0007-8434-5848>

^{3,4}alekseievdokimov05@gmail.com, <https://orcid.org/0009-0004-4331-1279>

Аннотация. В статье рассматривается эволюция атак программ-вымогателей (ransomware), от первоначальных блокировщиков до современных многоэтапных угроз, включающих кражу конфиденциальных данных и тактики двойного вымогательства. Анализируется недостаточность традиционных превентивных мер и обосновывается необходимость перехода к комплексным стратегиям киберустойчивости, которые интегрируют предотвращение, обнаружение, реагирование и надежные планы восстановления для минимизации ущерба и обеспечения непрерывности деятельности организаций.

Ключевые слова: программы-вымогатели, ransomware, эволюция атак, кибербезопасность, киберустойчивость.

Для цитирования: Березкин Ф.Е., Шапенская А.М., Евдокимов А.В., Шинаков К.Е. Эволюция атак программ-вымогателей (Ransomware): от превентивных мер к стратегиям киберустойчивости и восстановления // Актуальные проблемы кибербезопасности и их решения. Противодействие экстремизму и терроризму в информационной молодежной среде: сборник докладов I межрегиональной научно-практической конференции. – Брянск: БГТУ, 2025. – С. 43 – 47.

Программы-вымогатели, известные также как ransomware, представляют собой одну из наиболее значительных и динамично развивающихся угроз в современном киберпространстве [1]. Их воздействие на организации и частных лиц может быть разрушительным, приводя к значительным финансовым потерям, остановке операционной деятельности и утечке конфиденциальной информации [2]. Изначально воспринимаемые как относительно простая форма вредоносного программного обеспечения, блокирующего доступ к файлам с требованием выкупа, программы-вымогатели претерпели существенную эволюцию. Эта трансформация затронула как технические аспекты их реализации и распространения, так и саму бизнес-модель злоумышленников, что потребовало кардинального пересмотра стратегий защиты: от первоначального акцента на превентивные меры к комплексным подходам, включающим киберустойчивость и эффективное восстановление после инцидентов.

Исторически, первые образцы программ-вымогателей появились еще в конце 1980-х годов, но их массовое распространение и усложнение началось зна-

чительно позже, с развитием интернета и криптовалют, которые обеспечили злоумышленникам удобный и относительно анонимный способ получения выкупа [3]. Ранние версии ransomware часто использовали простые методы блокировки системы или слабое шифрование, которое иногда удавалось обойти без уплаты выкупа [4]. Основными векторами распространения служили фишинговые письма с вредоносными вложениями или ссылки на зараженные веб-сайты [5]. На этом этапе основное внимание защитных решений было сосредоточено на предотвращении проникновения вредоносного ПО в систему с помощью антивирусных программ, спам-фильтров и базовых правил сетевой безопасности. Предполагалось, что надежная периметральная защита и своевременное обновление антивирусных баз способны эффективно противостоять угрозе.

Однако ситуация начала кардинально меняться с появлением криптовымогателей, использующих стойкие асимметричные алгоритмы шифрования. Такие программы, как CryptoLocker и его многочисленные последователи, сделали восстановление зашифрованных файлов без ключа дешифровки практически невозможным [6]. Это значительно повысило эффективность атак и финансовую мотивацию злоумышленников. Параллельно происходило усложнение векторов атак: на смену простому спаму пришли целевые фишинговые кампании (spear-phishing), эксплуатация уязвимостей в программном обеспечении (как в случае с WannaCry, использовавшим уязвимость EternalBlue) [2, 3], атаки через незащищенный протокол удаленного рабочего стола (RDP) [1] и компрометация учетных данных. Злоумышленники стали активнее использовать инструменты для горизонтального перемещения внутри скомпрометированной сети, стремясь зашифровать как можно больше критически важных данных и систем.

Следующим значительным этапом эволюции стало появление модели Ransomware-as-a-Service (RaaS) [4]. На подпольных форумах стали доступны готовые наборы инструментов и инфраструктура для проведения атак, что позволило участвовать в них даже лицам без глубоких технических познаний. Операторы RaaS предоставляют вредоносное ПО, платформу для управления атаками и получения выкупов, забирая себе процент от прибыли. Это привело к резкому росту числа атак и их разнообразию, так как разные партнерские группы использовали различные тактики и цели [5]. Превентивные меры, хотя и оставались важными, уже не могли гарантировать стопроцентную защиту от такого потока разнообразных угроз. Стало очевидно, что необходимо готовиться к тому, что атака может оказаться успешной.

Кульминацией этой эволюции стал переход к тактике двойного и даже тройного вымогательства [6]. Осознав, что наличие резервных копий позволяет некоторым жертвам игнорировать требования о выкупе за дешифровку, злоумышленники изменили подход. Теперь перед шифрованием данных они предварительно похищают значительные объемы конфиденциальной информации [1]. Угроза публикации этих данных или их продажи на черном рынке становится дополнительным рычагом давления на жертву, даже если у нее есть возможность восстановить системы из бэкапов. Некоторые группы идут дальше, добавляя тре-

тий элемент шантажа – DDoS-атаки на инфраструктуру жертвы или прямые контакты с ее клиентами, партнерами и регуляторами для усиления репутационного ущерба [1]. Современные атаки ransomware часто носят многоэтапный характер, начинаясь с компрометации учетных данных или фишинга, продолжаясь разведкой внутри сети, кражей данных и завершаясь шифрованием и выдвижением требований [4, 6]. Злоумышленники целенаправленно ищут и пытаются уничтожить резервные копии, чтобы лишить жертву возможности восстановления [4].

Эта сложная и многогранная природа современных атак программ-вымогателей демонстрирует ограниченность подхода, основанного исключительно на предотвращении. Хотя превентивные меры, такие как использование надежных антивирусных решений, межсетевых экранов нового поколения (NGFW), систем предотвращения вторжений (IPS), регулярное обновление ПО, обучение сотрудников основам кибергигиены и защита электронной почты, остаются абсолютно необходимыми, они больше не являются панацеей [4, 6]. Злоумышленники постоянно ищут и находят новые уязвимости, применяют изощренные методы социальной инженерии и используют легитимные инструменты для маскировки своей активности [1]. Принцип "неизбежности взлома" (assume breach) становится все более актуальным.

В этих условиях на первый план выходит концепция киберустойчивости (Cyber Resilience). Киберустойчивость подразумевает способность организации не только предотвращать атаки, но и эффективно реагировать на них, минимизировать ущерб и быстро восстанавливать нормальную операционную деятельность [4]. Это требует комплексного подхода, охватывающего людей, процессы и технологии. Ключевым элементом стратегии киберустойчивости в контексте ransomware является надежное резервное копирование. Необходимо придерживаться правила "3-2-1" (три копии данных на двух разных носителях, одна из которых хранится вне основной площадки) и использовать технологии, обеспечивающие неизменяемость (immutability) или воздушный зазор (air gap) для резервных копий, чтобы защитить их от шифрования или удаления злоумышленниками [4, 6]. Регулярное тестирование процедур восстановления из бэкапов не менее важно, чем само их создание.

Другим важным аспектом является сегментация сети. Разделение корпоративной сети на изолированные сегменты с контролем трафика между ними может существенно ограничить возможности злоумышленников по горизонтальному перемещению и распространению ransomware в случае компрометации одного из сегментов [4]. Управление идентификацией и доступом (IAM), включая использование многофакторной аутентификации (MFA) для всех критически важных систем и учетных записей, особенно привилегированных, значительно усложняет компрометацию [6]. Принцип наименьших привилегий должен строго соблюдаться, чтобы пользователи и системы имели доступ только к тем ресурсам, которые им действительно необходимы для работы.

Технологии обнаружения и реагирования играют критическую роль в киберустойчивости. Решения класса Endpoint Detection and Response (EDR) и Extended Detection and Response (XDR) обеспечивают более глубокую видимость

происходящего на конечных точках и в сети, позволяя выявлять подозрительную активность, характерную для атак ransomware, на ранних стадиях и автоматизировать часть ответных действий [1, 4]. Мониторинг событий безопасности с использованием систем SIEM (Security Information and Event Management) помогает коррелировать события из различных источников и выявлять сложные атаки.

Наконец, неотъемлемой частью стратегии киберустойчивости является наличие проработанного и регулярно тестируемого плана реагирования на инциденты (Incident Response Plan, IRP) [4]. Этот план должен четко определять роли и обязанности сотрудников, процедуры изоляции зараженных систем, анализа инцидента, коммуникации с заинтересованными сторонами и шаги по восстановлению. Решение о выплате выкупа является сложным и должно приниматься взвешенно, учитывая юридические аспекты, репутационные риски и отсутствие гарантий получения рабочего дешифратора или непубликации украденных данных [2, 5]. После инцидента необходимо провести тщательный анализ для выявления причин проникновения и уязвимостей, чтобы предотвратить повторные атаки.

В заключение, эволюция программ-вымогателей от простых блокировщиков до сложных многоэтапных атак с кражей данных и многократным шантажом потребовала фундаментального сдвига в стратегиях киберзащиты.

Список источников

1. Атаки программ-вымогателей в 2022 году: эволюция методов и техник на примере Conti // Habr.com. 16.06.2022. URL: <https://habr.com/ru/companies/first/articles/670026/> (дата обращения: 16.04.2025).
2. Что такое атаки программ-вымогателей и их разновидности // Kaspersky.ru. URL: <https://www.kaspersky.ru/resource-center/threats/ransomware-attacks-and-types> (дата обращения: 16.04.2025).
3. Программа-вымогатель // Википедия. URL: <https://ru.wikipedia.org/wiki/Программа-вымогатель> (дата обращения: 16.04.2025).
4. Как эффективно защититься от программ-вымогателей // Anti-Malware.ru. 19.10.2021. URL: https://www.anti-malware.ru/analytics/Technology_Analysis/How-to-effectively-defend-against-ransomware (дата обращения: 16.04.2025).
5. Вирусы-вымогатели (шифровальщики) Ransomware // TAdviser.ru. URL: [https://www.tadviser.ru/index.php/Статья:Вирусы-вымогатели_\(шифровальщики\)_Ransomware](https://www.tadviser.ru/index.php/Статья:Вирусы-вымогатели_(шифровальщики)_Ransomware) (дата обращения: 16.04.2025).
6. Что такое программа-вымогатель? // Keepersecurity.com. URL: https://www.keepersecurity.com/ru_RU/threats/ransomware.html (дата обращения: 16.04.2025).

Статья поступила в редакцию 22.04.2025; принята к публикации 10.05.2025

Информация об авторах

Березкин Ф.Е. – студент кафедры «Системы информационной безопасности», направление подготовки 10.05.03 – Информационная безопасность автоматизированных систем ФГБОУ ВО «БГТУ».

Шапенская А.М. – ассистент кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Евдокимов А.В. – студент кафедры «Системы информационной безопасности», направление подготовки 10.05.03 – Информационная безопасность автоматизированных систем ФГБОУ ВО «БГТУ».

Шинаков К.Е. – к.т.н., доцент кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Вклад авторов

Березкин Ф.Е. – идея, сбор материала, обработка материала, частичное написание статьи (25%).

Шапенская А.М. – написание статьи, научное редактирование текста (25%).

Евдокимов А.В. – идея, сбор материала, обработка материала, частичное написание статьи (25%).

Шинаков К.Е. – сбор материала, обработка материала, частичное написание статьи (25%).

Конфликт интересов отсутствует.

Научная статья
УДК 004.056

Исследование применения модели Cyber-Kill Chain

Александр Александрович Бузылев^{1✉}, Владислав Павлович Киселёв²,
Дмитрий Андреевич Лысов³, Алексей Петрович Горлов⁴

^{1,2,3,4}Брянский государственный технический университет, Брянск, Россия

¹buzylev2018@yandex.ru✉, <https://orcid.org/0009-0005-3301-7006>

²vkiselev1213@gmail.com, <https://orcid.org/0009-0002-5845-1149>

³lysovdmitriia@gmail.com, <https://orcid.org/0009-0003-9666-7191>

⁴apgorlov@gmail.com, <https://orcid.org/0009-0003-3100-3466>

Аннотация. В статье проведено исследование применения модели Cyber-Kill Chain.

Ключевые слова: разведка, информация, атака, система, уязвимость, злоумышленник.

Для цитирования: Бузылев А.А., Киселёв В.П., Лысов Д.А., Горлов А.П. Исследование применения модели Cyber-Kill Chain // Актуальные проблемы кибербезопасности. Противодействие экстремизму и терроризму в информационной молодежной среде: сборник докладов I межрегиональной научно-практической конференции. – Брянск: БГТУ, 2025. – С. 48 – 51.

В современном мире в условиях стремительного развития цифровых технологий обеспечение безопасности информационных систем является критически важной задачей.

Эта необходимость обусловлена тем, что злоумышленники применяют системный подход при организации атак, разрабатывают многоступенчатые схемы для достижения своих целей.

Для построения проактивной защиты применяется модель Cyber-Kill Chain. Данная модель позволяет проводить системный анализ кибератак и своевременно на них реагировать.

Модель разбивает действия злоумышленника на этапы. Понимая особенности каждого этапа, специалисты по обеспечению безопасности могут:

- выявлять атаку на ранних этапах и своевременно на неё реагировать;
- прогнозировать следующие шаги злоумышленника;
- сократить время на реагирование, тем самым минимизировать убытки.

Особое значение в этой модели имеет начальный этап – разведка (Reconnaissance), который зачастую определяет успешность атаки в целом.

Разведка – это сбор и систематизация информации о целевой системе для поиска уязвимых точек входа. Существует два типа разведки: пассивная и активная.

Пассивная разведка использует методы сбора информации без непосредственного взаимодействия с целевой системой. К таким методам относятся:

- сбор информации о домене;

- поиск информации из открытых источников о сотрудниках и организации;
- поиск информации в закрытых источниках.

Активная разведка предполагает прямое взаимодействие с целевой системой. К методам активной разведки относятся:

- сканирование хостов на наличие открытых портов, идентификация версий служб, поиск уязвимостей.
- поиск поддоменов и скрытых директорий при помощи инструментов для перебора;
- проверка сведений о пользователях активными методами (наличие действительных учётных записей).

Следующим этапом является вооружение (Weaponization). На данном этапе злоумышленник создаёт, приобретает или компрометирует ресурсы, которые будут использованы для проведения и поддержки атаки.

В качестве ресурсов выступают: инфраструктура (домены, серверы, ботнет и др.), учётные записи и вредоносное программное обеспечение (например, эксплойты для уязвимостей, бэкдоры).

Стоит отметить, что первые два этапа могут полностью происходить без взаимодействия с целевой системой, тем самым не оставляют никаких следов и определить атаку крайне сложно.

Важным этапом в реализации атаки является доставка (Delivery). На данном этапе происходит передача вредоносного контента жертве.

Основная цель данного этапа – передать вредоносное программное обеспечение жертве и проникнуть в целевую систему. Основные техники реализации атаки:

- целевой фишинг;
- социальная инженерия;
- компрометация уязвимых служб.

На этапе эксплуатации (Exploitation) злоумышленник использует уязвимости в оборудовании для выполнения кода. Основная цель злоумышленника – заражение целевой системы.

На данном этапе злоумышленник использует техники для выполнения кода в скомпрометированной системе. Запуск различных эксплойтов помогает злоумышленнику закрепиться в системе и расширить доступ в сети, перемещаясь внутри периметра.

Злоумышленник может использовать легитимные процессы системы для противодействия обнаружению.

На этапе установки (Installation) злоумышленник использует техники для обеспечения постоянного присутствия в атакуемой системе.

Злоумышленнику необходимо быть уверенным в сохранности доступа к атакуемой системе, например, после перезапуска системы или смены учётных данных (изменение данных, деактивация учётных записей). Таким образом он сможет в любое время контролировать скомпрометированную систему.

Методы включают в себя любые действия, которые позволяют закрепиться в целевой системе (например, автозапуск кода при загрузке или входе в систему, использование внешних служб удалённого доступа).

Переломным этапом является «Командование и контроль» (Command & Control). На данном этапе злоумышленник начинает контролировать активы жертвы, что позволяет управлять системой и собирать данные.

Используемые методы для сбора данных: снимки экрана, нажатия клавиш, сбор критического контента. Обычно злоумышленники имитируют обычное поведение трафика, чтобы скрыть своё присутствие.

Завершающим этапом в модели Cyber-Kill Chain являются действия по достижению цели (Actions on Objectives). На данном этапе злоумышленник реализует конечную цель атаки:

- манипуляция данными (сбор, передача, шифрование и удаление);
- прерывание работы системы (перезагрузка системы, остановка служб, прекращение доступа к учётным записям, сетевые отказы в обслуживании);
- уничтожение системы (повреждение прошивки, удаление базы данных).

Затем происходит мероприятия по выявлению других целей с целью перемещения внутри периметра. Злоумышленник пытается проникнуть в другие сегменты сети.

Важной особенностью модели Cyber-Kill Chain является то, что она циклична, а не линейна. Для расширения внутри защитного периметра злоумышленнику необходимо повторить элементы цепочки, осуществляя дополнительной разведку и применяя новые методы для компрометации дополнительных целей.

В заключении стоит отметить, что модель Cyber-Kill Chain предлагает системный подход к противодействию атакам, позволяя анализировать действия злоумышленников на каждом этапе.

Внедрение данной модели позволяет не только снижать риски успешных кибератак, но и формировать устойчивую стратегию кибербезопасности в условиях постоянно меняющегося ландшафта угроз.

Список источников

1. The Cyber Kill Chain. 2025. URL: <https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html>.
2. Матрица MITRE ATT&CK. 2025. URL: <https://mitre.ptsecurity.com>.
3. OWASP Web Security Testing Guide. 2020. URL: <https://owasp.org/www-project-web-security-testing-guide/stable>.
4. Что такое Cyber-Kill Chain и почему ее надо учитывать в стратегии защиты? 2017. URL: <https://habr.com/ru/company/panda/blog/327488>.

Статья поступила в редакцию 19.04.2025; принята к публикации 10.05.2025

Информация об авторах

Бузылев А.А. – студент кафедры «Системы информационной безопасности», направление подготовки 10.04.01 – Информационная безопасность ФГБОУ ВО «БГТУ».

Киселёв В.П. – студент кафедры «Системы информационной безопасности», направление подготовки 10.03.01 – Информационная безопасность ФГБОУ ВО «БГТУ».

Лысов Д.А. – старший преподаватель кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Горлов А.П. – к.т.н., доцент кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Вклад авторов

Бузылев А.А. – идея, сбор материала, обработка материала, частичное написание статьи (60%).

Киселёв В.П. – сбор материала, обработка материала, частичное написание статьи (10%).

Лысов Д.А. – написание статьи, научное редактирование текста (20%).

Горлов А.П. – написание статьи, научное редактирование текста (10%).

Конфликт интересов отсутствует.

Научная статья
УДК 004.056

Управление рисками безопасности при реализации аутентификации и авторизации в Application Programming Interface

Александр Александрович Бузылев^{1✉}, Владислав Павлович Киселёв²,
Дмитрий Андреевич Лысов³, Алексей Петрович Горлов⁴

^{1,2,3,4}Брянский государственный технический университет, Брянск, Россия

¹buzylev2018@yandex.ru✉, <https://orcid.org/0009-0005-3301-7006>

²vkiselev1213@gmail.com, <https://orcid.org/0009-0002-5845-1149>

³lysovdmitriia@gmail.com, <https://orcid.org/0009-0003-9666-7191>

⁴apgorlov@gmail.com, <https://orcid.org/0009-0003-3100-3466>

Аннотация. В статье разработаны рекомендации по минимизации рисков безопасности, связанных с управлением доступом в API.

Ключевые слова: API, аутентификация, авторизация, конечная точка, эндпоинт, злоумышленник.

Для цитирования: Бузылев А.А., Киселёв В.П., Лысов Д.А., Горлов А.П. Управление рисками безопасности при реализации аутентификации и авторизации в Application Programming Interface // Актуальные проблемы кибербезопасности. Противодействие экстремизму и терроризму в информационной молодежной среде: сборник докладов I межрегиональной научно-практической конференции. – Брянск: БГТУ, 2025. – С. 52 – 56.

Application Programming Interface (API) – набор способов и правил, по которым различные сервисы общаются между собой и обмениваются данными.

API играют важную роль в построении гибких, масштабируемых и интегрируемых решений.

Однако скорость внедрения новых решений на базе API значительно быстрее реализации соответствующих мер защиты, что создаёт существенные риски для информационной безопасности.

Рейтинг OWASP API Security Top 10 – является одним из стандартов в области защиты API. Он предназначен для повышения компетенций в сфере информационной безопасности тех, кто занимается разработкой и поддержкой API (например, разработчиков, дизайнеров, архитекторов).

Особое внимание в стандарте уделяется вопросам, связанным с управлением доступом, поскольку нарушения в этой области входят в список наиболее критичных уязвимостей.

К рискам безопасности, связанным с управлением доступа, согласно OWASP API Security Top 10 относятся:

- API1:2023 – Broken Object Level Authorization;
- API2:2023 – Broken Authentication;
- API3:2023 – Broken Object Property Level Authorization;
- API5:2023 – Broken Function Level Authorization.

API1:2023 – Broken Object Level Authorization (ошибки авторизации на уровне объектов) – возникают, когда серверная часть полностью не отслеживает состояние клиента, а полагается на отправляемые клиентом параметры (например, идентификатор объекта), чтобы принять решение, к какому объекту предоставить доступ. Злоумышленник может манипулировать идентификатором объекта, который отправляется в запросе для получения конфиденциальной информации.

Пример уязвимости: на маркетплейсе доступ к заказам пользователя реализован через следующий запрос (рис. 1).



Рис. 1. Запрос для доступа к заказам

Если заказ № 999 принадлежит другому пользователю, но сервер не проверяет владельца, злоумышленник может получить доступ ко всем заказам, перебрав значения поля `order_id`.

Рекомендации по минимизации рисков:

- внедрение механизмов авторизации в соответствии с политиками разграничения доступа.
- использование механизмов авторизации для проверки, что пользователь имеет право доступа к объекту;
- использование уникальных значений вместо последовательных (например, замена ID на GUID).

API2:2023 – Broken Authentication (ошибки аутентификации) – возникают, если службы не обеспечивают должный уровень безопасности при передаче учётных данных и проверки подлинности. Атакующий может попытаться подделать данные для аутентификации и получить несанкционированный доступ.

Пример уязвимости: для смены адреса электронной почты, связанного с учётной записью, пользователь должен отправить следующий запрос в API (рис. 2).



Рис. 2. Запрос на обновление данных

Поскольку API не требует от пользователя подтверждения личности, злоумышленник после перехвата токена аутентификации может получить доступ к учётной записи жертвы, обновить адрес электронной почты и сменить пароль.

Рекомендации по минимизации рисков:

- требование повторной аутентификации для важных операций (например, смена почты/номера телефона пользователя);
- внедрение механизмов 2FA, при наличии технической возможности;
- внедрение механизмов защиты от атак методом перебора (ограничение запросов в секунду, использование reCAPTCHA и т.д.);
- внедрение механизмов блокировки учётных записей (настройка правил автоматической блокировки);
- внедрение проверки слабых паролей (реализация парольной политики, поиск утечек).

API3:2023 – Broken Object Property Level Authorization (ошибки авторизации на уровне свойств объекта) – возникают, когда конечные точки возвращают данные обо всех свойствах объекта.

Эндпоинт считается уязвимым, если он:

- представляет доступ ко всем свойствам объекта, в том числе к конфиденциальным данным, которые не должны быть доступны даже для чтения;
- позволяет добавлять, изменять или удалять значения свойств объекта, которые не должны быть доступны.

Пример уязвимости: видеохостинг применяет строгую фильтрацию контента и цензуру. Если загруженное видео было заблокировано, пользователь может изменить его описание с помощью следующего запроса (рис. 3).



Рис. 3. Запрос на обновление данных

Нарушитель может воспроизвести легитимный запрос и добавить следующую вредоносную полезную нагрузку (рис. 4).



Рис. 4. Модернизированный запрос

Эндпоинт уязвим, потому что не реализована проверка должен ли пользователь иметь доступ к внутреннему свойству объекта – `blocked`, нарушитель может изменить значение с `true` на `false` и разблокировать заблокированный контент.

Рекомендации по минимизации рисков:

- сведение возвращаемых структур данных к минимуму в соответствии с бизнес-логикой и функциональными требованиями для конечной точки;
- настройка разрешений на изменения только в те свойства объекта, которые должны быть обновлены клиентом;
- проверка доступа пользователя к публикуемым свойствам объекта;
- отказ от использования универсальных методов, таких как `to_json()` и `to_string()`. Выбор конкретных свойств объекта, которые вы хотите вернуть;
- отказ от использования функций, которые автоматически привязывают вводимые клиентом данные к переменным кода, внутренним объектам или свойствам объектов («массовое присваивание»);
- внедрение механизма проверки ответов на основе схемы в качестве дополнительного уровня безопасности.

API5:2023 – Broken Function Level Authorization (Ошибки авторизации на уровне функций) – уязвимость связанная с неправильной авторизацией на уровне функций в API.

Для эксплуатации уязвимости злоумышленнику необходимо отправлять легитимные вызовы API в конечную точку API, к которой у него не должно быть доступа в качестве анонимного пользователя или обычного пользователя без привилегий.

Пример реализации: API содержит эндпоинт, который должен быть доступен только администраторам – `GET /api/admin/v1/users/all`.

Эта конечная точка возвращает сведения обо всех пользователях и не выполняет проверку авторизации на уровне функций.

Злоумышленник изучает структуру API и получает доступ к этой конечной точке, которая раскрывает конфиденциальные сведения.

Такие уязвимости позволяют злоумышленникам получить доступ к функциям, для которых они не предназначены. Административные функции являются ключевыми целями для атак такого типа и могут привести к раскрытию, потере или повреждению данных.

Рекомендации по минимизации рисков:

- настройка механизмов обеспечения безопасности таким образом, чтобы по умолчанию был установлен запрет доступа ко всем функциям, требуя

явного предоставления доступа к каждой функции конкретным ролям пользователей.

- проверка эндпоинтов на наличие ошибок в авторизации на уровне функций, учитывая при этом бизнес-логику приложения.
- проверка наследования административных контроллеров (должны наследоваться от административного абстрактного контроллера, который выполняет проверку авторизации на основе группы/роли пользователя);
- административные функции внутри обычного контроллера должны реализовывать проверку авторизации на основе группы и роли пользователя.

В заключении стоит отметить, что большинство уязвимостей возникает из-за проблем с настройкой механизмов управления доступом (рейтинг OWASP API Security Top 10). Управление доступом в API – критически важный аспект в обеспечении безопасности.

Управление рисками безопасности в API – непрерывный процесс, который включает в себя построение грамотной архитектуры, тестирование безопасности, обучение сотрудников и позволяет защищать инфраструктуру от современных угроз.

Список источников

1. OWASP API Security Top 10. URL: <https://owasp.org/API-Security>.
2. OWASP Web Security Testing Guide. URL: <https://owasp.org/www-project-web-security-testing-guide/stable>.

Статья поступила в редакцию 19.04.2025; принята к публикации 10.05.2025

Информация об авторах

Бузылев А.А. – студент кафедры «Системы информационной безопасности», направление подготовки 10.04.01 – Информационная безопасность ФГБОУ ВО «БГТУ».

Киселёв В.П. – студент кафедры «Системы информационной безопасности», направление подготовки 10.03.01 – Информационная безопасность ФГБОУ ВО «БГТУ».

Лысов Д.А. – старший преподаватель кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Горлов А.П. – к.т.н., доцент кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Вклад авторов

Бузылев А.А. – идея, сбор материала, обработка материала, частичное написание статьи (60%).

Киселёв В.П. – сбор материала, обработка материала, частичное написание статьи (10%).

Лысов Д.А. – написание статьи, научное редактирование текста (20%).

Горлов А.П. – написание статьи, научное редактирование текста (10%).

Конфликт интересов отсутствует.

Научная статья
УДК 378:004

Обнаружение OSINT: современные методы выявления и защиты от разведки по открытым источникам

Денис Дмитриевич Воробьёв ^{1✉}, Алина Михайловна Шапенская ²

^{1,2}Брянский государственный технический университет, Брянск, Россия

¹dan.vorob2012@ya.ru✉, <https://orcid.org/0009-0000-0881-6782>

²alinashapenskaya@yandex.ru, <https://orcid.org/0009-0007-8434-5848>

Аннотация. Статья кратко рассматривает современные методы обнаружения OSINT – разведки по открытым источникам. Описаны техники мониторинга активности, включая анализ логов, использование honeypot-страниц и отслеживание данных в соцсетях, а также практические меры защиты, такие как обучение сотрудников, строгие внутренние политики и сегментация сети. Автор подчеркивает важность своевременного обнаружения цифровых следов для защиты конфиденциальной информации в условиях быстрого роста объема данных.

Ключевые слова: обнаружение OSINT, разведка по открытым источникам, мониторинг информации, защита данных, honeypot, анализ логов, кибербезопасность, скрейпинг.

Для цитирования: Воробьёв Д.Д., Шапенская А.М. Обнаружение OSINT: современные методы выявления и защиты от разведки по открытым источникам // Актуальные проблемы кибербезопасности и их решения. Противодействие экстремизму и терроризму в информационной молодежной среде: сборник докладов I межрегиональной научно-практической конференции. – Брянск: БГТУ, 2025. – С. 57 – 59.

В современном мире информационных технологий мы ежедневно сталкиваемся с огромным потоком данных, который заполняет интернет – от социальных сетей до специализированных порталов. В этом океане открытых источников рождается понятие OSINT (Open Source Intelligence), то есть получение ценной информации из общедоступных ресурсов. Эта статья посвящена анализу того, что такое OSINT, почему его обнаружение становится всё более актуальным и как современные технологии позволяют извлекать нужные данные для принятия управленческих решений.

OSINT представляет собой процесс поиска, сбора и анализа информации из открытых источников, таких как новости, государственные базы данных, социальные сети и многое другое. Значимость OSINT заключается в его способности быстро и эффективно предоставлять полезные данные для различных сфер – от безопасности и бизнеса до государственного управления. Благодаря тому, что объем информации, генерируемой ежедневно, растет в геометрической прогрессии, умение извлекать и обрабатывать эти данные становится критически важным навыком [1].

Согласно отчету Global Market Insights, мировой рынок OSINT превысил 5 млрд долларов США в 2022 году, а прогнозируется, что в период с 2023 по 2032 год его среднегодовой темп роста (CAGR) составит почти 25% [2].

Кроме того, эксперты, опираясь на данные из Википедии по теме OSINT, отмечают, что до 80-90% разведывательной информации для принятия управленческих решений поступает именно из открытых источников.

С увеличением объема доступной информации возникает не только возможность для получения полезных данных, но и риск того, что злоумышленники или конкуренты смогут собрать детальные сведения о вашей компании или личных данных. Обнаружение OSINT – это процесс систематического мониторинга открытых источников с целью выявления случаев, когда кто-либо пытается собрать информацию о вас. Если злоумышленники изучают ваши профили в социальных сетях, обсуждают данные на форумах или извлекают информацию из публичных баз данных, своевременное обнаружение такой активности позволяет оперативно принять меры по защите данных.

Автоматизация процессов сбора и анализа данных, использование специализированных платформ для мониторинга упоминаний и утечек позволяют выявлять скрытые закономерности и тренды, а также предвидеть потенциальные риски. Например, анализ логов серверов может выявить подозрительные паттерны запросов, характерные для скрейпинга (программы или скрипты, используемые для автоматического сбора данных с веб-сайтов) данных [3], а honeypot-страницы – служить ловушкой для автоматизированных OSINT-ботов.

Методы обнаружения активности OSINT и практические меры защиты можно описать следующим образом. Во-первых, проводится мониторинг логов серверов и анализ трафика: при обнаружении необычно высокой частоты запросов с одних и тех же IP-адресов или повторяющихся шаблонов URL становится очевидна активность автоматизированных скрейперов. Во-вторых, используются honeypots – специальные «ловушки» в виде неиндексируемых страниц, запросы к которым позволяют выявить попытки несанкционированного сбора данных [4]. В-третьих, осуществляется постоянный мониторинг публичных упоминаний и утечек: специализированные платформы, такие как сервисы Threat Intelligence, автоматически отслеживают появление конфиденциальной информации в интернете, включая форумы, социальные сети и публичные базы данных. В-четвёртых, анализируется активность в социальных сетях, поскольку многие злоумышленники собирают данные о сотрудниках и структуре организаций через такие ресурсы.

Практические меры защиты включают обучение сотрудников основам информационной безопасности (например, регулярные тренинги о том, какую информацию можно публиковать в соцсетях), разработку и соблюдение внутренних политик, ограничивающих распространение конфиденциальных данных, а также внедрение принципа минимальных привилегий и сегментацию сети, что помогает ограничить ущерб в случае компрометации. Эти меры позволяют оперативно реагировать на обнаруженные угрозы, своевременно блокировать подозрительные действия и минимизировать риски несанкционированного доступа к корпоративной информации [5].

Подводя итог, можно сказать, что в современном мире умение анализировать и обнаруживать активность, связанную с OSINT, становится настоящей

необходимостью. Это как поиск иголки в стоге сена – важно знать, где искать и как отделять ценную информацию от шума. Такой подход помогает своевременно защищать данные и минимизировать риски утечек, что особенно актуально как для бизнеса, так и для личной безопасности.

Список источников

1. habr.com: OSINT: инструменты / Хабр: сайт. URL: <https://habr.com/ru/articles/769690/> (дата обращения: 10.02.2025).
2. gminsights.com: Market research reports, consulting: Global Market Insights Inc. – сайт. URL: <https://www.gminsights.com/> (дата обращения: 12.02.2025).
3. medium.com: Webscraping OSINT – A Beginner's Guide. URL: <https://medium.com/@investigator515/webscraping-osint-a-beginners-guide-bec9ef686dd> (дата обращения: 12.02.2025).
4. medium.com: Honeypot OSINT. URL: <https://medium.com/@ecojumper30/honeypot-osint-3a37c017d9e3> (дата обращения: 15.02.2025).
5. blog.skillfactory.ru: OSINT – что это: поиск по открытым источникам. URL: <https://blog.skillfactory.ru/glossary/osint/> (дата обращения: 18.02.2025).

Статья поступила в редакцию 25.03.2025; принята к публикации 10.05.2025

Информация об авторах

Воробьев Д.Д. – студент кафедры «Системы информационной безопасности», направление подготовки 10.05.03 – Информационная безопасность автоматизированных систем ФГБОУ ВО «БГТУ».

Шапенская А.М. – ассистент кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Вклад авторов

Воробьев Д.Д. – идея, сбор материала, обработка материала, написание статьи (50%).

Шапенская А.М. – научное редактирование текста, частичное написание статьи (50%).

Конфликт интересов отсутствует.

Научная статья
УДК 004.056.55

Обнаружение атак на офисную Wi-Fi-инфраструктуру: анализ угроз и защитных решений

Максим Дмитриевич Грива ¹, Сергей Игоревич Коновалов ^{2✉},
Павел Александрович Аверин ³

^{1,2,3}Брянский государственный технический университет, Брянск, Россия

¹maks.griva.04@mail.ru, <https://orcid.org/0009-0004-8177-360X>

²velvet1way@gmail.com ✉, <https://orcid.org/0009-0008-5867-635X>

³stopnotwont@gmail.com, <https://orcid.org/0009-0003-5074-7217>

Аннотация. Статья посвящена вопросам обеспечения безопасности офисных Wi-Fi-сетей в условиях роста числа киберугроз. Рассматриваются наиболее распространённые типы атак на беспроводной периметр, включая MitM, Evil Twin, Brute Force, Reaver, Deauthentication, Jamming и DDoS на основе Probe Request Flood. Приведён анализ эффективности современных программных средств обнаружения и противодействия атакам, таких как Aircrack-ng, Kismet, Wireshark, NetSpot, Nmap и Wifiphisher. Особое внимание уделяется комплексному подходу к обеспечению безопасности, основанному на регулярном мониторинге, аудите и использовании специализированных инструментов. Сделан вывод о необходимости интеграции технических и организационных мер для повышения устойчивости корпоративной Wi-Fi-инфраструктуры к внешним и внутренним угрозам.

Ключевые слова: Wi-Fi, информационная безопасность, офисный периметр, кибератака, Evil Twin, MitM, Brute Force, Reaver, DDoS, обнаружение угроз, защита беспроводных сетей, сетевой мониторинг, анализ трафика.

Для цитирования: Грива М.Д., Коновалов С.И., Аверин П.А. Обнаружение атак на офисную Wi-Fi-инфраструктуру: анализ угроз и защитных решений // Актуальные проблемы кибербезопасности. Противодействие экстремизму и терроризму в информационной молодежной среде: сборник докладов I межрегиональной научно-практической конференции. – Брянск: БГТУ, 2025. – С. 60 – 63.

Современные офисные сети всё чаще становятся объектами кибератак, что связано с широким распространением технологий беспроводной передачи данных, в частности Wi-Fi. Лёгкость развёртывания, мобильность и доступность Wi-Fi делают его неотъемлемой частью корпоративной инфраструктуры, но при этом создают дополнительные векторы угроз. Особую опасность представляет то, что атаки на Wi-Fi не требуют физического доступа к сети — достаточно находиться в пределах радиуса действия сигнала. В условиях высокой зависимости бизнеса от стабильного доступа к данным и непрерывной работы сетевых сервисов защита периметра офиса становится одной из ключевых задач информационной безопасности. Настоящая статья посвящена анализу существующих методов атак на офисный Wi-Fi-периметр и средств их обнаружения, с целью оценки эффективности существующих подходов и выявления направлений для повышения уровня защищённости беспроводных корпоративных сетей.

Один из наиболее распространённых методов взлома корпоративных Wi-Fi-сетей — атака типа «человек посередине» (Man-in-the-Middle), реализуемая через подмену легитимной точки доступа фальшивой (Evil Twin). Пользователь, не отличающий клонированную сеть от настоящей, подключается к ней, после чего трафик проходит через контролируемое злоумышленником устройство. Это даёт возможность перехватывать передаваемую информацию, внедрять вредоносный код или изменять содержимое сообщений в реальном времени. С технической точки зрения, данная атака часто сопровождается поддельной аутентификацией и принудительным отключением пользователей от основной сети.

Другим вектором угрозы выступают атаки методом перебора пароля (Brute Force), при которых злоумышленник последовательно проверяет возможные комбинации ключей доступа. Их эффективность напрямую зависит от качества и сложности пароля. При успешном подборе обеспечивается полный доступ к инфраструктуре, включая возможность внедрения бэкдоров, изменения конфигурации сети и получения административного контроля.

Опасность представляют также атаки на протокол WPS (Reaver-атаки), использующий восьмизначный PIN-код для подключения устройств. Несмотря на удобство использования WPS, его уязвимость обусловлена отсутствием механизма блокировки после многократных попыток подбора кода. В результате осуществляется прямой доступ к сети даже без знания основного пароля, что делает данную уязвимость особенно критичной в средах с минимальным администрированием.

Принудительное отключение пользователей с помощью деаутентификационных пакетов также используется как способ дальнейшего компрометирования сети. После разрыва соединения устройства автоматически пытаются переподключиться, что открывает возможность для внедрения фальшивых точек доступа или анализа повторных аутентификаций. Этот метод применяется как часть более сложных атак и затрудняет своевременное обнаружение нарушения.

Кроме того, к числу активных атак относится создание помех (jamming), приводящих к потере связи, и перегрузка сетевых устройств за счёт массовых подключений или запросов (DDoS на основе Probe Request Flood). Эти методы не столько направлены на непосредственный захват информации, сколько создают условия для отвлечения внимания, снижения эффективности защиты или принуждения к действиям, повышающим уязвимость сети.

Актуальность проблемы подтверждается данными исследований. По отчёту компании Cisco за 2024 год, около 60% инцидентов корпоративной кибербезопасности были связаны с уязвимостями в беспроводных сетях [1, 2]. Компания Kaspersky Lab также провела исследование, которое показало, что в 2024 году было зафиксировано более 500 тысяч попыток взлома корпоративных Wi-Fi-сетей. Более половины из них были успешными, что привело к утечке конфиденциальных данных и финансовым потерям компаний [3].

В условиях многообразия угроз наиболее эффективным является комплексный подход к обнаружению и предотвращению атак, основанный на использовании специализированных программных решений. Среди наиболее

надёжных и функциональных инструментов можно выделить Aircrack-ng, предназначенный для захвата и анализа трафика, а также тестирования прочности ключей шифрования. Программа позволяет проводить аудит сетевой безопасности и выявлять слабые места в конфигурации. Kismet, в свою очередь, ориентирован на пассивный мониторинг и анализ сетевого трафика, включая возможность выявления скрытых точек доступа и анализа топологии сети. Благодаря модульной архитектуре и поддержке GPS, он предоставляет расширенные функции для картографирования покрытия и локализации угроз [4]. Ещё один важный инструмент — Wireshark, сетевой анализатор, позволяющий фиксировать и исследовать трафик на уровне пакетов. Он применяется для детального анализа подозрительной активности и ретроспективного расследования инцидентов. Для оценки качества сигнала и выявления потенциальных уязвимостей инфраструктуры используется NetSpot, способный наглядно отобразить проблемные зоны покрытия и определить наличие помех. Программа полезна на этапе проектирования и оптимизации сети. Nmap, несмотря на ориентацию на проводные сети, также используется в беспроводных средах благодаря своей гибкости в обнаружении активных устройств, открытых портов и уязвимостей, что делает его незаменимым для проведения первичного аудита. Завершает перечень Wifiphisher — специализированная утилита для имитации фальшивых точек доступа и анализа поведения пользователей в условиях атаки Evil Twin, позволяющая в контролируемой среде оценить реакцию системы безопасности.

Проведённый анализ подтверждает, что угрозы, связанные с беспроводными технологиями, имеют системный характер и требуют постоянного мониторинга. В условиях отсутствия универсальных решений, устойчивость корпоративной Wi-Fi-сети может быть обеспечена только посредством использования набора взаимодополняющих программных средств и внедрения процедур регулярного аудита, анализа трафика и своевременного реагирования на инциденты. Таким образом, для повышения эффективности защиты офисного периметра необходима не просто установка технических решений, а формирование комплексной стратегии информационной безопасности, включающей как технические, так и организационные меры противодействия Wi-Fi-атакам.

Список источников

1. Verizon Data Breach Investigations Report (DBIR) // Verizon Enterprise Solutions : [сайт]. URL: <https://enterprise.verizon.com/resources/reports/dbir/> (дата обращения: 20.02.2025).
2. Mandiant Threat Intelligence Report // Mandiant : [сайт]. URL: <https://www.mandiant.com/resources/threat-intelligence-report> (дата обращения: 22.02.2025).
3. FireEye Cyber Trends Report // FireEye : [сайт]. URL: <https://www.fireeye.com/current-threats/annual-threat-report.html> (дата обращения: 24.02.2025).
4. IBM Cost of a Data Breach Report // IBM Security : [сайт]. URL: <https://www.ibm.com/security/data-breach> (дата обращения: 23.02.2025).

5. Positive Technologies Cloud Security Report // Positive Technologies : [сайт]. URL: <https://www.ptsecurity.com/ru-ru/research/cloud-security-report-2021/> (дата обращения: 21.02.2025).

Статья поступила в редакцию 22.04.2025; принята к публикации 10.05.2025

Информация об авторах

Грива М.Д. – студент кафедры «Системы информационной безопасности», направление подготовки 10.03.01 – Информационная безопасность ФГБОУ ВО «БГТУ»

Коновалов С.И. – студент кафедры «Системы информационной безопасности», специальность 10.05.03 – Информационная безопасность автоматизированных систем, специализация «Безопасность открытых информационных систем» ФГБОУ ВО «БГТУ».

Аверин П.А. – студент кафедры «Системы информационной безопасности», специальность 10.05.03 – Информационная безопасность автоматизированных систем, специализация «Безопасность открытых информационных систем» ФГБОУ ВО «БГТУ».

Вклад авторов

Грива М.Д. – сбор материала, обработка материала, частичное написание статьи (33%).

Коновалов С.И. – идея, сбор материала, обработка материала, написание статьи (34%).

Аверин П.А. – сбор материала, обработка материала, частичное написание статьи (33%).

Научный руководитель

Шапенская А.М. – ассистент кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Конфликт интересов отсутствует.

Научная статья
УДК 004.056.5

О применении стеганографии в различных сферах

Максим Леонидович Гулак

Брянский государственный технический университет, Брянск, Россия
gml13@yandex.ru, <http://orcid.org/0009-0009-3131-4292>

Аннотация. Описаны различные методы стеганографии, способы выявления её применения, приведены примеры использования стеганографии в различных сферах, от защиты интеллектуальной собственности до преступлений в киберпространстве

Ключевые слова: киберпространство, кибербезопасность, информационная безопасность, стеганография.

Для цитирования: Гулак М.Л. О применении стеганографии в различных сферах // Актуальные проблемы кибербезопасности. Противодействие экстремизму и терроризму в информационной молодежной среде: сборник докладов I межрегиональной научно-практической конференции. – Брянск: БГТУ, 2025. – С. 64 – 68.

Киберпространство – это весьма сложная среда, возникающая в результате тесного взаимодействия людей, программного обеспечения и услуг в сети Интернет с использованием технологических устройств и подключенных к нему сетей, которые не существуют в какой-либо физической форме.

В международном стандарте ISO/IEC 27032:20125 даются следующие определения терминов «киберпространство» и «кибербезопасность»:

Кибербезопасность (или безопасность киберпространства) – сохранение конфиденциальности, целостности и доступности информации в киберпространстве.

Одно из направлений обеспечения кибербезопасности – возможность скрытой передачи данных, используя для обеспечения конфиденциальности различных криптографических методов. Одним из таких методов является стеганографическое сокрытие информации.

В статье рассмотрены история появления стеганографии, способы и формы ее применения в легитимных и преступных целях, а также методы выявления факта наличия скрытой посредством стеганографии информации.

Согласно классическому определению, стеганография – это способ скрытой передачи информации, направленный на утаивание самого факта такой передачи. Изначально предполагалось, что передаваемое сообщение должно скрываться внутри какой-либо другой информации или какого-то объекта, и его содержание при этом может не шифроваться. Однако, впоследствии применение стеганографии не исключало криптографического преобразования передаваемой информации для обеспечения более высокой степени защищенности.

Современные технологии позволяют обмениваться большими объемами информации практически мгновенно, однако вопрос безопасности передачи данных остается актуальным. Одной из угроз является возможность перехвата конфиденциальной информации третьими лицами. Для решения данной проблемы широко применяется такое направление криптографии, как шифрование, но оно имеет существенный недостаток: шифрованные сообщения привлекают внимание потенциальных злоумышленников. В отличие от криптографии, стеганография скрывает сам факт наличия тайного сообщения, что делает её эффективным инструментом для обеспечения конфиденциальности

В средние века термин «стеганография» был впервые использован в 1499 году аббатом Иоганном Тритемием. Однако различные методы сокрытия сообщений использовались и до появления термина. Например, Геродот описал в труде "История" некоторые техники, используемые греками в период войн с Персией. Среди них были такие, как нанесение татуировки с текстом на голове курьера, которому после отрастания волос предстояло отправиться по назначению или нанесение текста на вощеную табличку, скрытую за вторым слоем воска.

Впоследствии появились такие способы стеганографии, как использование симпатических чернил, которые бесцветны при обычных условиях, но проявляются при воздействии определённым реактивом или температуры.

Стремительное развитие техники, в частности фотографии, проводных и беспроводных средств связи, дало возможность применять новые способы стеганографии, которые нашли свое применение, например, в работе спецслужб.

В эпоху широкого распространения цифровых технологий применение методов стеганографии стала по-настоящему массовым. Причем нашла она свое применение и в легитимных целях, и для вредоносного воздействия.

В наше время методы стеганографии активно используются в разнообразных ситуациях в различных сферах, например, для передачи информации при необходимости обеспечить ее защиту от несанкционированного доступа.

Цифровые графические изображения – один из наиболее популярных типов файлов, используемых в качестве контейнеров (носителей) для стеганографического сокрытия информации. Алгоритмы внедряют скрываемые данные в наименее значимые биты, лишь в минимальной степени влияя на визуальное восприятие изображения пользователем, почти не ухудшая его качества.

Внедрение данных в аудиофайлы выполняется путем изменения таких характеристик звуковых волн как амплитуда или частота. Человеческий слух не в состоянии уловить эти изменения, но они могут быть декодированы с помощью специализированного программного обеспечения.

Стеганографические методы позволяют скрывать данные и в видеофайлах. Внедрение скрываемой информации осуществляется либо в частотных характеристиках видеопотока, либо в виде отдельных кадров.

Помимо защиты конфиденциальности информации стеганография позволяет размещать цифровые водяные знаки для указания на авторские права новостных материалов, защиты различного цифрового контента, например, потокового видео и аудио, от несанкционированного воспроизведения.

В контексте стремительного увеличения количества и сложности проводимых кибератак стеганография также используется для скрытой передачи данных. Уже в начале 2000-х годов злоумышленники начали использовать методы стеганографии в преступных целях.

Злоумышленники используют стеганографию для скрытия вредоносного программного кода в изображениях, аудиофайлах и других файлах, что позволяет избежать выявления этого вредоносного программного обеспечения системами безопасности и антивирусами, поскольку скрытая информация воспринимается как обычный файл. Однако, когда жертва получает файл с внедренным вредоносным кодом через соцсети или электронную почту и открывает его, вредоносное ПО активируется и запускает атаку. Самая известная атака с использованием методов стеганографии произошла в 2020 году, когда злоумышленники взломали SolarWinds, используя XML-файлы в качестве контейнеров для похищенных данных. В 2024 году группировка TA558 использовала для атак на 320 организаций по всему миру вредоносные программы, замаскированные под файлы JPEG.

Преступные группировки могут использовать стеганографию для обмена конфиденциальной информацией, такой как данные о банковских счетах, пароли или координация незаконных финансовых операций.

Эти и многие другие примеры показывают, насколько опасной и гибкой может быть стеганография в руках преступников. Борьба с такими угрозами требует развития специализированных инструментов и технологий, позволяющих выявлять скрытые данные.

Можно с уверенностью констатировать, что защита от атак с использованием стеганографии является весьма актуальной задачей.

Выявление стеганографии – весьма сложная задача. Программные средства стегоанализа существуют достаточно давно, однако сложность состоит в том, что проверить все графические, аудио и видеофайлы может оказаться невозможно из-за количества и размера. В некоторых случаях аудио и видео могут быть потоковыми, и их требуется анализировать «на лету».

С целью обеспечения требуемой защищенности от использования стеганографии в преступных целях применяются различные методы и подходы. Рассмотрим некоторые основные стратегии:

Специализированные программные инструменты анализа способны обнаруживать данные, скрытые в медиафайлах. Эти инструменты проводят анализ метаданных, статистические проверки и другие виды тестирования, чтобы выявить аномалии, характерные для файлов, подвергшихся стеганографической модификации.

Контроль за обменом медиаконтентом осуществляется с помощью систем мониторинга трафика и контент-фильтрации, отслеживающих подозрительные файлы. Это особенно важно для организаций, занимающихся обработкой большого объема мультимедийных данных.

Проверка цифровых подписей и сертификатов позволяет определить, был ли файл изменен после подписания и что документ или файл исходит от надежного источника.

Ограничение доступа к данным позволяет строго контролировать доступ к конфиденциальной информации и ограничить возможность ее передачи через неконтролируемые каналы связи.

Обучение сотрудников должно осуществляться на регулярной основе, проводимые курсы и тренинги по информационной безопасности должны включать темы, касающиеся распознавания потенциально опасных файлов и подозрительных сообщений.

Анализ поведения пользователей с целью выявления аномалий с использованием современных систем кибербезопасности позволяют, проанализировав поведение пользователей, выявлять отклонения, например, необычные объемы передачи данных или взаимодействие с определенными типами файлов.

Антивирусные решения и системы обнаружения вторжений могут включать функции определения скрытых данных.

Е. Калюшина, аналитик Positive Technologies, рекомендует для обнаружения вредоносной активности в сетевом трафике и борьбы со стеганографическими методами маскировки применять системы мониторинга и корреляции событий (SIEM), песочницы, средства детектирования и предотвращения вторжений (IDS/IPS).

Таким образом, можно сделать вывод, что построение системы защиты от использования стеганографических методов требует комплексного подхода, включающего технические меры, обучение персонала и постоянное совершенствование процессов управления.

Подводя итоги, можно сделать следующие выводы:

Технологии стеганографии используются не только для защиты от серьезных угроз, но и для достижения вредоносных целей. Применение этих методов не требует высокой квалификации и эффективно помогает маскировать злонамеренную активность, в том числе от средств защиты.

Использование программных инструментов для выявления стеганографии может быть трудоёмким, особенно при большом объёме данных. Однако решение должно быть комплексным.

Важным направлением является повышение осведомлённости сотрудников об основных угрозах стеганографии и методах реагирования на них.

Среди положительных аспектов стеганографии можно выделить такие, как возможность невидимого сокрытия данных, устойчивость к перехвату скрываемых сообщений, легкость интеграции с файлами различных типов, возможность многоуровневой защиты скрываемых данных путем комбинирования стеганографии с криптографией, малое искажение файла-контейнера, широкие возможности применения.

Позитивные стороны стеганографии сопровождаются негативными: ограниченный объем информации, которую можно скрыть в одном файле, уязви-

мость к разрушению скрываемых данных в случае повреждения файла-контейнера, зависимость от качества файла-контейнера, невозможность использования для динамических данных.

Список источников

1. Стеганография в кибератаках: скрытая передача данных в обход защиты. – Режим доступа: https://www.anti-malware.ru/analytics/Threats_Analysis/Steganography-Cyber-Attacks?utm_source=google&utm_medium=email&utm_campaign=amdelivery.
2. Uncovering the social impact of digital steganalysis tools applied to cyber-crime investigations: a European Union perspective. – Режим доступа: <https://crimesciencejournal.biomedcentral.com/articles/10.1186/s40163-024-00209-7>.
3. Стеганография в современных кибератаках. – Режим доступа: <https://securelist.ru/steganography-in-contemporary-cyberattacks/79090/?ysclid=m8fxinqrtx534557525>.
4. Как выявить атаку злоумышленников в сетевом трафике. – Режим доступа: <https://www.anti-malware.ru/practice/methods/How-to-detect-attackers-in-network-traffic>.

Статья поступила в редакцию 26.04.2025; принята к публикации 15.05.2025

Информация об авторе

Гулак М.Л. – к.т.н., доцент кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Научная статья
УДК 004

Проактивный поиск сложных киберугроз (threat hunting)

Алексей Владимирович Евдокимов ^{1✉}, Федор Евгеньевич Березкин ²,
Кирилл Александрович Анищенко ³

^{1, 2, 3}Брянский государственный технический университет, Брянск, Россия

¹alekseievdokimov05@gmail.com ✉, <https://orcid.org/0009-0004-4331-1279>

²fedor.berezkin32@yandex.ru, <https://orcid.org/0009-0002-0105-7335>

³kirill.anishenkov@gmail.com, <https://orcid.org/0009-0000-9011-2804>

Аннотация. В данной статье рассмотрен проактивный поиск сложных киберугроз как один из методов защиты информации.

Ключевые слова: Threat hunting, обнаружение угроз, киберугрозы, гипотеза, компрометация.

Для цитирования: Евдокимов А.В., Березкин Ф.Е., Анищенко К.А. Проактивный поиск сложных киберугроз (threat hunting) // Актуальные проблемы кибербезопасности и их решения. Противодействие экстремизму и терроризму в информационной молодежной среде: сборник докладов I межрегиональной научно-практической конференции. – Брянск: БГТУ, 2025. – С. 69 – 71.

Со временем киберугрозы становятся все более продвинутыми и могут успешно обходить различные методы защиты, а также оставаться незамеченными для ИБ специалистов. Ввиду этого, для современных систем защиты информации будет недостаточно только превентивных средств защиты, но также нужны и средства мониторинга. В данной статье будет рассмотрен Threat hunting или ТН – проактивный поиск следов взлома или функционирования вредоносных программ, которые не обнаружены стандартными средствами защиты.

В отличие от классических систем защиты, в которых аналитик действует по срабатыванию сенсоров системы защиты, в процессе threat hunting аналитик целенаправленно ищет следы компрометации. Для этого он вырабатывает «гипотезы» – предположения, как злоумышленники могли проникнуть в сеть [1].

При этом процесс Threat Hunting должен проводиться непрерывно, в соответствии с разработанными гипотезами и планами обнаружения скрытых угроз - это значит, что поиск киберугроз не может иметь хаотичный или спорадический характер, когда ИБ-аналитики лишь время от времени проверяют, нет ли в зафиксированных ранее событиях ИБ признаков каких-то незамеченных киберинцидентов [2].

Гипотезы для threat hunting можно формировать из различных источников, например, из:

- матрица MITRE ATT&CK;

- отчеты Threat Intelligence, содержащие много полезной информации о техниках и процедурах атакующих, использованных ими в реальных инцидентах;
- блоги, Twitter, выступления на конференциях исследователей и специалистов по кибербезопасности, которые охотно делятся результатами исследований;
- практика реагирования и расследования инцидентов, помогающая погрузиться в сам процесс;
- опыт специалистов по тестированию на проникновение, изучение которого позволяет ознакомиться с актуальными методиками [3].

Теперь, рассмотрим то, как внедрить в организацию Threat Hunting. Для того, чтобы внедрить процесс поиска киберугроз в компании важно разработать политику Threat Hunting, в которую следует включить правила разработки и документирования гипотез. Порядок формирования плана поиска признаков, не обнаруженных иными способами атак, плана выполнения действий при успешном подтверждении разработанной гипотезы, способы улучшения процесса поиска киберугроз при завершении очередной проверки гипотезы, способы передачи полученных знаний и предложений по повышению уровня защищенности компании заинтересованным лицам. Также следует перечислить необходимые ресурсы для выполнения процесса поиска киберугроз, определить ожидаемые результаты и формы отчетности, способы передачи обнаруженных угроз команде реагирования, закрепить полномочия ответственных и исполнителей, а затем согласовать разработанную политику у руководителя структурного подразделения [3].

Однако, стоит сказать, что использование Threat hunting – это дорогостоящий и сложный процесс, и оправдать вложения может только в организациях с высоким уровнем зрелости ИБ. Тем не менее, это также мощный инструмент защиты информационных систем.

Список источников

1. Что такое Threat hunting и как правильно охотиться на киберпреступников. URL: <https://habr.com/ru/companies/pt/articles/510362/>.
2. Охота за угрозами, зачем она нужна. URL: <https://cyberpolygon.com/ru/materials/threat-hunting-why-might-you-need-it/>.
3. Threat hunting: методы и практики обнаружения угроз. URL: https://www.securityvision.ru/info/threat_hunting/.

Статья поступила в редакцию 22.04.2025; принята к публикации 10.05.2025

Информация об авторах

Евдокимов А.В. – студент кафедры «Системы информационной безопасности», направление подготовки 10.05.03 – Информационная безопасность автоматизированных систем ФГБОУ ВО «БГТУ».

Березкин Ф.Е. – студент кафедры «Системы информационной безопасности», направление подготовки 10.05.03 – Информационная безопасность автоматизированных систем ФГБОУ ВО «БГТУ».

Анищенков К.А. – студент кафедры «Системы информационной безопасности», направление подготовки 10.05.03 – Информационная безопасность автоматизированных систем ФГБОУ ВО «БГТУ».

Вклад авторов

Евдокимов А.В. – сбор материала, обработка материала, частичное написание статьи (34%).

Березкин Ф.Е. – частичное написание статьи, редактирование статьи (33%).

Анищенков К.А. – идея, частичный сбор материала (33%).

Научный руководитель

Шапенская А.М. – ассистент кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Конфликт интересов отсутствует.

Научная статья
УДК 004.056

Анализ нормативных основ, регламентирующих безопасность интернета вещей в России и мире

Владислав Павлович Киселев^{1✉}, Александр Александрович Бузылев^{2✉},
Дмитрий Андреевич Лысов^{3✉}, Алексей Петрович Горлов^{4✉}

^{1,2,3,4} Брянский государственный технический университет, Брянск, Россия

¹vkiselev1213@gmail.com[✉], <https://orcid.org/0009-0002-5845-1149>

²buzylev2018@yandex.ru[✉], <https://orcid.org/0009-0005-3301-7006>

³lysovdmritriia@gmail.com[✉], <https://orcid.org/0009-0003-9666-7191>

⁴apgorlov@gmail.com[✉], <https://orcid.org/0009-0003-3100-3466>

Аннотация. В статье рассматриваются правовые основы обеспечения информационной безопасности Интернета вещей (IoT) в России и за рубежом.

Ключевые слова: интернет вещей (IoT), правовые основы, защита информации, требования.

Для цитирования: Киселев В.П., Бузылев А.А., Лысов Д.А., Горлов А.П. Анализ нормативных основ, регламентирующих безопасность интернета вещей в России и мире // Актуальные проблемы кибербезопасности. Противодействие экстремизму и терроризму в информационной молодежной среде: сборник докладов I межрегиональной научно-практической конференции. – Брянск: БГТУ, 2025. – С. 72 – 75.

Интернет вещей (IoT) становится неотъемлемой частью цифрового мира, но сопровождается рисками информационной безопасности, а единых методов правового регулирования в этой сфере на данный момент нет. Каждая страна разрабатывает свои нормы, но они имеют существенные различия по уровню детализации, подходам и мерам.

Рассмотрим зарубежные и отечественные правовые решения по обеспечению безопасности устройств интернета вещей.

Зарубежные правовые основы:

1. Законодательство Великобритании

Закон о безопасности продуктов и телекоммуникационной инфраструктуры (PSTI Act) от 29 апреля 2023года:

- статья о паролях запрещает использование предустановленных паролей по умолчанию для IoT-устройств и требует уникальный пароль для каждого устройства;
- статья об уязвимостях обязывает производителей иметь общедоступную точку контакта для сообщений об уязвимостях;
- статья об обновлениях требует от производителей указывать минимальный срок поддержки обновлений безопасности для устройств;
- статья о штрафах: нарушение требований может привести к штрафам до 10 миллионов долларов или 4% годового дохода компании.

2. Евросоюз

Евросовет принял закон, который устанавливает правила по кибербезопасности для подключенных цифровых устройств, связанных с интернетом вещей. Этот закон начнет действовать с 1 ноября 2024 года.

Регламент, вышедший 10 октября 2024 года, вводит общие требования для всех стран ЕС по кибербезопасности IoT-устройств. Эти требования касаются проектирования, разработки, производства и продажи аппаратного и программного обеспечения.

3. США:

- закон о совершенствовании кибербезопасности IoT от 4 декабря 2020 года. Статья о стандартах NIST требует от NIST разрабатывать и публиковать стандарты для федерального правительства по использованию и управлению IoT-устройствами, включая минимальные требования к информационной безопасности;
 - статья об ограничениях на приобретение запрещает федеральным агентствам приобретать IoT-устройства, не соответствующие этим стандартам, за исключением случаев национальной безопасности или исследований.

Общие черты зарубежных подходов:

- Акцент на обязательные технические требования к устройствам, такие как уникальные пароли и обновления;
- Обязательная сертификация и стандартизация;
- Прозрачность и ответственность производителей;
- Защита персональных данных в соответствии с GDPR и другими нормами.

Российские правовые основы

1. Федеральный закон №152-ФЗ «О персональных данных»:

- статья 5, пункт 2 – обработка персональных данных должна ограничиваться конкретными, законными и заранее определёнными целями. Это важно для IoT-устройств, которые собирают данные пользователей;
 - статья 6 – обязательное получение согласия субъекта персональных данных на их обработку, включая данные, получаемые через IoT-устройства;
 - требования к уничтожению или обезличиванию данных после достижения цели обработки.
- Федеральный закон №149-ФЗ «Об информации, информационных технологиях и о защите информации»:
- статья 3, пункт 7 – неприкосновенность частной жизни, запрещается сбор, хранение, использование и распространение информации о частной жизни без согласия лица;
 - статья 5 – регулирует режимы доступа к информации, включая ограничения и условия предоставления;
 - статья 16 – общие условия защиты информации, включая информационные системы и сети, что применимо к IoT-инфраструктуре.

2. Федеральный закон №187-ФЗ «О безопасности критической информационной инфраструктуры», устанавливает требования к защите объектов критической информационной инфраструктуры, к которым могут относиться IoT-системы в стратегически важных отраслях.

3. Доктрина информационной безопасности Российской Федерации, подчеркивает важность защиты информационной безопасности граждан и государства, включая развитие технологий IoT.

4. Приказ Минкомсвязи России №637 утверждает «дорожную карту» развития узкополосных беспроводных сетей IoT, включая разработку моделей угроз и мер защиты.

5. ГОСТ Р 71168-2023 - стандарт, устанавливающий требования безопасности и конфиденциальности передачи данных IoT, включая шифрование и аутентификацию устройств.

6. Стандартизация и технические меры.

В России разрабатываются национальные стандарты, например ГОСТы по безопасности IoT, а также применяются международные стандарты ISO/IEC 27001. Но их внедрение и контроль пока не являются строго обязательными.

Обеспечение безопасности IoT-устройств требует учета различных юридических аспектов. В других странах уже принимают законы с конкретными требованиями к безопасности, сертификации и контролю производителей. В России пока действуют только общие законы о персональных данных и информации. Чтобы повысить безопасность, нужно разработать обязательные стандарты и сотрудничать с другими странами. Это поможет улучшить защиту устройств интернета вещей как в нашей стране, так и за рубежом.

Список источников

1. Хабр. URL: <https://habr.com/ru/articles/700800/> (дата обращения: 18.04.2025).

2. CYBER LENINKA. URL: <https://cyberleninka.ru/article/n/pravovoe-regulirovanie-ispolzovaniya-interneta-veschey> (дата обращения: 18.04.2025).

3. Правовая характеристика использования Интернета вещей. URL: <http://www.publishing-vak.ru/file/archive-law-2023-4/c24-lunkin-dmitrii.pdf> (дата обращения: 20.04.2025).

4. Anti-Malware. URL: <https://www.anti-malware.ru/news/2024-10-14-121598/44389> (дата обращения: 21.04.2025).

Статья поступила в редакцию 23.04.2025; принята к публикации 10.05.2025

Информация об авторах

Киселев В.П. – студент кафедры «Системы информационной безопасности», направление подготовки 10.03.01 – Информационная безопасность ФГБОУ ВО «БГТУ».

Бузылев А.А. – студент кафедры «Системы информационной безопасности», направление подготовки 10.04.01 – Информационная безопасность ФГБОУ ВО «БГТУ».

Лысов Д.А. – старший преподаватель кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Горлов А.П. – к.т.н., доцент кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Вклад авторов

Киселев В.П. – идея, сбор материала, обработка материала, частичное написание статьи (25%).

Бузылев А.А. – сбор материала, обработка материала, частичное написание статьи (25%).

Лысов Д.А. – написание статьи, научное редактирование текста (25%).

Горлов А.П. – написание статьи, научное редактирование текста (25%).

Конфликт интересов отсутствует.

Научная статья
УДК 378:004

Оценка уязвимости объектов: подход к определению вероятного внутреннего нарушителя

Ольга Сергеевна Козлова

Брянский государственный технический университет, Брянск, Россия
koz0042112@gmail.com, <https://orcid.org/0009-0008-1222-9554>

Аннотация. Статья посвящена оценке потенциала нарушителей информационной безопасности. В ней рассматриваются методы оценки уязвимости информационных систем через анализ действий внутренних нарушителей. Особое внимание уделяется критериям оценки риска, связанного с сотрудниками организации, таким как уровень доступа, технические навыки, мотивация, опыт нарушений и физический доступ. Предлагается подход к систематизации оценки риска и разработке мер по защите информации.

Ключевые слова: оценка потенциала нарушителя, внутренние угрозы, сценарии реализации угроз, защита данных, уровень доступа, технические навыки, мотивация нарушителя.

Для цитирования: Козлова О.С. Оценка уязвимости объектов: подход к определению вероятного внутреннего нарушителя // Актуальные проблемы кибербезопасности. Противодействие экстремизму и терроризму в информационной молодежной среде: сборник докладов I межрегиональной научно-практической конференции. – Брянск: БГТУ, 2025. – С. 76 – 80.

В современном мире, где цифровые технологии играют важную роль в жизни и бизнесе, обеспечение информационной безопасности становится всё более значимым. Оценка потенциала нарушителей — ключевой элемент в разработке эффективной стратегии защиты информации. Она позволяет предвидеть возможные атаки и заранее подготовиться к их отражению.

На основе отчёта Экспертно-аналитического центра ГК InfoWatch за 2024 год выявлено, что доля умышленных нарушений составила 97,9%, а случайных — 2,1%. Внешние нарушители остаются основной причиной утечек данных, однако внутренние также представляют значительный риск. В 2024 году увеличилась доля утечек по вине привилегированных пользователей, таких как руководители и системные администраторы, а также подрядчиков. При этом доля нарушений со стороны непривилегированных пользователей немного уменьшилась.

Для обнаружения внутренних нарушителей и оценки угрозы необходимо учитывать несколько критериев. Во-первых, должность нарушителя: привилегированные пользователи и подрядчики требуют особого контроля, так как имеют доступ к значительным объёмам данных и могут нанести серьёзный ущерб при нарушении безопасности. Во-вторых, тип нарушения: умышленные нарушения доминируют, но случайные также могут привести к серьёзным последствиям, особенно если речь идёт о крупных базах данных.

Оценка угрозы может быть следующей: высокий уровень угрозы характерен для компаний с большим количеством привилегированных пользователей и

подрядчиков, имеющих доступ к чувствительным данным. Средний уровень угрозы наблюдается в организациях, где есть баланс между количеством привилегированных и непривилегированных пользователей. Низкий уровень угрозы присущ компаниям, которые строго контролируют доступ к данным и регулярно проводят обучение сотрудников по вопросам информационной безопасности.

Распределение утечек по типам нарушителей различается в зависимости от страны. Например, в США внешние нарушители стали причиной 95,8% утечек, а сотрудники — 2,6%. В России эти показатели составляют 87,4% и 10,1% соответственно. В Великобритании — 90% и 8,7%.

Распределение утечек информации по типам внутренних нарушителей за 2024 год:

- Другие/Неизвестно — 3,44%.
- Подрядчик — 2,55%.
- Бывший сотрудник — 0,12%.
- Системный администратор — 0,03%.
- Руководитель — 0,12%.
- Сотрудник — 3,13%.

Ввиду приведенной статистики целесообразно рассмотреть внутренних нарушителей и определить по каким критериям нужно рассчитывать угрозу.

Для эффективного выявления и оценки потенциальной опасности внутренних нарушителей необходимо учитывать несколько важных параметров. Во-первых, уровень доступа сотрудника к информации и системам играет решающую роль. Пользователи с ограниченным доступом, например, обычные офисные работники, представляют меньшую угрозу, тогда как привилегированные пользователи — системные администраторы, руководители отделов — имеют широкий доступ к критичным данным и могут нанести значительный ущерб при нарушении безопасности. Во-вторых, технические навыки сотрудника существенно влияют на его возможности обойти защитные меры. Пользователи с базовыми знаниями вряд ли смогут сознательно нанести вред, тогда как опытные IT-специалисты обладают инструментами и знаниями для реализации сложных атак. В-третьих, мотивация нарушителя — важнейший фактор. Случайные ошибки и неосознанные нарушения встречаются часто, но именно умышленные действия, связанные с личной выгодой или желанием навредить, требуют особого внимания и контроля. Также следует учитывать опыт нарушений: сотрудники с историей нарушений безопасности и умением скрывать следы представляют повышенную угрозу. Оценка угрозы может быть следующей: высокий уровень угрозы характерен для компаний с большим количеством привилегированных пользователей и подрядчиков, имеющих доступ к чувствительным данным. Средний уровень угрозы наблюдается в организациях, где есть баланс между количеством привилегированных и непривилегированных пользователей, с учётом возможных случайных нарушений. Низкий уровень угрозы присущ компаниям, которые строго контролируют доступ к данным и регулярно проводят обучение сотрудников по вопросам информационной безопасности. Наконец, физический доступ

к важным объектам — серверным помещениям, центрам обработки данных — увеличивает возможности для реализации угроз и требует усиленного контроля.

Таблица 1

Таблица параметров оценки внутренних нарушителей

Параметр	Объяснение простыми словами	1 балл	2 балла	3 балла	4 балла	5 баллов
Уровень доступа	Насколько много информации и систем может использовать сотрудник	Доступ только к личной почте и файлам	Доступ к нескольким отдельным папкам	Доступ к документам и базам данных отдела	Доступ к важным системам и настройкам	Полный доступ к критичной информации и системам
Технические навыки	Насколько хорошо сотрудник умеет работать с компьютерами и системами	Знает только базовые функции (почта, текстовый редактор)	Может пользоваться офисным ПО и простыми программами	Уверенно работает с разными программами, умеет обходить простые ограничения	Знает основы администрирования и настройки систем	Профессиональный IT-специалист с глубокими знаниями и навыками взлома
Мотивация	Насколько сильно сотрудник хочет или может навредить	Нет желания вредить, случайные ошибки	Небольшая заинтересованность, неосознанные нарушения	Возможна выгода, иногда нарушает правила	Явная личная заинтересованность в нарушениях	Целенаправленное вредительство, саботаж, злонамеренные действия
Опыт нарушений	Был ли у сотрудника опыт нарушения безопасности	Нет опыта нарушений	Были мелкие нарушения, исправленные быстро	Единичные нарушения с последствиями	Несколько серьезных нарушений, умение скрывать следы	Частые нарушения, систематический вред, опыт сокрытия
Физический доступ	Насколько сотрудник может физически попасть к важным объектам	Нет физического доступа (работает удаленно)	Редкие посещения офиса, без доступа к техническим помещениям	Регулярное присутствие в офисе, но без доступа к серверным	Имеет ключи или пропуск в технические помещения	Полный физический доступ к серверным, ЦОД и другим важным зонам

Таблица 2

**Классификация внутренних нарушителей по сумме баллов
и уровню риска (с категориями нарушителей,
диапазонами баллов и примерами)**

Категория	Уровень	Суммарный балл
1	Базовый	5-8
2	Базовый повышенный	9-12
3	Средний	13-17
4	Высокий	18-25

На основе проведённой оценки уязвимостей и классификации внутренних нарушителей по уровню риска предлагаю следующие меры по нейтрализации потенциальных угроз:

Для категории 1 (базовый уровень, 5–8 баллов) необходимо внедрить строгие процедуры управления доступом к информационным системам и ресурсам, ограничить возможности использования корпоративных данных. Также важно организовать регулярные обучающие программы по информационной безопасности для повышения осведомлённости сотрудников о существующих правилах и рисках и реализовать систему мониторинга действий пользователей для оперативного выявления и анализа подозрительной активности.

Для категории 2 (базовый повышенный уровень, 9–12 баллов) следует ужесточить политику доступа к чувствительным данным и системам, минимизировав привилегии для пользователей, отнесённых к категории повышенного риска. Необходимо периодически проводить ревизию и корректировку прав доступа в соответствии с актуальными ролями и обязанностями сотрудников и внедрить многофакторную аутентификацию для усиления защиты учётных записей и предотвращения несанкционированного доступа.

Для категории 3 (средний уровень, 13–17 баллов) требуется ограничить физический доступ к критически важным объектам и зонам для лиц, не обладающих соответствующими полномочиями. Также нужно установить и настроить системы обнаружения вторжений и аномальной активности для своевременного реагирования на потенциальные угрозы и проводить регулярные аудиты безопасности с целью выявления и устранения уязвимостей в информационных системах.

Для категории 4 (высокий уровень, 18–25 баллов) необходимо провести полный аудит прав доступа с последующей минимизацией привилегий для пользователей, представляющих высокий уровень риска. Следует внедрить решения для шифрования данных и защиты критически важной информации от несанкционированного доступа, создать изолированные сетевые сегменты для ограничения распространения угроз в случае их возникновения и разработать и внедрить детальный план реагирования на инциденты, предусматривающий быстрые

и эффективные меры по устранению последствий возможных нарушений безопасности.

Таким образом, в статье рассмотрен простой и понятный способ оценки уязвимости информационных систем через анализ действий внутренних нарушителей. Предложенные таблицы с критериями и баллами помогают систематизировать подход к оценке риска, связанного с сотрудниками организации.

Важно отметить, что выделены пять основных параметров — уровень доступа, технические навыки, мотивация, опыт нарушений и физический доступ — которые вместе дают полную картину потенциальной угрозы. На основе суммы баллов нарушителей можно разделить на группы по уровню риска, что позволяет сосредоточить внимание и ресурсы именно на тех, кто представляет наибольшую опасность.

Кроме того, данный подход достаточно гибкий и может быть адаптирован под разные организации и ситуации. Он позволяет не только выявлять потенциальных нарушителей, но и принимать более обоснованные решения по защите информации — например, усиливать контроль, проводить обучение или ограничивать доступ.

В итоге, предложенный подход к определению вероятного внутреннего нарушителя помогает сделать систему безопасности более эффективной и снизить риски, связанные с внутренними угрозами. Это особенно важно, ведь именно сотрудники часто оказываются источником проблем, и грамотная оценка их возможностей и мотивации является ключом к надежной защите.

Список источников

1. Методический документ «Методика оценки угроз безопасности информации»; «БДУ - Нарушители» (утв. Федеральной службой по техническому и экспортному контролю 5 февраля 2021 г.). URL: <https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-5-fevralya-2021-g> (дата обращения: 11.03.2025).
2. Аналитический отчет Infowatch – 2024. URL: <https://www.infowatch.ru/sites/default/files/analytics/files/utechki-informatsii-v-mire-2023-2024-gody.pdf>.

Статья поступила в редакцию 27.04.2025; принята к публикации 10.05.2025

Информация об авторе

Козлова О.С. – студент кафедры «Системы информационной безопасности», направление подготовки 10.03.01 – Информационная безопасность, профиль «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Научный руководитель

Голембиовская О.М. – канд. техн. наук, доцент, доц. каф. «СИБ» ФГБОУ ВО «БГТУ».

Научная статья
УДК 004

Обзор средств защиты и мониторинга информационных систем

Сергей Игоревич Коновалов ^{1✉}, Павел Александрович Аверин ²,
Кирилл Вадимович Логинов ³

^{1, 2, 3} Брянский государственный технический университет, Брянск, Россия

¹ velvet1way@gmail.com [✉], <https://orcid.org/0009-0008-5867-635X>

² stopnotwont@gmail.com, <https://orcid.org/0009-0003-5074-7217>

³ kirill228.log@gmail.com, <https://orcid.org/0009-0008-5065-6530>

Аннотация. Статья представляет собой обзор современных средств защиты и мониторинга информационных систем (ИС). В ней рассматриваются основные типы угроз, актуальные тенденции в развитии средств защиты и мониторинга, а также их классификация по функциональным возможностям. Цель статьи – дать структурированный обзор текущего состояния средств защиты и мониторинга, а также обозначить направления для дальнейших исследований в этой области.

Ключевые слова: информационная безопасность, информационная система, защита информации, мониторинг, SIEM, IDS/IPS, SOC, SOAR, антивирус, межсетевой экран, машинное обучение, искусственный интеллект, угрозы.

Для цитирования: Коновалов С.И., Аверин П.А., Логинов К.В. Обзор средств защиты и мониторинга информационных систем // Актуальные проблемы кибербезопасности. Противодействие экстремизму и терроризму в информационной молодежной среде: сборник докладов I межрегиональной научно-практической конференции. – Брянск: БГТУ, 2025. – С. 81 – 84.

ИТ-инфраструктура современных предприятий с развитием информационных технологий претерпевает постоянные изменения [1]. В связи с этим, информационные системы (ИС) играют ключевую роль в деятельности большинства организаций. С увеличением зависимости от ИС растут и риски, связанные с информационной безопасностью. Надежная защита и непрерывный мониторинг становятся критически важными для обеспечения непрерывности бизнеса, защиты конфиденциальной информации и соблюдения нормативных требований.

Средства защиты информации — это совокупность инженерно-технических, электрических, электронных, оптических и других устройств и приспособлений, приборов и технических систем, а также иных вещных элементов, используемых для решения различных задач по защите информации, в том числе предупреждения утечки и обеспечения безопасности защищаемой информации [2]. Средства защиты информации подразделяются на несколько категорий в зависимости от выполняемых функций.

Одним из ключевых направлений защиты является аутентификация и авторизация, которые обеспечивают контроль доступа к информационным ресурсам. Традиционная парольная защита требует строгого соблюдения политики безопасности, включая использование сложных комбинаций символов и регулярную смену паролей. Кроме того, существенно повышает уровень безопасности многофакторная аутентификация, включающая несколько независимых методов подтверждения личности. А в последнее время широкое распространение получила биометрическая аутентификация, основанная на использовании уникальных биологических характеристик пользователя.

Криптографические методы играют центральную роль в защите конфиденциальной информации. По данным InfoWatch, более 70% российских компаний используют средства криптографической защиты информации (СКЗИ) для защиты конфиденциальных данных [3]. Это обусловлено требованиями российского законодательства в области защиты персональных данных и государственной тайны.

Для предотвращения несанкционированного доступа применяются системы обнаружения и предотвращения вторжений. Они подразделяются на системы обнаружения атак (IPS), которые уведомляют администратора о подозрительной активности, и системы предотвращения атак (IDS), способные автоматически блокировать угрозы в режиме реального времени. Анализ рынка показывает, что наиболее популярными российскими межсетевыми экранами являются продукты компаний "Код Безопасности" и "С-Терра СиЭсПи" [4].

Межсетевые экраны (firewall) — это ключевой элемент защиты сети, обеспечивающий фильтрацию входящего и исходящего трафика. Пакетные фильтры контролируют соединения на основе IP-адресов, портов и протоколов, но не отслеживают состояние сеансов. Более продвинутые сетевые экраны с отслеживанием состояния соединений учитывают контекст взаимодействий, что повышает их эффективность. Межсетевые экраны нового поколения (NGFW) сочетают классическую фильтрацию с глубоким анализом пакетов (DPI), встроенной системой предотвращения вторжений (IPS) и антивирусной защитой, что позволяет выявлять сложные угрозы и обеспечивать более высокий уровень безопасности.

Средства мониторинга информационной безопасности (СМИБ) — это программно-аппаратные комплексы, предназначенные для сбора, анализа и корреляции событий информационной системы с целью выявления угроз и аномалий. Они анализируют сетевой трафик и журналы событий, чтобы обнаруживать подозрительную активность и потенциальные атаки.

Одним из наиболее эффективных инструментов мониторинга является система управления событиями безопасности (SIEM), обеспечивающая централизованный сбор и анализ данных из различных источников. По последним данным, спрос на российские SIEM-системы, такие как MaxPatrol SIEM (Positive Technologies) и Solar Dozor (Ростелеком-Солар) непрерывно растет в связи с требованиями регуляторов (ФСТЭК, Банк России) по обеспечению мониторинга и реагирования на инциденты информационной безопасности.

Внедрение технологии Security Orchestration, Automation and Response (SOAR) позволяет автоматизировать процессы реагирования на инциденты, сокращая время их устранения. Существенную роль играют системы мониторинга сети, анализирующие трафик для выявления подозрительной активности. Использование методов машинного обучения и поведенческого анализа способствует обнаружению сложных кибератак, которые не могут быть выявлены традиционными средствами защиты. Эти средства мониторинга обеспечивают комплексный подход к наблюдению за состоянием ИС, позволяя своевременно выявлять и реагировать на потенциальные угрозы.

Так же, современные тенденции показывают рост интереса к созданию центров мониторинга и реагирования на инциденты (SOC, Security Operations Center). Это специализированное подразделение или сервис, занимающееся обнаружением, анализом и реагированием на киберугрозы в режиме реального времени. По оценкам экспертов, более 50% крупных российских компаний создали собственные SOC или пользуются услугами коммерческих SOC для защиты от кибератак и минимизации последствий инцидентов [2]. Основная причина распространения SOC — необходимость оперативного выявления и устранения угроз, а также соответствие требованиям законодательства в области информационной безопасности.

Обеспечение информационной безопасности представляет собой сложную и многогранную задачу. Для эффективной защиты информационных систем необходим комплексный подход, включающий использование разнообразных средств защиты и мониторинга, а также постоянный анализ угроз и адаптация к изменяющимся условиям. Внедрение перспективных технологий, таких как искусственный интеллект и машинное обучение, обещает значительно повысить эффективность защиты и мониторинга в будущем. Дальнейшие исследования в этой области направлены на создание более эффективных и автоматизированных средств защиты, способных противостоять современным и будущим угрозам.

Список источников

1. Стукалин А. А., Назарова О. Б. Системы мониторинга информационных инцидентов (SIEM-системы): обзор и сравнительный анализ // Управленческие механизмы противодействия идеологии экстремизма и терроризма. 2018. С. 116-121.
2. Средства защиты информации // StudFiles. URL: <https://studfile.net/preview/6006132/page:4/> (дата обращения: 26.03.2025).
3. Утечки информации ограниченного доступа в России // InfoWatch. URL: <https://www.infowatch.ru/analytics/analitika/rossiya-utechki-informatsii-ogranichennogo-dostupa-2022-2023-gody> (дата обращения: 26.03.2025).
4. Технические средства мониторинга ИБ // Habr. URL: <https://habr.com/ru/articles/549050/> (дата обращения: 26.03.2025).

Статья поступила в редакцию 22.04.2025; принята к публикации 10.05.2025

Информация об авторах

Коновалов С.И. – студент кафедры «Системы информационной безопасности», специальность 10.05.03 – Информационная безопасность автоматизированных систем, специализация «Безопасность открытых информационных систем» ФГБОУ ВО «БГТУ».

Аверин П.А. – студент кафедры «Системы информационной безопасности», специальность 10.05.03 – Информационная безопасность автоматизированных систем, специализация «Безопасность открытых информационных систем» ФГБОУ ВО «БГТУ».

Логинов К.В. – студент кафедры «Системы информационной безопасности», направление подготовки 10.03.01 – Информационная безопасность ФГБОУ ВО «БГТУ».

Вклад авторов

Коновалов С.И. – идея, сбор материала, обработка материала, частичное написание статьи (35%).

Аверин П.А. – сбор материала, обработка материала, частичное написание статьи (35%).

Логинов К.В. – идея, сбор материала, обработка материала, частичное написание статьи (30%).

Научный руководитель

Шапенская А.М. – ассистент кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Конфликт интересов отсутствует.

Научная статья
УДК 004

Оценка соответствия требованиям приказа ФСТЭК России № 31

Сергей Игоревич Коновалов ^{1✉}, Павел Александрович Аверин ²,
Даниил Алексеевич Лактюшин ³

^{1, 2, 3} Брянский государственный технический университет, Брянск, Россия

¹ velvet1way@gmail.com [✉], <https://orcid.org/0009-0008-5867-635X>

² stopnotwont@gmail.com, <https://orcid.org/0009-0003-5074-7217>

³ mr.laktyushin99@mail.ru, <https://orcid.org/0009-0005-1641-5723>

Аннотация. Рассматриваются вопросы оценки соответствия требованиям приказа ФСТЭК России № 31, устанавливающего требования к обеспечению безопасности значимых объектов критической информационной инфраструктуры (КИИ). Представлены основные положения нормативного документа, методики оценки соответствия, а также анализ практических аспектов внедрения требований безопасности. Приведены примеры реализации требований, возникающие вызовы и возможные пути их преодоления.

Ключевые слова: приказ, ФСТЭК, оценка соответствия, защита информации, государственные информационные системы, аттестация, информационная безопасность, требования к защите.

Для цитирования: Коновалов С.И., Аверин П.А., Лактюшин Д.А. Оценка соответствия требованиям приказа ФСТЭК России № 31 // Актуальные проблемы кибербезопасности. Противодействие экстремизму и терроризму в информационной молодежной среде: сборник докладов I межрегиональной научно-практической конференции. – Брянск: БГТУ, 2025. – С. 85 – 88.

В условиях роста киберугроз обеспечение безопасности критической информационной инфраструктуры становится приоритетной задачей для государственных и частных организаций. В 2024 году число кибератак на российские компании увеличилось в 2,5 раза, достигнув 911 тысяч инцидентов, а утечки персональных данных затронули более 286 миллионов уникальных телефонных номеров и 96 миллионов адресов электронной почты [1]. Согласно отчетам, 15% всех атак в 2024 году были направлены на государственные учреждения, что на 6% больше, чем в 2023 году. Также около 30% всех киберинцидентов были связаны с действиями хактивистов [2]. Приказ ФСТЭК России № 31 устанавливает единые требования к защите значимых объектов КИИ, регламентирует порядок их категорирования, обеспечения безопасности и контроля за выполнением установленных норм. Оценка соответствия требованиям приказа является ключевым этапом в процессе обеспечения безопасности и устойчивости объектов КИИ.

Основные положения приказа ФСТЭК 31 Приказ ФСТЭК № 31 регламентирует требования к защите значимых объектов КИИ в зависимости от их категории значимости. Основные положения документа включают:

1. Процедуру категорирования объектов КИИ и определение их значимости.

2. Определение угроз безопасности информации и оценку рисков.
3. Выбор и внедрение организационных и технических мер защиты.
4. Проведение мониторинга, контроля и анализа эффективности применяемых мер.

5. Подготовку отчетности и взаимодействие с органами ФСТЭК России [3].

Приказ обязывает организации внедрять комплексные системы защиты, сочетающие технические и организационные меры. Это означает, что системы мониторинга должны постоянно отслеживать аномалии в сетевом трафике и действиях пользователей, системы обнаружения атак применять как сигнатурный, так и эвристический анализ для своевременного выявления угроз, а системы реагирования обеспечивать быструю изоляцию и нейтрализацию инцидентов. Важным условием является использование исключительно сертифицированных средств, соответствующих национальным стандартам и методическим рекомендациям ФСТЭК России, что гарантирует надежность и эффективность защиты.

Оценка соответствия требованиям ФСТЭК 31 осуществляется по следующим этапам:

1. Определение категории значимости объекта КИИ.
2. Анализ угроз и моделирование потенциальных атак.
3. Разработка и внедрение комплекса защитных мер.
4. Проведение испытаний и аудитов безопасности.
5. Оформление отчетности и подготовка рекомендаций.

Аудит и проверка соответствия осуществляются как силами собственных подразделений организаций, так и привлечёнными внешними экспертами, аккредитованными для проведения подобных оценок. Внутренний аудит позволяет оперативно выявлять несоответствия и оперативно реагировать на выявленные проблемы, используя глубокое знание внутренних процессов и специфики организации. С другой стороны, привлечение внешних экспертов обеспечивает независимую и объективную оценку, которая может выявить слабые места, незаметные для сотрудников компании. Чтобы повысить эффективность такого рода оценок, рекомендуется применение автоматизированных средств мониторинга и анализа событий информационной безопасности. Такие системы позволяют собирать и обрабатывать данные в режиме реального времени, что существенно ускоряет процесс выявления потенциальных угроз и несоответствий [4].

Процесс внедрения требований ФСТЭК 31 является не простым процессом, который сопровождается разными трудностями, например:

1. Высокие затраты на реализацию мер защиты и закупку сертифицированных средств.
2. Сложность трактовки отдельных положений приказа и необходимость экспертного анализа.
3. Дефицит квалифицированных специалистов в области кибербезопасности.
4. Постоянное изменение ландшафта угроз и необходимость регулярного обновления защитных мер [5].

Для успешного внедрения требований ФСТЭК 31 необходимо использовать комплексный подход, включающий разработку внутренних регламентов, обучение персонала, применение современных технологий защиты информации и регулярные проверки соответствия. Созданные регламенты обеспечивают единообразие действий, обучение повышает квалификацию сотрудников, а технологии способствуют своевременному выявлению угроз. Регулярные проверки, проводимые как внутренними подразделениями, так и внешними экспертами, позволяют объективно оценивать эффективность мер и вносить корректировки.

Оценка соответствия требованиям ФСТЭК 31 играет важную роль в обеспечении безопасности значимых объектов КИИ, поскольку правильное внедрение и контроль выполнения установленных требований значительно повышают уровень защиты информационных ресурсов. Несмотря на существующие сложности, перспективными направлениями развития являются совершенствование методов оценки соответствия, автоматизация процессов мониторинга и интеграция требований ФСТЭК 31 с международными стандартами информационной безопасности, что позволит более эффективно реагировать на современные вызовы в сфере кибербезопасности.

Список источников

1. Российский бизнес под атакой. Число хакерских нападений на компании за год выросло в 2,5 раза // CNews. URL: https://www.cnews.ru/news/top/2025-01-14_chislo_kiberatak_na_rossijskie (дата обращения: 27.03.2025).
2. Актуальные киберугрозы: III квартал 2024 года // Positive Technologies. URL: <https://www.ptsecurity.com/ru-ru/research/analytics/aktualnye-kiberugrozy-iii-kvartal-2024-goda/> (дата обращения: 27.03.2025).
3. ФСТЭК России. Приказ № 31 «О требованиях к обеспечению безопасности значимых объектов критической информационной инфраструктуры».
4. Сабельфильд Н. В. Оценка соответствия параметров средств защиты информации требованиям безопасности // Актуальные проблемы авиации и космонавтики. – 2017. – Т. 2. – № 13. – С. 224-226.
5. ФСТЭК России. Приказ от 25.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»

Статья поступила в редакцию 22.04.2025; принята к публикации 10.05.2025

Информация об авторах

Коновалов С.И. – студент кафедры «Системы информационной безопасности», специальность 10.05.03 – Информационная безопасность автоматизированных систем, специализация «Безопасность открытых информационных систем» ФГБОУ ВО «БГТУ».

Аверин П.А. – студент кафедры «Системы информационной безопасности», специальность 10.05.03 – Информационная безопасность автоматизированных систем, специализация «Безопасность открытых информационных систем» ФГБОУ ВО «БГТУ».

Лактюшин Д.А. – студент кафедры «Системы информационной безопасности», направление подготовки 10.05.03 – Информационная безопасность автоматизированных систем ФГБОУ ВО «БГТУ».

Вклад авторов

Коновалов С.И. – идея, сбор материала, обработка материала, частичное написание статьи.

Аверин П.А. – сбор материала, обработка материала, частичное написание статьи.

Лактюшин Д.А. – сбор материала, обработка материала, частичное написание статьи.

Научный руководитель

Шапенская А.М. – ассистент кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Конфликт интересов отсутствует.

Научная статья
УДК 004

Основные методы взлома паролей и способы противодействия им

Сергей Игоревич Коновалов^{1✉}, Павел Александрович Аверин²,
Дмитрий Андреевич Лысов³

^{1, 2, 3}Брянский государственный технический университет, Брянск, Россия

¹velvet1way@gmail.com✉, <https://orcid.org/0009-0008-5867-635X>

²stopnotwont@gmail.com, <https://orcid.org/0009-0003-5074-7217>

³lysovdmitriia@gmail.com, <https://orcid.org/0009-0003-9666-7191>

Аннотация. В статье рассматриваются основные методы взлома паролей, включая словарные атаки, полный перебор, использование радужных таблиц, фишинг, вредоносное ПО и социальную инженерию. Подробно анализируются принципы хеширования паролей и различия между устаревшими и современными алгоритмами защиты, такими как MD5, SHA-1, SHA-256, bcrypt, scrypt и Argon2. Отдельное внимание уделяется современным подходам к защите учётных данных: многофакторной аутентификации, использованию менеджеров паролей и принципам нулевого доверия. Сделан вывод о необходимости сочетания технологических и поведенческих мер для обеспечения устойчивой защиты от угроз, связанных с компрометацией паролей.

Ключевые слова: взлом паролей, словарная атака, brute-force, радужные таблицы, фишинг, хеширование, шпионское ПО, социальная инженерия, алгоритмы хеширования, многофакторная аутентификация, безопасность учётных данных, информационная безопасность.

Для цитирования: Коновалов С.И., Аверин П.А., Лысов Д.А. Основные методы взлома паролей и способы противодействия им // Актуальные проблемы кибербезопасности. Противодействие экстремизму и терроризму в информационной молодежной среде: сборник докладов I межрегиональной научно-практической конференции. – Брянск: БГТУ, 2025. – С. 89 – 91.

Современные информационные системы сталкиваются с постоянными угрозами несанкционированного доступа, основным вектором которых остаётся компрометация аутентификационных данных пользователей. Атаки на пароли становятся всё более разнообразными и технологически сложными, требуя соответствующего развития защитных механизмов. Цель данной статьи — провести системный анализ методов взлома паролей и методов их нейтрализации на основе теоретических основ криптографии, практических кейсов, а также последних исследований в области информационной безопасности.

Одним из наиболее распространённых подходов к подбору пароля является словарная атака, при которой злоумышленник использует заранее подготовленный список часто встречающихся паролей [1]. Этот метод эффективен в тех случаях, когда пользователь применяет простые или популярные комбинации символов. Несмотря на кажущуюся примитивность, словарные атаки нередко демонстрируют высокую результативность при отсутствии надлежащих мер защиты со стороны пользователя.

Брутфорс-атака (brute-force) представляет собой метод перебора всех возможных комбинаций символов, начиная с самых коротких. Алгоритмическая сложность данного подхода делает его крайне ресурсоёмким, однако с развитием вычислительных мощностей, в том числе с использованием GPU и распределённых вычислений, брутфорс остаётся угрозой для коротких и несложных паролей [2]. Радужные таблицы являются ещё одним инструментом, используемым для восстановления паролей из их хешей. Этот метод основывается на предварительно созданных таблицах, сопоставляющих хеши и соответствующие им пароли [3]. Основной уязвимостью, на которой строится эффективность радужных таблиц, является использование устаревших алгоритмов хеширования без соли (salt). Противодействием служит введение уникальных солевых значений и использование современных алгоритмов, способных замедлить процесс генерации хеша.

Фишинг и социальная инженерия не требуют технического взлома и направлены на обман пользователя. Фишинговые схемы предполагают подделку интерфейсов авторизации, что позволяет злоумышленнику получить пароль напрямую. Социальная инженерия, в свою очередь, использует психологическое давление, манипуляцию и доверие для получения конфиденциальной информации. Практические исследования показывают, что успешность подобных атак во многом зависит от уровня цифровой грамотности пользователей и качества обучения мерам кибергигиены.

Сохранённые пароли в браузерах и приложениях представляют собой потенциальную уязвимость, особенно в случае физического доступа к устройству или заражения его вредоносным ПО. Шпионские программы, такие как кейлоггеры и трояны, позволяют перехватывать вводимые данные в реальном времени и передавать их третьим лицам. Эффективной мерой противодействия этим угрозам является использование антивирусного программного обеспечения, контроль над правами доступа и регулярный аудит системы безопасности.

Ключевым элементом обеспечения надёжности хранения паролей выступает их хеширование. В отличие от шифрования, хеширование является необратимым процессом, не предполагающим расшифровки. Современные системы аутентификации применяют алгоритмы хеширования с высокой стойкостью к коллизиям и атаке методом перебора. Наиболее известными алгоритмами, используемыми в прошлом, являются MD5 и SHA-1, однако в настоящее время они считаются недостаточно безопасными. Алгоритмы нового поколения — SHA-256, bcrypt, scrypt и Argon2 — обеспечивают высокий уровень защиты благодаря функции замедления (time cost), использованию соли и возможности настройки параметров ресурсоёмкости.

Актуальные методы защиты учётных данных предполагают комплексный подход. Создание надёжных, уникальных паролей, длиной не менее 12 символов с использованием различных типов символов, значительно снижает риск их компрометации. Менеджеры паролей позволяют автоматически генерировать и хранить такие пароли, минимизируя человеческий фактор. Дополнительный уро-

вень безопасности обеспечивает многофакторная аутентификация (MFA), требующая, помимо пароля, подтверждения личности через одноразовый код, биометрию или аппаратный ключ. Применение протоколов типа WebAuthn и аппаратных токенов соответствует современным стандартам нулевого доверия (zero trust).

Таким образом, анализ методов взлома и средств защиты паролей демонстрирует необходимость постоянного совершенствования как технических решений, так и пользовательских практик. Несмотря на наличие большого числа уязвимостей, применение современных алгоритмов хеширования, многофакторной аутентификации и повышение цифровой грамотности пользователей позволяет существенно снизить риск компрометации учётных данных. Научные исследования и практика показывают, что устойчивость системы аутентификации формируется не только техническими средствами, но и социальной составляющей информационной безопасности.

Список источников

1. Зверев О. В. Методы взлома паролей и меры по противодействию взлому паролей // Безопасность информационных технологий: сб. науч. ст. С. 25.
2. Брутфорс // Сбербанк. URL: <http://www.sberbank.ru/ru/person/ki-brary/vocabulary/brutfors> (дата обращения: 18.04.2025).
3. 6 наиболее распространенных типов атак на пароль // Keeper Security. URL: <https://www.keepersecurity.com/blog/ru/2024/01/12/types-of-password-attacks/> (дата обращения: 18.04.2025).

Статья поступила в редакцию 19.04.2025; принята к публикации 10.05.2025

Информация об авторах

Коновалов С.И. – студент кафедры «Системы информационной безопасности», специальность 10.05.03 – Информационная безопасность автоматизированных систем, специализация «Безопасность открытых информационных систем» ФГБОУ ВО «БГТУ».

Аверин П.А. – студент кафедры «Системы информационной безопасности», специальность 10.05.03 – Информационная безопасность автоматизированных систем, специализация «Безопасность открытых информационных систем» ФГБОУ ВО «БГТУ».

Лысов Д.А. – старший преподаватель кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Вклад авторов

Коновалов С.И. – идея, сбор материала, обработка материала, частичное написание статьи (33%).

Аверин П.А. – сбор материала, обработка материала, частичное написание статьи (33%).

Лысов Д.А. – частичное написание статьи, научное редактирование текста (34%).

Конфликт интересов отсутствует.

Научная статья
УДК 004

Применение утилиты Hashcat в аудите безопасности паролей

Сергей Игоревич Коновалов ¹✉, Павел Александрович Аверин ²,
Дмитрий Андреевич Лысов ³

^{1, 2, 3}Брянский государственный технический университет, Брянск, Россия

¹velvet1way@gmail.com✉, <https://orcid.org/0009-0008-5867-635X>

²stopnotwont@gmail.com, <https://orcid.org/0009-0003-5074-7217>

³lysovdmitriia@gmail.com, <https://orcid.org/0009-0003-9666-7191>

Аннотация. Исследуются возможности утилиты Hashcat как средства для восстановления паролей и анализа защищённости хешей. Рассмотрены теоретические аспекты архитектуры Hashcat, поддерживаемые алгоритмы, виды реализуемых атак, а также особенности аппаратного ускорения. Проведён сравнительный анализ с альтернативными инструментами и обсуждены практические сценарии использования в рамках тестов на проникновение. Делается обоснованный вывод о применимости Hashcat как инструмента оценки эффективности политики паролей в современных условиях.

Ключевые слова: аудит паролей, Hashcat, информационная безопасность, перебор паролей, хеширование, пентестинг, GPU-ускорение, восстановление паролей.

Для цитирования: Коновалов С.И., Аверин П.А., Лысов Д.А. Применение утилиты Hashcat в аудите безопасности паролей // Актуальные проблемы кибербезопасности. Противодействие экстремизму и терроризму в информационной молодежной среде: сборник докладов I межрегиональной научно-практической конференции. – Брянск: БГТУ, 2025. – С. 92 – 94.

Современные системы информационной безопасности сталкиваются с постоянными угрозами, связанными с компрометацией учетных данных. Одним из ключевых методов оценки устойчивости паролей является проведение аудита безопасности с использованием специализированных утилит, таких как Hashcat. Hashcat представляет собой высокопроизводительный инструмент для восстановления паролей, основанный на использовании вычислительных мощностей центральных и графических процессоров. Его применение в пентестинге и анализе защищённости паролей позволяет выявить уязвимые места в системах хранения хешей и оценить эффективность используемой политики аутентификации.

Hashcat появился как ответ на потребность в более гибком и масштабируемом средстве для подбора паролей. Благодаря активному развитию, утилита стала кроссплатформенным решением с поддержкой множества алгоритмов хеширования, включая MD5, SHA-1, SHA-256, bcrypt, NTLM, а также более специализированные форматы, применяемые в корпоративных и облачных средах [1]. Эффективность работы Hashcat во многом определяется способностью использовать аппаратное ускорение через GPU, что значительно повышает скорость вычислений по сравнению с программными средствами, работающими исключительно на CPU.

Одним из центральных аспектов, отличающих Hashcat, является наличие широкого спектра атак, каждая из которых имеет специфическую область применения [2]. Масочная атака позволяет задать шаблон пароля с учетом известных или предполагаемых элементов, например, фиксированной длины или позиции цифр. Словарная атака основывается на использовании заранее подготовленного списка паролей, что особенно эффективно против слабых или часто встречающихся комбинаций. Перестановочная атака и атака на основе правил расширяют словарный подход, позволяя динамически изменять базовые слова согласно заданным правилам, что приближает процесс подбора к реальному поведению пользователей. Комбинаторная атака объединяет элементы различных словарей, а функции смены регистра имитируют человеческие привычки изменять написание слов [3].

Hashcat использует консольный интерфейс с гибкой системой параметров, что делает его удобным для автоматизации и интеграции в скрипты. Команды позволяют точно указать алгоритм хеширования, тип атаки, используемые словари и конфигурационные параметры GPU. Примеры синтаксиса охватывают как простые задачи, так и сложные сценарии перебора, включая одновременное использование нескольких атакующих методов в рамках одного процесса.

Практическое применение Hashcat в процессе пентестинга демонстрирует его эффективность при проверке корпоративных баз данных, извлечённых, например, из Active Directory. Анализ взломанных хешей позволяет аудитору сделать выводы о слабых паролях, распространенных шаблонах и необходимости усиления политики паролей. Кроме того, Hashcat может использоваться в процедурах оценки ущерба после утечки данных, предоставляя информацию о том, насколько быстро злоумышленник может скомпрометировать учетные записи.

По сравнению с альтернативными инструментами, такими как John the Ripper и Cain & Abel, Hashcat демонстрирует превосходство в производительности и масштабируемости, особенно при работе с GPU. John the Ripper, несмотря на широкую поддержку форматов, уступает в скорости и гибкости конфигурации. Cain & Abel, в свою очередь, ориентирован преимущественно на Windows-платформу и не обладает сопоставимым уровнем поддержки современных алгоритмов хеширования.

Тем не менее, Hashcat имеет ограничения, связанные с невозможностью прямого взлома солёных хешей с уникальными солями для каждого пароля без предварительной обработки. Кроме того, эффективность утилиты напрямую зависит от наличия высокопроизводительного оборудования и оптимизации параметров запуска. Это накладывает ограничения на использование Hashcat в условиях ограниченных ресурсов.

Таким образом, Hashcat является мощным инструментом в арсенале специалиста по информационной безопасности, позволяющим не только проводить эффективный аудит паролей, но и строить обоснованные рекомендации по повышению устойчивости систем аутентификации. Теоретическая основа утилиты, подтверждённая многочисленными практическими исследованиями, делает её

важным компонентом современных подходов к обеспечению кибербезопасности. Статистические данные, полученные в ходе тестирования корпоративных баз, свидетельствуют о высокой вероятности успешного подбора слабых паролей в течение короткого времени, что подчеркивает актуальность регулярного проведения аудита с применением инструментов уровня Hashcat.

Список источников

1. Жулев С. А., Позняк И. С. Аудит безопасности Wi-Fi сетей // XLIX Samara Regional Student Scientific Conference. 2023. Т. 1. № S. С. 415-415.
2. Hranický R. et al. Distributed password cracking with BOINC and hashcat // Digital Investigation. 2019. Т. 30. С. 161-172.
3. start [hashcat wiki] // Hashcat URL: <https://hashcat.net/wiki/> (дата обращения: 18.04.2025).

Статья поступила в редакцию 19.04.2025; принята к публикации 10.05.2025

Информация об авторах

Коновалов С.И. – студент кафедры «Системы информационной безопасности», специальность 10.05.03 – Информационная безопасность автоматизированных систем, специализация «Безопасность открытых информационных систем» ФГБОУ ВО «БГТУ».

Аверин П.А. – студент кафедры «Системы информационной безопасности», специальность 10.05.03 – Информационная безопасность автоматизированных систем, специализация «Безопасность открытых информационных систем» ФГБОУ ВО «БГТУ».

Лысов Д.А. – старший преподаватель кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Вклад авторов

Коновалов С.И. – идея, сбор материала, обработка материала, частичное написание статьи (33%).

Аверин П.А. – сбор материала, обработка материала, частичное написание статьи (33%).

Лысов Д.А. – частичное написание статьи, научное редактирование текста (34%).

Конфликт интересов отсутствует.

Научная статья
УДК 004

Технология Secure Enclave как основа аппаратной безопасности в iOS-устройствах: архитектура и принципы защиты данных

Сергей Игоревич Коновалов ^{1✉}, Павел Александрович Аверин ²,
Кирилл Андреевич Седаков ³

^{1, 2, 3}Брянский государственный технический университет, Брянск, Россия

¹velvet1way@gmail.com [✉], <https://orcid.org/0009-0008-5867-635X>

²stopnotwont@gmail.com, <https://orcid.org/0009-0003-5074-7217>

³sekira98@mail.ru, <https://orcid.org/0009-0002-9284-4624>

Аннотация. Рассматривается технология Secure Enclave как ключевой элемент аппаратной архитектуры защиты в устройствах Apple. Описана структура анклава, его изолированность от основной системы, принципы генерации и хранения криптографических ключей, а также методы защиты биометрических данных. Особое внимание уделено механизмам защиты от атак через сторонние каналы и вопросам аппаратной привязки данных к конкретному устройству. Также затронуты примеры известных уязвимостей и направления дальнейшего развития технологии. Secure Enclave рассматривается как эффективный инструмент реализации доверенной среды для выполнения операций с высокой степенью конфиденциальности.

Ключевые слова: Secure Enclave, iOS, аппаратная безопасность, защита данных, криптография, биометрическая аутентификация, Trusted Execution Environment, шифрование AES, UID, Apple.

Для цитирования: Коновалов С.И., Аверин П.А., Седаков К.А. Технология Secure Enclave как основа аппаратной безопасности в iOS-устройствах: архитектура и принципы защиты данных // Актуальные проблемы кибербезопасности. Противодействие экстремизму и терроризму в информационной молодежной среде: сборник докладов I межрегиональной научно-практической конференции. – Брянск: БГТУ, 2025. – С. 95 – 97.

С ростом объема персональных данных, хранимых на мобильных устройствах, обеспечение их безопасности становится ключевой задачей. Пользователи ожидают, что конфиденциальная информация будет надёжно защищена от любых угроз. Безопасность данных всё чаще становится решающим фактором при выборе устройства, поэтому производители стремятся интегрировать в архитектуру своих решений надежные механизмы защиты. Apple реализует комплексный подход к кибербезопасности, внедряя собственные аппаратно-программные технологии. Одним из важнейших компонентов этой системы является Secure Enclave — изолированная подсистема для хранения и обработки чувствительных данных. С момента своего появления в iPhone 5s Secure Enclave стала центральным элементом аппаратной безопасности в экосистеме iOS [1].

Secure Enclave представляет собой выделенную область в системе на кристалле (SoC), физически и логически изолированную от основного процессора. Такая изоляция позволяет минимизировать риски даже в случае компрометации операционной системы или приложения. Подсистема имеет собственный

сопроцессор, защищенное загрузочное ПЗУ, криптографические модули (в том числе AES и генератор случайных чисел), а также доступ к защищённой памяти.

Функционируя в оперативной памяти устройства, Secure Enclave применяет динамически сгенерированный ключ, уникальный для каждой сессии [2]. Все данные в анклаве шифруются с использованием AES и сопровождаются тегами аутентификации. Если при чтении тег не совпадает, система блокирует доступ до перезагрузки. Этот механизм исключает возможность незаметной подмены или считывания данных.

Ключевой компонент подсистемы — сопроцессор на базе микроядра L4. Его архитектура исключает возможность атак через изменение тактовой частоты или другие методы внешнего воздействия. Кроме того, он полностью обособлен от главной ОС и работает только в интересах анклава, что повышает устойчивость к вредоносному ПО.

Одной из практических задач Secure Enclave является обработка биометрических данных (Face ID, Touch ID). Эти данные никогда не покидают устройство, не передаются в облако и хранятся в зашифрованном виде внутри анклава. Процесс аутентификации осуществляется локально путём сравнения текущего сканирования с сохранёнными шаблонами, что обеспечивает безопасность и приватность пользователя. Каждое устройство с Secure Enclave содержит уникальный аппаратный идентификатор (UID), привязывающий зашифрованные данные к конкретному устройству. Даже при физическом извлечении памяти расшифровать её на другом устройстве невозможно. Начиная с чипов A9, добавлены защиты от атак через сторонние каналы — например, анализ энергопотребления или электромагнитного излучения [3].

Несмотря на высокий уровень защиты, Secure Enclave неоднократно становился целью для исследователей безопасности. Например, в 2020 году была обнаружена уязвимость в чипах A10–A11, позволяющая получить доступ к зашифрованной памяти Secure Enclave при наличии физического доступа и применения эксплойта через интерфейс загрузки [4]. Однако даже в этом случае расшифровка данных невозможна без уникального ключа, который генерируется на конкретном устройстве и никогда не покидает его пределы. Это подтверждает одну из ключевых идей архитектуры Secure Enclave — полная невозможность восстановления данных на другом устройстве или в лабораторных условиях, даже если аппаратная оболочка будет частично скомпрометирована.

Apple продолжает развивать архитектуру Secure Enclave, повышая её устойчивость к современным угрозам. В последних версиях (на базе чипов A15 и M-серии) используются более совершенные механизмы защиты, включая улучшенные алгоритмы генерации случайных чисел, аппаратные фьюзы для UID и расширенные функции контроля доступа на уровне микропрошивки. Также наблюдается тенденция интеграции Secure Enclave в общую экосистему доверенных вычислений Apple, включая работу с iCloud Keychain, iMessage и системой восстановления данных. С развитием технологий, связанных с цифровыми удостоверениями, электронными паспортами и правами собственности (например, ключами от автомобилей в Apple Wallet), значение защищённых анклавов будет

только расти. Это требует постоянного совершенствования аппаратных решений, способных обеспечивать доверие в условиях эволюции угроз.

Таким образом, Secure Enclave представляет собой высокозащищённую среду для выполнения операций с конфиденциальной информацией. Его архитектура и принципы работы позволяют достигать высокого уровня безопасности, сочетая аппаратные меры с криптографической защитой. В условиях постоянного роста угроз аппаратная изоляция и такие технологии, как Secure Enclave, становятся критически важными элементами защиты пользовательских данных и укрепляют доверие к мобильным устройствам.

Список источников

1. Zhao S. et al. Sectee: A software-based approach to secure enclave architecture using tee // Proceedings of the 2019 ACM SIGSAC conference on computer and communications security. 2019. С. 1723-1740.
2. Безопасность платформы Apple // Apple Support. URL: <https://support.apple.com/ru-ru/102614> (дата обращения: 05.11.2024).
3. Secure Enclave - Служба поддержки Apple (RU) // Apple Support. URL: <https://support.apple.com/ru-ru/guide/security/sec59b0b31ff/web> (дата обращения: 05.11.2024).
4. Pwnie Awards 2020: наиболее существенные уязвимости и провалы в безопасности // The OpenNET Project. URL: <https://www.opennet.ru/opennews/art.shtml?num=54243> (дата обращения: 15.04.2025).

Статья поступила в редакцию 22.04.2025; принята к публикации 10.05.2025

Информация об авторах

Коновалов С.И. – студент кафедры «Системы информационной безопасности», специальность 10.05.03 – Информационная безопасность автоматизированных систем, специализация «Безопасность открытых информационных систем» ФГБОУ ВО «БГТУ».

Аверин П.А. – студент кафедры «Системы информационной безопасности», специальность 10.05.03 – Информационная безопасность автоматизированных систем, специализация «Безопасность открытых информационных систем» ФГБОУ ВО «БГТУ».

Седаков К.А. – ассистент кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Вклад авторов

Коновалов С.И. – идея, сбор материала, обработка материала, частичное написание статьи (33%).

Аверин П.А. – сбор материала, обработка материала, частичное написание статьи (33%).

Седаков К.А. – частичное написание статьи, научное редактирование текста (34%).

Конфликт интересов отсутствует.

Научная статья
УДК 004.056

Оценка соответствия требованиям приказа ФСТЭК России № 237

Евгения Станиславовна Куцева ^{1✉}, Алексей Владимирович Евдокимов ^{2✉}

^{1,2}Брянский государственный технический университет, Брянск, Россия

¹ kesls2002@gmail.com [✉], <http://orcid.org/0009-0000-4141-737X>

² alekseievdokimov05@gmail.com [✉], <https://orcid.org/0009-0004-4331-1279>

Аннотация. В статье рассматривается оценка соответствия требованиям приказа ФСТЭК №237, который регламентирует защиту информации в области экспортного контроля.

Ключевые слова: ФСТЭК России, экспортный контроль, внешнеэкономическая деятельность, товар.

Для цитирования: Куцева Е.С., Евдокимов А.В. Оценка соответствия требованиям приказа ФСТЭК России № 237 // Актуальные проблемы кибербезопасности и их решения. Противодействие экстремизму и терроризму в информационной молодежной среде: сборник докладов I межрегиональной научно-практической конференции. – Брянск: БГТУ, 2025. – С. 98 – 101.

В современном мире информационная безопасность играет ключевую роль в обеспечении устойчивого развития организаций и государства в целом. Одним из ключевых нормативных документов, регулирующих требования к защите информации, является ФСТЭК №237. Он направлен на предупреждение нарушений при проведении мероприятий по контролю со стороны ФСТЭК России в рамках государственного контроля за соблюдением российского законодательства участниками внешнеэкономической деятельности.

По состоянию на 1 апреля 2024 г. количество российских участников ВЭД, осуществляющих внешнеэкономическую деятельность в отношении товаров, информации, работ, услуг, результатов интеллектуальной деятельности (прав на них), которые могут быть использованы при создании оружия массового поражения, средств его доставки, иных видов вооружения и военной техники либо при подготовке и (или) совершении террористических актов (далее – товары и технологии, подлежащие экспортному контролю), или осуществляющих ввоз в Российскую Федерацию и вывоз из Российской Федерации таких товаров, информации, работ, услуг, результатов интеллектуальной деятельности (прав на них), составляет более 4800.

При анализе правоприменительной практики было проведено 39 плановых выездных, 6 плановых документарных, 3 внеплановые выездные и 7 внеплановых документарных проверок. В общей сложности проведенными 55 проверками было охвачено 1,14% подконтрольных субъектов проверок [1].

Преимущественное использование выездной формы проверок связано с необходимостью в ограниченные сроки качественного и всестороннего рассмот-

рения надлежащего объема документов и информации, требующихся для объективной оценки фактического состояния выполнения проверяемым лицом обязательных требований, являющихся предметом проверки.

По результатам проведенных проверок у 38 российских участников ВЭД (69,1% из числа проверенных) выявлены нарушения требований, установленных законодательством Российской Федерации в области экспортного контроля, из них 12 являются субъектами малого и среднего предпринимательства. Общее количество выявленных нарушений норм, установленных законодательством Российской Федерации, составило 128, из которых 33 являются нарушениями обязательных требований в области экспортного контроля. По 24 нарушениям требований законодательства Российской Федерации в области экспортного контроля, подпадающим под действие Кодекса Российской Федерации об административных правонарушениях, были возбуждены дела об административных правонарушениях, 21 из них были рассмотрены территориальными органами ФСТЭК России, 3 – судами. По результатам рассмотрения дел об административных правонарушениях в 17 случаях на российских участников ВЭД наложены административные штрафы на общую сумму около 7000 тыс. руб. По выявленным нарушениям выдано 46 предписаний об устранении допущенных нарушений, которые были исполнены субъектами проверок в установленные сроки.

Типичными нарушениями обязательных требований, установленных законодательством Российской Федерации в области экспортного контроля, являлись:

- несоблюдение установленного порядка учета внешнеэкономических сделок с товарами, информацией, работами, услугами, результатами интеллектуальной деятельности (правами на них) для целей экспортного контроля согласно статье 23 Федерального закона «Об экспортном контроле» – выявлено 13 нарушений;
- осуществление внешнеэкономических операций с товарами, информацией, работами, услугами, результатами интеллектуальной деятельности (правами на них), на которые в соответствии со статьями 6 и 20 вышеуказанного Федерального закона распространяется экспортный контроль, без лицензий или разрешений – выявлено 10 нарушений.

Также одним из наиболее частых нарушений законодательства РФ в сфере экспортного контроля является несоблюдение правил идентификации контролируемых товаров и технологий (согласно ст. 24 Федерального закона «Об экспортном контроле»).

Необходимо отметить, что в соответствии с Федеральным законом «Об экспортном контроле» полученная в ходе проверок информация является информацией ограниченного доступа и используется исключительно в целях экспортного контроля. В этой связи конкретные примеры нарушений обязательных требований российскими участниками ВЭД не могут быть приведены.

Учитывая, какие нарушения были обнаружены в прошлом году, следует не просто устранить недостатки, а кардинально пересмотреть и усилить систему защиты для будущего года. Требуется организовать многоуровневую систему защиты, способную обнаруживать и устранять ошибки на различных стадиях процесса [2, 3].

Возможно следует включить следующие меры:

1. Обязательная экспертиза всех контрактов специалистом по экспортному контролю до их подписания.
2. Включение в контракты положений, чётко определяющих ответственность сторон за соблюдение требований экспортного контроля.
3. Разработка и использование чек-листов для проверки контрактов на соответствие требованиям экспортного контроля.
4. Усиленная идентификация товаров/услуг:
 - 4.1. Создание и ведение подробного реестра всех товаров, услуг, информации, результатов интеллектуальной деятельности, используемых компанией.
 - 4.2. Регулярное обновление реестра с учетом изменений в законодательстве и номенклатуре.
 - 4.3. Внедрение системы автоматической проверки контрагентов по всем доступным санкционным спискам и базам данных.
 - 4.4. Настройка автоматических уведомлений о выявлении потенциально рискованных контрагентов.
5. Регулярное обновление инструкций с учетом изменений в законодательстве и лучших практик.
6. Обязательное вводное обучение для всех новых сотрудников, участвующих во внешнеэкономической деятельности.
7. Внутренний аудит, направленный на выявление возможностей для улучшения системы экспортного контроля.
8. Анализ полученной информации для выявления системных проблем и принятия корректирующих мер.
9. Чёткое определение действий, которые необходимо предпринять в случае выявления нарушения (например, немедленное уведомление руководства, приостановка сделки, проведение внутреннего расследования). А также назначить ответственных за выполнение каждого действия или пункта действия.
10. Необходимо разработать процесс информирования ФСТЭК о принятых действиях и окончательном решении.

Если сослаться к техническим средствам, можно было бы попытаться внедрить специализированное программное обеспечение для экспортного контроля, которое включало бы различные модули классификации товаров, анализа контрагентов, ведения учёта, генерации отчётов и т.д. [4].

Поскольку сейчас развиваются системы искусственного интеллекта, можно было бы его использовать для автоматизации по обнаружению подозрительных операций (транзакций) и прогнозирования рисков той или иной внешнеэкономической деятельности, а также для автоматического анализа данных.

В данной статье была рассмотрена оценка соответствия требованиям приказа ФСТЭК №237 и выявлено, что программа мер по контролю за участниками внешнеэкономической деятельности требует многоуровневой защиты для повышения эффективности и результативности.

Список источников

1. Приказ ФСТЭК России от 19.12.2024 № 237 «Об утверждении Программы профилактики нарушений обязательных требований, соблюдение которых оценивается при проведении ФСТЭК России мероприятий по контролю в рамках государственного контроля за соблюдением российскими участниками внешнеэкономической деятельности законодательства Российской Федерации в области экспортного контроля, на 2025 год».
2. Галатенко В. А. Основы информационной безопасности. – М.: ИНТУИТ, 2016.
3. Мельников В. П., Клейменов С. А., Петраков А. М. Информационная безопасность и защита информации. – М.: Академия, 2016.
4. Хорев П. Б. Методы и средства защиты информации в компьютерных системах. – М.: Академия, 2016.

Статья поступила в редакцию 19.04.2025; принята к публикации 10.05.2025

Информация об авторах

Куцева Е.С. – студент кафедры «Системы информационной безопасности», направление подготовки 10.03.01 – Информационная безопасность ФГБОУ ВО «БГТУ».

Евдокимов А.В. – студент кафедры «Системы информационной безопасности», направление подготовки 10.05.03 – Информационная безопасность автоматизированных систем ФГБОУ ВО «БГТУ».

Вклад авторов

Куцева Е.С. – частичное написание статьи, сбор материала, обработка материала (50%).

Евдокимов А.В. – частичное написание статьи, обработка материала (50%).

Научный руководитель

Шапенская А.М. – ассистент кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Конфликт интересов отсутствует.

Научная статья

УДК 004.9

Исследование методов защиты пользователей от агрессивного поведения в игровых сообществах и чатах

Маргарита Сергеевна Лукутина^{1✉}, Диана Игоревна Денисеня²,
Дмитрий Андреевич Лысов³

^{1,2,3} Брянский государственный технический университет, Брянск, Россия

¹m.lukutina10@gmail.com✉, <https://orcid.org/0009-0003-7143-9344>

²d.diana1519@gmail.com, <https://orcid.org/0009-0004-6440-7632>

³lysovdmitriia@gmail.com, <https://orcid.org/0009-0003-9666-7191>

Аннотация. Статья посвящена рассмотрению методов защиты пользователей от агрессивного поведения в игровых сообществах и чатах, выявлению проблем этих методов.

Ключевые слова: кибербезопасность, защита пользователей, игровые сообщества, игровые чаты, кибербуллинг.

Для цитирования: Лукутина М.С., Денисеня Д.И., Лысов Д.А. Исследование методов защиты пользователей от агрессивного поведения в игровых сообществах и чатах // Актуальные проблемы кибербезопасности. Противодействие экстремизму и терроризму в информационной молодежной среде: сборник докладов I межрегиональной научно-практической конференции. – Брянск: БГТУ, 2025. – С. 102 – 104.

Многопользовательские онлайн-игры стали неотъемлемой частью цифровой культуры и социальной жизни миллионов пользователей по всему миру. Чаты в играх, голосовые и текстовые, являются важным элементом в таких играх, позволяя игрокам координировать действия, придумывать стратегии и просто общаться между собой. Но с ростом популярности таких проектов возрастает и количество угроз информационной безопасности в процессе общения.

Наиболее популярной из проблем является агрессия в чатах, включая кибербуллинг, оскорбления, манипуляции. Кроме того, злоумышленники всё чаще прибегают к приёмам социальной инженерии, стремясь выведать личные данные, логины и пароли, используя доверие и невнимательность других игроков. Подобные действия могут привести к серьёзным последствиям – от психологических травм до краж аккаунтов и утечек персональных данных.

Согласно отчёту ADL в 2023 году, 76% взрослых игроков (в возрасте 18–45 лет) и 75% подростков (10–17 лет) в многопользовательских онлайн играх сообщили о столкновении с агрессией и буллингом во время игры [1].

А исследование Pew Research Center показало, что 80% подростков из США считают, что травля в онлайн-играх является проблемой для их возраста [2].

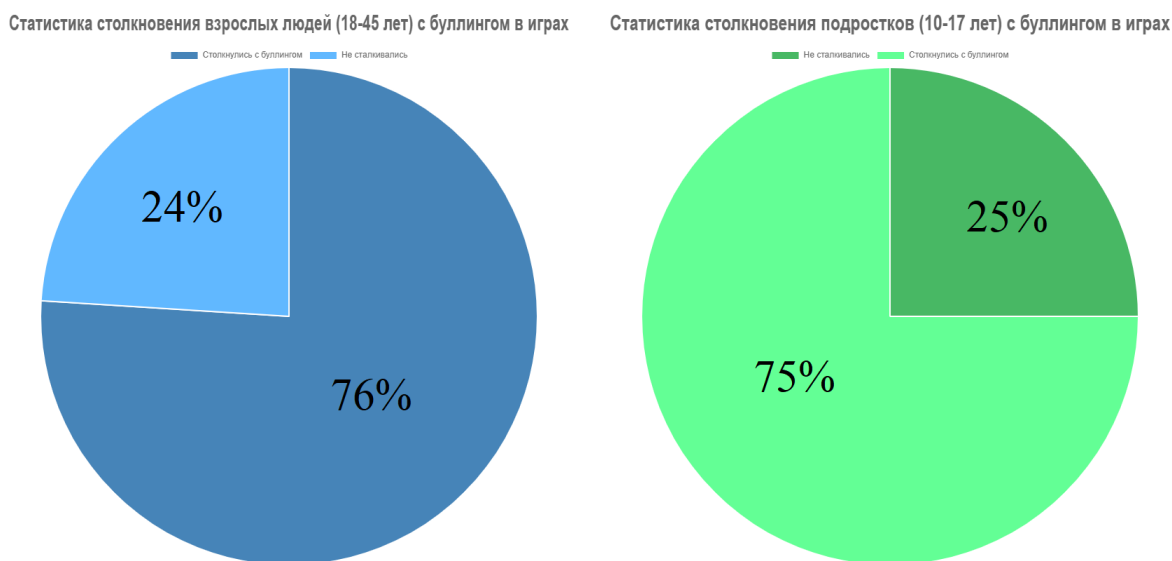


Рис. 1. Процент взрослых и подростков, столкнувшихся с агрессией в онлайн-играх по данным ADL

Для предотвращения опасностей, связанных с игровыми чатами, в играх есть методы защиты, такие как:

- автоматическая модерация: фильтры на нецензурную лексику, обнаружение ключевых слов;
- искусственный интеллект: машинное обучение для распознавания агрессии по лексике, стилю общения, частоте сообщений;
- ручная модерация и система жалоб: возможность сообщить о нарушителе, система временных и постоянных блокировок;
- механизмы самозащиты пользователя: "чёрные списки", отключение чатов, индивидуальные настройки приватности;
- образовательные меры: предупреждения при входе в чат, правила поведения, обучение распознаванию манипуляций.

Однако, все эти варианты не идеальны и имеют ряд проблем, поэтому для эффективной защиты необходимо учитывать особенности каждой из игр и грамотно сочетать эти методы. Наиболее важные проблемы в обеспечении безопасности, существующие на данный момент, несмотря на прогресс в развитии технологий:

- ложные срабатывания автоматических систем: автоматические фильтры и ИИ могут блокировать нейтральные или положительные высказывания, неверно интерпретируя их.
- ограничения масштабируемости: модерация вручную требует значительных ресурсов, а в случае крупных онлайн-игр охватить всю активность пользователей становится невозможным.

- анонимность как фактор безнаказанности: отсутствие реальной идентификации позволяет нарушителям избегать последствий, создавая новые аккаунты после блокировки и продолжая нежелательную активность.

Безопасность пользователей в игровых сообществах и чатах остаётся одной из ключевых задач в сфере информационной безопасности. Для ее решения уже разработаны методы, при правильном сочетании которых можно достичь безопасной и комфортной среды для общения пользователей.

Список источников

1. Hate is No Game: Hate and Harassment in Online Games 2023. URL: <https://www.adl.org/resources/report/hate-no-game-hate-and-harassment-online-games-2023> (дата обращения: 26.04.2025).
2. Teens and Video Games Today. URL: <https://www.pewresearch.org/internet/2024/05/09/teens-and-video-games-today/> (дата обращения: 26.04.2025).
3. Как отвечать на буллинг в онлайн-играх. URL: <https://www.kaspersky-security.ru/2216.html> (дата обращения: 26.04.2025).

Статья поступила в редакцию 27.04.2025; принята к публикации 10.05.2025

Информация об авторах

Лукутина М.С. – студент кафедры «Информатика и программное обеспечение», направление подготовки 09.03.01 – Информатика и вычислительная техника ФГБОУ ВО «БГТУ».

Денисеня Д.И. – студент кафедры «Компьютерные технологии и системы», направление подготовки 09.03.02 – Информационные системы и технологии ФГБОУ ВО «БГТУ».

Лысов Д.А. – старший преподаватель кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Вклад авторов

Лукутина М.С. - идея, сбор материала, обработка материала, частичное написание статьи (50%).

Денисеня Д.И. - идея, сбор материала, обработка материала, частичное написание статьи (10%).

Лысов Д.А. - написание статьи, научное редактирование текста (40%).

Конфликт интересов отсутствует.

Научная статья
УДК 004.056

Сравнительный анализ эффективности технических средств защиты от различных векторов атак социальной инженерии

Дмитрий Андреевич Лысов¹, Федор Евгеньевич Березкин^{2✉}

^{1, 2}Брянский государственный технический университет, Брянск, Россия

¹lysovdmitriia@gmail.com, <https://orcid.org/0009-0003-9666-7191>

²fedor.berezkin32@yandex.ru[✉], <https://orcid.org/0009-0002-0105-7335>

Аннотация. В статье рассматривается проблема человеческого фактора как ключевой уязвимости в корпоративной информационной безопасности, несмотря на развитие сложных технических средств защиты.

Ключевые слова: социальная инженерия, человеческий фактор, информационная безопасность, кибербезопасность, корпоративная безопасность, фишинг, осведомленность в безопасности, комплексная защита, анализ уязвимостей.

Для цитирования: Лысов Д.А., Березкин Ф.Е. Сравнительный анализ эффективности технических средств защиты от различных векторов атак социальной инженерии // Актуальные проблемы кибербезопасности и их решения. Противодействие экстремизму и терроризму в информационной молодежной среде: сборник докладов I межрегиональной научно-практической конференции. – Брянск: БГТУ, 2025. – С. 105 – 110.

Социальная инженерия, как метод атак, направленных на использование человеческих слабостей и психологических уязвимостей для обхода систем безопасности, представляет собой одну из наиболее стойких и динамичных угроз в современном киберпространстве. В отличие от атак, эксплуатирующих исключительно технические недостатки программного или аппаратного обеспечения, социальные инженеры манипулируют людьми, заставляя их раскрыть конфиденциальную информацию, предоставить несанкционированный доступ или совершить иные действия, компрометирующие безопасность [1, 8]. Учитывая центральную роль человеческого фактора, может показаться, что технические средства защиты отходят на второй план. Однако на практике именно они формируют необходимый первый рубеж обороны, способный отсеять значительную часть автоматизированных и массовых атак, а также усложнить действия злоумышленников при более целенаправленных попытках обмана [8]. Эффективность этих технических средств неодинакова и существенно зависит как от конкретного инструмента, так и от вектора атаки социальной инженерии, против которого он применяется. Поэтому сравнительный анализ действенности различных технологических барьеров против многообразных методов социальной инженерии имеет критическое значение для построения эшелонированной и адаптивной системы защиты информации.

Одним из самых распространенных каналов для атак социальной инженерии остается электронная почта, используемая для различных форм фишинга [1,

7]. Для противодействия этому вектору был разработан ряд технических решений, направленных на аутентификацию отправителя и фильтрацию вредоносного контента. Протоколы аутентификации электронной почты, такие как SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail) и DMARC (Domain-based Message Authentication, Reporting, and Conformance), играют важную роль в борьбе со спуфингом – подделкой адреса отправителя [8]. SPF позволяет серверу-получателю проверить, авторизован ли отправляющий почтовый сервер для отправки писем от имени указанного домена. DKIM добавляет цифровую подпись к письму, гарантируя его целостность и подтверждая домен отправителя. DMARC, в свою очередь, объединяет SPF и DKIM, позволяя владельцу домена определить политику обработки писем, не прошедших проверку (например, поместить их в спам или отклонить), и получать отчеты о попытках подделки [8]. Внедрение этих протоколов способно значительно сократить количество фишинговых писем, использующих прямой спуфинг домена, по некоторым оценкам, до 80% [8]. Однако их эффективность не абсолютна. Злоумышленники могут использовать похожие доменные имена (тайпсквоттинг, добавление символов), которые визуально трудно отличить от легитимных, но которые не подпадают под действие DMARC-политики оригинального домена. Кроме того, эти протоколы не защищают от атак, исходящих с уже скомпрометированных легитимных почтовых ящиков, поскольку такие письма проходят все проверки подлинности.

Помимо аутентификации отправителя, современные системы фильтрации почты и шлюзы безопасности используют многоуровневый анализ содержимого писем. Они сканируют текст на наличие характерных для фишинга фраз и признаков, анализируют репутацию ссылок и IP-адресов, проверяют вложения на наличие вредоносного ПО с помощью интегрированных антивирусных движков [2, 8]. Эвристические анализаторы и алгоритмы машинного обучения помогают выявлять новые, ранее неизвестные угрозы. Эти системы достаточно эффективны против массовых фишинговых кампаний и известных вредоносных программ. Тем не менее, злоумышленники постоянно совершенствуют методы обхода фильтров: используют обфускацию кода, шифрование архивов с вредоносным ПО, встраивание вредоносных ссылок в изображения или PDF-документы, а также применяют методы социальной инженерии непосредственно в тексте письма, побуждая пользователя перейти на легитимный, но скомпрометированный сайт или сообщить данные в ответном письме, что сложнее обнаружить автоматическими средствами [1]. Особенно сложной задачей для автоматических фильтров остается выявление особо подготовленных фишинговых атак (spear phishing), где письмо тщательно готовится под конкретного получателя и не содержит явных признаков мошенничества [1, 8].

Антивирусное программное обеспечение является еще одним важным компонентом технической защиты, особенно актуальным при противодействии атакам, направленным на доставку вредоносного ПО через методы социальной инженерии, таким как фишинговые вложения или метод приманки (baiting) с ис-

пользованием зараженных USB-носителей [1, 8]. Современные антивирусы используют комбинацию сигнатурного анализа (для обнаружения известных угроз), эвристического анализа (для выявления подозрительного поведения) и облачных технологий (для оперативного обновления баз и анализа репутации файлов). Их эффективность в обнаружении и блокировке известных вредоносных программ весьма высока, достигая, по некоторым данным, 95% предотвращения заражений через вложения [8]. Однако антивирусы имеют свои ограничения. Они могут быть неэффективны против новейших, так называемых "zero-day" угроз, для которых еще нет сигнатур. Полиморфные и метаморфные вирусы, изменяющие свой код при каждом новом заражении, также представляют сложность для сигнатурного обнаружения. Кроме того, антивирусное ПО практически бесполезно против атак социальной инженерии, не использующих вредоносный код напрямую, например, классического фишинга, направленного на кражу учетных данных через поддельные веб-страницы [2, 8]. Пользователь может сам ввести свои логин и пароль на фишинговом сайте, и антивирус этому не воспрепятствует, если сам сайт не внесен в черные списки.

Учитывая, что значительная часть атак социальной инженерии нацелена на кражу учетных данных, многофакторная аутентификация (MFA), или двухфакторная аутентификация (2FA), стала одним из наиболее эффективных технических барьеров [8]. MFA требует от пользователя предоставить как минимум два различных типа доказательств своей личности для получения доступа к системе. Обычно это комбинация чего-то, что пользователь знает (пароль, PIN-код), чего-то, что он имеет (токен, смарт-карта, код из СМС или приложения-аутентификатора на телефоне), и/или чего-то, чем он является (биометрические данные – отпечаток пальца, распознавание лица) [8]. Даже если злоумышленнику удастся с помощью фишинга или других методов социальной инженерии украсть пароль пользователя, он не сможет получить доступ к системе без второго фактора. Внедрение MFA значительно снижает успешность атак, основанных на компрометации паролей, по некоторым оценкам, на 40% и более [8]. Однако и MFA не является панацеей. Злоумышленники разрабатывают методы обхода MFA, например, через атаки типа "MFA fatigue" (бомбардировка пользователя запросами на подтверждение в надежде, что он по ошибке одобрит один из них), перехват кодов из СМС (через вредоносное ПО на телефоне или SIM-свопинг), или создание фишинговых сайтов, которые не только крадут пароль, но и запрашивают одноразовый код MFA в реальном времени, передавая его на легитимный сервис для авторизации от имени жертвы [1, 7]. Следовательно, хотя MFA существенно повышает планку для атакующих, она не отменяет необходимости бдительности пользователя и использования других мер защиты.

Защита на уровне веб-приложений и браузеров также вносит свой вклад в противодействие социальной инженерии. Веб-аппликационные фаерволы (WAF) анализируют HTTP-трафик между пользователем и веб-сервером, блокируя подозрительные запросы, которые могут указывать на попытки эксплуатации уязвимостей, таких как SQL-инъекции или межсайтовый скриптинг (XSS)

[8]. Хотя основная задача WAF – защита самого веб-приложения, они могут косвенно препятствовать социальной инженерии, предотвращая взлом легитимных сайтов, которые могли бы быть использованы для размещения фишинговых страниц или распространения вредоносного ПО. Согласно некоторым источникам, WAF способны блокировать до 90% атак через веб-интерфейсы [8]. Современные веб-браузеры (Chrome, Firefox, Яндекс.Браузер и др.) также имеют встроенные механизмы защиты от фишинга и вредоносных сайтов, часто используя базы данных небезопасных ресурсов, такие как Google Safe Browsing [8]. При попытке перехода на известный фишинговый или вредоносный сайт браузер выводит предупреждение или блокирует доступ. Эффективность этой защиты зависит от своевременности обновления баз и способности обнаруживать новые, еще не внесенные в списки угрозы. Злоумышленники используют различные техники для обхода этих фильтров, например, быстро меняющиеся домены, множественные редиректы или методы клоакинга, когда пользователю и сканеру безопасности показывается разное содержимое страницы. Настройки приватности в браузерах, ограничивающие отслеживание и сбор данных, также могут косвенно снижать риски, уменьшая объем информации, доступной злоумышленникам для подготовки таргетированных атак [8].

Однако существует ряд векторов атак социальной инженерии, против которых существующие технические средства защиты оказываются малоэффективными или практически бессильными. Голосовой фишинг (вишинг) и СМС-фишинг (смишинг) являются яркими примерами [1, 5]. Хотя существуют мобильные приложения для блокировки спам-звонков и СМС, они часто опираются на пользовательские базы данных и могут пропускать новые номера или ошибочно блокировать легитимные сообщения. Основная линия защиты от вишинга и смишинга лежит в плоскости осведомленности и критического мышления самого пользователя, его способности распознать манипулятивные тактики и не поддаваться давлению [5, 8]. Аналогичная ситуация складывается с атаками, использующими новейшие технологии искусственного интеллекта и дипфейки [3, 8]. Автоматически распознать высококачественный синтезированный голос или дипфейк-видео существующими техническими средствами крайне сложно. Хотя ведутся разработки в области обнаружения дипфейков, общедоступных и надежных инструментов пока нет, и защита от таких атак в значительной степени полагается на бдительность людей и проверку информации по альтернативным каналам связи [8]. Атаки с использованием поддельных QR-кодов также представляют сложность для превентивной технической защиты [3]. Сам по себе QR-код – это лишь графическое представление данных (обычно ссылки), и технически заблокировать его сканирование практически невозможно. Защита здесь смещается на уровень устройства, которое должно проанализировать ссылку после сканирования и определить, является ли она вредоносной, что возвращает нас к проблеме эффективности веб-фильтров и антивирусной защиты на мобильных устройствах [3, 8]. Физические методы, такие как тейлгейтинг или шолдерсерфинг, по своей природе обходят большинство цифровых средств защиты, и

противодействие им требует физических мер безопасности (турникеты, системы видеонаблюдения) и внимательности сотрудников [1, 3].

Таким образом, сравнительный анализ эффективности технических средств защиты показывает, что ни одно из них не является универсальным решением против всего спектра атак социальной инженерии. Каждое средство имеет свою нишу и свои ограничения. Протоколы аутентификации почты (SPF, DKIM, DMARC) эффективны против прямого спуфинга, но уязвимы для атак с похожих доменов или скомпрометированных аккаунтов. Почтовые фильтры и антивирусы хорошо справляются с массовыми угрозами и известным вредоносным ПО, но могут пропускать таргетированные атаки и новейшие угрозы. Многофакторная аутентификация является мощным барьером против кражи учетных данных, но не защищает от компрометации самого второго фактора или от атак, не связанных с несанкционированным входом. Веб-фильтры и WAF обеспечивают защиту на уровне браузера и сервера, но не могут полностью исключить переход пользователя на вредоносный сайт или загрузку вредоносного файла. Против таких векторов, как вишинг, смишинг, атаки с использованием дипфейков или физические методы, эффективность существующих технических средств весьма ограничена, и основная нагрузка ложится на человека. Это подчеркивает фундаментальную истину: технология сама по себе не может полностью решить проблему, порожденную человеческой психологией. Максимальная эффективность достигается только при использовании многоуровневого подхода (defense-in-depth), где различные технические средства дополняют друг друга, перекрывая слабые стороны каждого отдельного компонента. Однако даже самый совершенный набор технических инструментов должен быть обязательно подкреплён организационными мерами, четкими политиками безопасности и, что самое важное, постоянным обучением и повышением осведомленности пользователей, которые остаются последним и зачастую решающим рубежом обороны от изощренных атак социальной инженерии.

Список источников

1. Habr: Разнообразный арсенал социальной инженерии: виды атак и способы их предотвращения. URL: <https://habr.com/ru/companies/first/articles/670766/> (дата обращения: 10.04.2025).
2. Kaspersky Resource Center: Как избежать атаки с использованием социальной инженерии. URL: <https://www.kaspersky.ru/resource-center/threats/how-to-avoid-social-engineering-attacks> (дата обращения: 16.04.2025).
3. Arxiv: Social Engineering Attacks and Defenses in the Physical World vs. Cyberspace: A Contrast Study. URL: <https://arxiv.org/abs/2203.04813> (дата обращения: 10.04.2025).
4. Wikipedia: Кевин Дэвид Митник. URL: https://ru.wikipedia.org/wiki/Митник,_Кевин (дата обращения: 10.04.2025).
5. Five internet and cell phone frauds to LOOK OUT for in Russia. URL: <https://www.rbth.com/lifestyle/332484-5-internet-and-cell-phone-frauds-russia> (дата обращения: 10.04.2025).

6. Number of fraudulent phone numbers identified due to unauthorized financial transactions in Russia in 2023, by type. URL: <https://www.statista.com/statistics/1059117/blocked-phishing-phone-numbers-by-type-russia/> (дата обращения: 10.04.2025).

7. Актуальные киберугрозы: III квартал 2023 года. URL: <https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2023-q3/> (дата обращения: 10.04.2025).

8. MTUCI InfoSec Start: Социальная инженерия: методы атак и защиты. URL: <https://infosec-start-mtuci.notion.site/3-7d563b53513f4e3c8800a00a7ee6cd46#df56b20ed09d44e49171a056af467502> (дата обращения: 10.04.2025).

Статья поступила в редакцию 22.04.2025; принята к публикации 10.05.2025

Информация об авторах

Лысов Д.А. – старший преподаватель кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Березкин Ф.Е. – студент кафедры «Системы информационной безопасности», направление подготовки 10.05.03 – Информационная безопасность автоматизированных систем ФГБОУ ВО «БГТУ».

Вклад авторов

Лысов Д.А. – частичное написание статьи, научное редактирование текста (50%).

Березкин Ф.Е. – идея, сбор материала, обработка материала, частичное написание статьи (50%).

Конфликт интересов отсутствует.

Научная статья

УДК 004.056:159.9

Человеческий фактор как ключевая уязвимость: анализ эффективности комплексных мер защиты от социальной инженерии в корпоративной среде

Дмитрий Андреевич Лысов¹, Федор Евгеньевич Березкин^{2✉}

^{1, 2}Брянский государственный технический университет, Брянск, Россия

¹lysovdmitriia@gmail.com, <https://orcid.org/0009-0003-9666-7191>

²fedor.berezkin32@yandex.ru✉, <https://orcid.org/0009-0002-0105-7335>

Аннотация. В статье рассматривается проблема человеческого фактора как ключевой уязвимости в корпоративной информационной безопасности, несмотря на развитие сложных технических средств защиты.

Ключевые слова: социальная инженерия, человеческий фактор, информационная безопасность, кибербезопасность, корпоративная безопасность, фишинг, осведомленность в безопасности, комплексная защита, анализ уязвимостей.

Для цитирования: Лысов Д.А., Березкин Ф.Е. Человеческий фактор как ключевая уязвимость: анализ эффективности комплексных мер защиты от социальной инженерии в корпоративной среде // Актуальные проблемы кибербезопасности и их решения. Противодействие экстремизму и терроризму в информационной молодежной среде: сборник докладов I межрегиональной научно-практической конференции. – Брянск: БГТУ, 2025. – С. 111 – 116.

Статистика из года в год доказывает, что человек является самым уязвимым звеном в любой системе защиты, даже при учёте должного отношения к другим аспектам построения системы защиты. Технологические средства контроля, такие как системы обнаружения вторжений, многоуровневые межсетевые экраны и криптографические механизмы, могут быть нейтрализованы не вследствие их технического несовершенства, а посредством воздействия на персонал с использованием методов социальной инженерии [2]. Данный подход направлен не на технологические компоненты, а на психологические аспекты. Эксплуатируются такие особенности человеческого поведения, как склонность к доверию, особенно по отношению к авторитетным фигурам или лицам, воспринимаемым как часть референтной группы; эмоциональные реакции, включая страх, любопытство или альтруистические побуждения; а также когнитивные искажения, препятствующие критической оценке ситуации [1, 8]. Вследствие этого индивиды неосознанно способствуют действиям злоумышленников, предоставляя им несанкционированный доступ к корпоративным информационным ресурсам.

Суть атак, опирающихся на методы социальной инженерии, заключается в эксплуатации человеческого доверия и невнимательности. Злоумышленники, применяющие данные методы, осведомлены об особенностях человеческой психологии, в частности о склонности людей к автоматическому поведению, следованию социальным нормам и подверженности влиянию факторов срочности или

предполагаемой важности запроса. Это обуславливает эффективность атак социальной инженерии даже в отношении сотрудников, обладающих достаточным уровнем технической грамотности [1]. Пример Кевина Митника, известного специалиста по компьютерной безопасности, чья ранняя деятельность была связана с хакингом, иллюстрирует превалирование манипулятивных техник и установления доверительных отношений над глубокими техническими знаниями для достижения целей несанкционированного доступа [4]. Данный опыт подчеркивает недопустимость игнорирования человеческого фактора при построении систем защиты. Для обеспечения высокого уровня безопасности организациям необходимо не только инвестировать в технологические решения, но и анализировать причины уязвимости персонала к манипулятивным воздействиям, разрабатывая на этой основе комплексные контрмеры, ориентированные на человеческий элемент.

Методология, применяемая социальными инженерами, включает разнообразные техники и постоянно совершенствуется. Наиболее распространенной техникой остается фишинг – действия, направленные на получение конфиденциальной информации или побуждение пользователя к установке вредоносного программного обеспечения посредством использования поддельных электронных писем, сообщений в системах обмена мгновенными сообщениями или фальсифицированных веб-ресурсов [1, 7]. Типичной реализацией являются массовые рассылки, имитирующие легитимные сообщения от финансовых учреждений, онлайн-сервисов или внутренних подразделений организации [2]. Вместе с тем, существуют более таргетированные варианты. Целевой фишинг (spear phishing) представляет собой атаку, специально подготовленную для конкретного индивида или ограниченной группы лиц. Предварительно осуществляется сбор информации о потенциальных жертвах из открытых источников, включая социальные сети, с целью максимальной персонализации сообщения и повышения его убедительности. Особую опасность представляет "китобойный" фишинг (whale phishing), объектами которого являются руководители высшего звена и ключевые сотрудники, обладающие привилегированным доступом к критически важной информации или финансовым активам [1].

Помимо классического фишинга, реализуемого через электронную почту, активно задействуются иные каналы коммуникации. Вишинг (голосовой фишинг) представляет собой мошеннические действия с использованием телефонной связи, в ходе которых злоумышленник, выдавая себя за представителя банка, службы технической поддержки или правоохранительных органов, пытается путем психологического давления получить конфиденциальные данные или склонить жертву к совершению определенных действий [5, 6]. Смишинг использует аналогичную тактику посредством SMS-сообщений, часто содержащих вредоносные гиперссылки или указания срочно связаться по предоставленному номеру. Претекстинг заключается в создании сложного вымышленного сценария (предлога) для легитимизации запроса на получение конфиденциальной информации [8]. Атакующий может конструировать целую историю для снижения бдительности цели. Техника бейтинга эксплуатирует любопытство или корыстные

мотивы: потенциальной жертве предлагается зараженный USB-носитель с привлекательной маркировкой или возможность загрузки пиратского программного обеспечения, содержащего вредоносный код [1]. Физические методы также применяются: тейлгейтинг подразумевает проход через систему контроля доступа вслед за авторизованным сотрудником, а подглядывание через плечо (shoulder surfing) используется для кражи паролей [1, 3]. Отмечается появление новых угроз, связанных с развитием технологий: распространение фальшивых QR-кодов, перенаправляющих на фишинговые ресурсы, и потенциальное использование систем искусственного интеллекта для генерации высокореалистичных поддельных сообщений, включая аудио- и видеодипфейки, что существенно усложняет задачу идентификации обмана [3, 8].

Учитывая ограниченность исключительно технологических подходов к решению проблемы человеческой уязвимости, необходима реализация комплексной, эшелонированной стратегии защиты. Технические средства контроля, безусловно, формируют базовый уровень обороны. Современные системы фильтрации электронной почты, использующие стандарты SPF, DKIM, DMARC для аутентификации отправителя, антивирусные решения с обновляемыми сигнатурными базами и межсетевые экраны уровня веб-приложений (WAF), обеспечивающие защиту от атак на веб-сервисы, способны автоматически детектировать и блокировать значительную долю известных угроз и массовых фишинговых кампаний [8]. Применение многофакторной аутентификации (MFA), требующей для доступа помимо пароля предоставления дополнительного фактора (например, кода из SMS, биометрических данных или аппаратного токена), значительно повышает уровень защиты учетных записей даже в случае компрометации пароля [8]. Однако следует признать, что ни одна технология не обеспечивает абсолютной гарантии. Наиболее совершенные фильтры могут пропустить тщательно замаскированное фишинговое сообщение, а MFA неэффективна, если пользователь добровольно передает одноразовый код злоумышленнику под влиянием обмана [2]. В связи с этим укрепление осведомленности и бдительности персонала ("человеческого брандмауэра") приобретает не меньшую, а потенциально и большую значимость.

В этом контексте приоритетными становятся организационные меры и систематическая работа с персоналом. В организации должны быть разработаны, внедрены и доведены до сведения всех сотрудников четкие, доступные для понимания и практически выполнимые политики информационной безопасности. Данные политики должны регламентировать ключевые аспекты работы с информацией: правила формирования и хранения аутентификационных данных, процедуры использования корпоративной электронной почты и доступа в Интернет, алгоритмы действий при обнаружении подозрительных сообщений или запросов, правила обращения со съемными носителями информации и мобильными устройствами [2]. Эффективность формализованных политик напрямую зависит от их знания, понимания и соблюдения персоналом. Следовательно, ключевым элементом становится непрерывное обучение и повышение уровня осведомлен-

ности. Регулярное проведение тренингов, семинаров, распространение информационных материалов должны знакомить сотрудников с актуальными примерами атак социальной инженерии, разъяснять используемые злоумышленниками психологические приемы, обучать идентификации характерных признаков фишинга и других видов мошенничества, и, что наиболее важно, формировать устойчивые навыки безопасного поведения в цифровой среде [1, 2].

Эффективным инструментом для оценки и закрепления знаний являются симуляционные фишинговые атаки. Проведение таких контролируемых имитаций позволяет объективно оценить уровень бдительности сотрудников, идентифицировать уязвимые области и адаптировать программы обучения, акцентируя внимание на проблемных аспектах [1, 8]. Важно, чтобы подобные симуляции рассматривались как образовательный инструмент, а не как средство наказания. Критически важно также способствовать развитию общей культуры безопасности в организации. Это предполагает создание среды, в которой сотрудники осознают персональную ответственность за защиту корпоративной информации, не испытывают затруднений при обращении за разъяснениями в случае возникновения сомнений и оперативно информируют службу безопасности о любых подозрительных инцидентах без опасения негативных последствий за возможные ошибки. Максимальная эффективность защиты достигается при синергии технических и человеческих факторов: технические средства блокируют основной объем угроз, а подготовленный и мотивированный персонал выступает в качестве последнего рубежа обороны, способного распознать и нейтрализовать атаки, преодолевшие технологические барьеры [2, 8].

Тем не менее, построение и поддержание такой комплексной системы защиты является непрерывным и ресурсоемким процессом. Угрозы социальной инженерии постоянно эволюционируют: разрабатываются новые схемы атак, используются актуальные информационные поводы (например, глобальные события) для повышения правдоподобности легенд, тактики адаптируются под новые технологические реалии [7]. Это требует от подразделений информационной безопасности постоянного мониторинга ландшафта угроз и своевременной актуализации как технических средств защиты, так и программ обучения персонала. Распространение гибридных и удаленных форматов работы также создает дополнительные вызовы: сотрудники чаще используют личные устройства и домашние сети с потенциально более низким уровнем защищенности, а ограниченность прямого взаимодействия с коллегами и руководством может снижать эффективность неформального контроля и обсуждения подозрительных ситуаций [3]. Кроме того, нельзя игнорировать такие факторы, как текучесть кадров, требующая организации обучения для новых сотрудников, и потенциальный эффект "усталости от безопасности" у персонала с большим стажем работы, что может привести к снижению уровня бдительности. Все перечисленное обуславливает необходимость постоянных, планомерных усилий по поддержанию требуемого уровня защищенности.

Подводя итог, можно констатировать, что человеческий фактор является и будет оставаться критической уязвимостью в системах корпоративной информационной безопасности. Социальная инженерия представляет собой преимущественно психологическую, а не техническую атаку, эффективно использующую особенности человеческого поведения для обхода наиболее совершенных технологических средств защиты. Следовательно, опора исключительно на технические решения оставляет значительные возможности для действий злоумышленников. Надежная оборона требует комплексного подхода, гармонично интегрирующего современные технические средства защиты с непрерывным, целенаправленным обучением персонала и формированием осознанной культуры безопасности на уровне всей организации. Технические меры, включая MFA и интеллектуальные системы фильтрации, являются важными компонентами, однако их эффективность должна подкрепляться четкими организационными политиками и, прежде всего, высоким уровнем осведомленности и бдительности каждого сотрудника. Только непрерывное совершенствование всех элементов этого многоуровневого подхода, его адаптация к динамично меняющимся угрозам и глубокое понимание психологии человеческого поведения позволят организациям минимизировать риски и эффективно противостоять атакам, нацеленным на наиболее уязвимое звено – человека.

Список источников

1. Habr: Разнообразный арсенал социальной инженерии: виды атак и способы их предотвращения. URL: <https://habr.com/ru/companies/first/articles/670766/> (дата обращения: 11.04.2025).
2. Kaspersky Resource Center: Как избежать атаки с использованием социальной инженерии. URL: <https://www.kaspersky.ru/resource-center/threats/how-to-avoid-social-engineering-attacks> (дата обращения: 11.04.2025).
3. Arxiv: Social Engineering Attacks and Defenses in the Physical World vs. Cyberspace: A Contrast Study. URL: <https://arxiv.org/abs/2203.04813> (дата обращения: 11.04.2025).
4. Wikipedia: Кевин Дэвид Митник. URL: https://ru.wikipedia.org/wiki/Митник,_Кевин (дата обращения: 11.04.2025).
5. Five internet and cell phone frauds to LOOK OUT for in Russia. URL: <https://www.rbth.com/lifestyle/332484-5-internet-and-cell-phone-frauds-russia> (дата обращения: 11.04.2025).
6. Number of fraudulent phone numbers identified due to unauthorized financial transactions in Russia in 2023, by type. URL: <https://www.statista.com/statistics/1059117/blocked-phishing-phone-numbers-by-type-russia/> (дата обращения: 11.04.2025).
7. Актуальные киберугрозы: III квартал 2023 года. URL: <https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2023-q3/> (дата обращения: 11.04.2025).
8. MTUCI InfoSec Start: Социальная инженерия: методы атак и защиты. URL: <https://infosec-start-mtuci.notion.site/3->

[7d563b53513f4e3c8800a00a7ee6cd46#df56b20ed09d44e49171a056af467502](https://doi.org/10.26907/2542-0408.2025.7d563b53513f4e3c8800a00a7ee6cd46#df56b20ed09d44e49171a056af467502) (дата обращения: 11.04.2025).

Статья поступила в редакцию 22.04.2025; принята к публикации 10.05.2025

Информация об авторах

Лысов Д.А. – старший преподаватель кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Березкин Ф.Е. – студент кафедры «Системы информационной безопасности», направление подготовки 10.05.03 – Информационная безопасность автоматизированных систем ФГБОУ ВО «БГТУ».

Вклад авторов

Лысов Д.А. – частичное написание статьи, научное редактирование текста (50%).

Березкин Ф.Е. – идея, сбор материала, обработка материала, частичное написание статьи (50%).

Конфликт интересов отсутствует.

Научная статья

УДК 004

Идентификация и эксплуатация уязвимостей в информационных системах

Роман Александрович Мамичев¹, Сергей Игоревич Коновалов^{2✉},

Павел Александрович Аверин³

^{1, 2, 3}Брянский государственный технический университет, Брянск, Россия

¹mami4ev.roman@yandex.ru, <https://orcid.org/0009-0004-5539-8746>

²velvet1way@gmail.com✉, <https://orcid.org/0009-0008-5867-635X>

³stopnotwont@gmail.com, <https://orcid.org/0009-0003-5074-7217>

Аннотация. Рассматриваются методы идентификации и эксплуатации уязвимостей в информационных системах, а также их влияние на безопасность предприятий. Описываются методы, такие как статический и динамический анализ кода, сканирование уязвимостей, проведение аудита и использование фреймворков для эксплуатации уязвимостей. Рассматриваются популярные инструменты для тестирования безопасности, такие как Metasploit, Burp Suite, Nessus, и OpenVAS. Статья подчеркивает необходимость комплексного подхода к идентификации уязвимостей и разработке стратегий реагирования на инциденты безопасности для защиты информационных систем от атак.

Ключевые слова: идентификация уязвимостей, эксплуатация уязвимостей, кибератаки, безопасность информационных систем, статический анализ кода, динамический анализ, сканеры уязвимостей, аудит, Metasploit, Burp Suite, Nessus, OpenVAS.

Для цитирования: Мамичев Р.А., Коновалов С.И., Аверин П.А. Идентификация и эксплуатация уязвимостей в информационных системах // Актуальные проблемы кибербезопасности. Противодействие экстремизму и терроризму в информационной молодежной среде: сборник докладов I межрегиональной научно-практической конференции. – Брянск: БГТУ, 2025. – С. 117 – 120.

С каждым годом количество кибератак, использующих уязвимости в программном обеспечении, продолжает расти. Злоумышленники активно используют эти уязвимости для получения несанкционированного доступа к информационным системам, похищения данных и нарушений нормальной работы предприятий [1]. В связи с этим, одной из ключевых задач службы безопасности становится своевременная идентификация и нейтрализация угроз, связанных с уязвимостями, что требует постоянного совершенствования методов защиты.

Статистика за второй квартал 2024 года показывает, что было публично зарегистрировано 768 случаев эксплуатации уязвимостей. Этот показатель превысил данные за второй квартал 2023 года на 20%, подобных случаев насчитывалось 639 [2]. Проанализировав данные, можно заметить динамику роста случаев эксплуатации уязвимостей, это напрямую связано с публикацией крупных отчётов по кибербезопасности в конце года. Руководителям службы безопасности следует уделить особое внимание разработке политики ИБ на предприятиях, а именно пунктов, затрагивающих оперативное реагирование на инциденты безопасности и угрозы.

Идентификация уязвимости – выявление компонента в информационной системе, подверженного особому риску.

Метод статистического анализа кода включает анализ исходного кода без его выполнения, что позволяет обнаружить потенциальные уязвимости на ранних этапах разработки. Этот метод помогает выявить ошибки, связанные с логикой программы, синтаксисом и структурой данных, но не может обнаружить уязвимости, связанные с конфигурацией или поведением программы в реальных условиях эксплуатации. Инструменты, такие как «SonarQube», «Fortify Static» и «Code Analyzer», анализируют весь код, включая неактивные участки, что позволяет найти дефекты безопасности, которые трудно выявить другими методами, но могут генерировать ложные срабатывания.

Метод динамического анализа кода заключается в проверке работы приложения в процессе его выполнения, что позволяет обнаружить уязвимости, которые проявляются только в реальных условиях эксплуатации. Этот метод полезен для выявления проблем с конфигурацией, таких как неправильные настройки сервера или базы данных, а также уязвимостей, которые связаны с взаимодействием приложения с внешними системами. Инструменты, такие как «Burp Suite» и «OWASP ZAP», позволяют имитировать атаки на приложение и тестировать его безопасность в реальном времени. Однако динамический анализ требует выполнения программы, что делает его более ресурсоемким и ограничивает охват тестируемых сценариев.

Метод сканирования уязвимостей используется для автоматической проверки сети и систем на наличие известных уязвимостей, которые могут быть использованы злоумышленниками для несанкционированного доступа. Сканеры уязвимостей проводят анализ программного обеспечения, операционных систем и сетевых устройств, выявляя проблемы, такие как неправильные настройки или устаревшее ПО. Эти инструменты используют базы данных с известными уязвимостями (например, CVE) для поиска угроз и предоставляют отчеты с рекомендациями по их устранению. Работа сканера, как правило, включает в себя следующие пункты:

1. Сканирование открытых портов, обнаружение запущенных сервисов.
2. Выявление уязвимости.
3. Проведение оценки безопасности.
4. Создание отчёта.

К популярным инструментам сетевого сканирования можно отнести: «Nessus», «OpenVAS», «Nmap».

Метод проведения аудита также является эффективной мерой при идентификации уязвимости. Он предполагает ручную проверку кода, конфигураций и системных настроек опытными специалистами для выявления уязвимостей, которые могут быть не замечены автоматическими инструментами. Аудит позволяет детально анализировать архитектуру приложения и инфраструктуры, а также оценить соблюдение стандартов безопасности. Этот метод эффективен для обнаружения сложных и скрытых уязвимостей, таких как ошибки в логике приложения или неправильные настройки безопасности, которые могут не быть

включены в базы данных сканеров уязвимостей. Однако у него есть и недостатки: аудит требует значительных временных затрат и высокой квалификации специалистов, что делает его более ресурсоёмким и затратным по сравнению с автоматизированными методами.

Эксплуатация уязвимости – процесс использования уязвимости для получения несанкционированного доступа к информационной системе [3]. Эксплуатация уязвимостей также совершается с помощью разных методов.

Использование фреймворков позволяет протестировать ПО на безопасность. Metasploit Framework это один из самых популярных инструментов, предоставляющий обширную базу данных эксплойтов и модули для автоматизации процессов эксплуатации уязвимостей [4]. Он позволяет исследовать и использовать уязвимости в приложениях, операционных системах и сетевых сервисах, что делает его незаменимым для профессионалов в области безопасности при проведении тестов на проникновение.

Общие типы эксплуатации включают в себя: использование уязвимостей в SQL-запросах для получения доступа к базе данных, внедрение вредоносного JavaScript-кода на веб-страницу, который выполняется в браузере пользователя, переполнение буфера, использование уязвимости для выполнения произвольного кода на удаленной системе, атаки типа «отказ в обслуживании» (DDoS), использование методов социальной инженерии.

Таким образом, идентификация и эксплуатация уязвимостей являются важными аспектами работы специалистов информационной безопасности, поскольку эти процессы помогают разработать план реагирования на инциденты, связанные с несанкционированным доступом (НСД) к информационной системе. Идентификация уязвимостей включает в себя поиск слабых мест в системе с использованием различных методов, таких как сканирование уязвимостей, анализ кода и аудит конфигураций. Специалист должен уметь выявить потенциальные уязвимости, которые могут быть использованы злоумышленниками для проникновения в систему. Эксплуатация уязвимостей предполагает использование таких инструментов, как Metasploit или Burp Suite, для проверки уязвимостей в реальных условиях, что позволяет протестировать систему на устойчивость к атакам и выявить возможные последствия эксплуатации этих слабых мест. Для эффективной защиты системы специалист должен не только уметь обнаруживать уязвимости, но и оценивать риски, а также разрабатывать план действий в случае инцидентов, чтобы минимизировать ущерб от НСД и обеспечить безопасность информационной системы.

Список источников

1. Скоробогатов Р. Г. Идентификация уязвимостей, анализ рисков, разработка рекомендаций по устранению уязвимостей и обеспечению безопасности активов организации // Современные наука и образование: достижения и перспективы развития: сборник материалов XXX международной очно-заочной научно-практической конференции. В 4 т. Т. 3. 7 июня, 2023. – М.: Изд-во НИЦ «Империя», 2023.– С. 126.

2. Анализ случаев эксплуатации уязвимостей за 2024 год. URL: VulnCheck.ru (дата обращения: 13.02.2025).

3. ГОСТ Р 56545-2015. Защита информации. Уязвимости информационных систем. Правила описания уязвимостей.

4. Metasploit Documentation // Metasploit. URL: <https://docs.metasploit.com/> (дата обращения: 26.03.2025).

Статья поступила в редакцию 22.04.2025; принята к публикации 10.05.2025

Информация об авторах

Мамичев Р.А. – студент кафедры «Системы информационной безопасности», направление подготовки 10.03.01 – Информационная безопасность ФГБОУ ВО «БГТУ».

Коновалов С.И. – студент кафедры «Системы информационной безопасности», специальность 10.05.03 – Информационная безопасность автоматизированных систем, специализация «Безопасность открытых информационных систем», ФГБОУ ВО «БГТУ».

Аверин П.А. – студент кафедры «Системы информационной безопасности», специальность 10.05.03 – Информационная безопасность автоматизированных систем, специализация «Безопасность открытых информационных систем», ФГБОУ ВО «БГТУ».

Вклад авторов

Мамичев Р.А. – частичное написание статьи, сбор материала, обработка материала (33%).

Коновалов С.И. – идея, сбор материала, обработка материала, частичное написание статьи (33%).

Аверин П.А. – сбор материала, обработка материала, частичное написание статьи (34%).

Научный руководитель

Шапенская А.М. – ассистент кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Конфликт интересов отсутствует.

Научная статья
УДК 004:056

**Анализ актуальности разработки платформ для работы
с нормативно-правовыми актами как инструмента
для комплексного подхода к соблюдению отраслевых требований
в вопросах защиты информации**

**Карина Владимировна Морозова^{1✉}, Павел Дмитриевич Горелов²,
Диана Игоревна Денисеня³, Дмитрий Андреевич Лысов⁴**
^{1,2,3,4} Брянский государственный технический университет, Брянск, Россия
¹marus.korotkova@yandex.ru ✉, <http://orcid.org/0009-0007-2396-4469>
²pashkayr@yandex.ru, <https://orcid.org/0009-0008-7487-6124>
³d.diana1519@gmail.com, <https://orcid.org/0009-0004-6440-7632>
⁴lysovdmitriia@gmail.com, <https://orcid.org/0009-0003-9666-7191>

Аннотация. В статье анализируется актуальность разработки платформ для работы с нормативно-правовыми актами в области защиты информации. Рассмотрены современные вызовы, включая увеличение объема законодательства, частые изменения и отсутствие специализированных инструментов в существующих решениях. Выделена практическая значимость разработки, направленной на минимизацию рисков и повышение эффективности управления нормативной базой.

Ключевые слова: информационная безопасность, нормативно-правовые акты, автоматизация анализа, соблюдение требований, законодательство.

Для цитирования: Морозова К.В., Горелов П.Д., Денисеня Д.И., Лысов Д.А. Анализ актуальности разработки платформ для работы с нормативно-правовыми актами как инструмента для комплексного подхода к соблюдению отраслевых требований в вопросах защиты информации // Актуальные проблемы кибербезопасности. Противодействие экстремизму и терроризму в информационной молодежной среде: сборник докладов I межрегиональной научно-практической конференции. – Брянск: БГТУ, 2025. – С. 121 – 124.

Современные требования информационной безопасности и значительные изменения в законодательной базе подчеркивают необходимость разработки специализированных инструментов, позволяющих организациям оперативно адаптироваться к нормативным изменениям и эффективно интегрировать требования в свои процессы. Это связано с необходимостью адаптации законодательства к новым вызовам цифровой трансформации, росту числа кибератак и усилению требований к защите критической информационной инфраструктуры (КИИ).

Согласно исследованию экспертно-аналитического центра ГК InfoWatch от 08.02.2024, за период с 2021 по 2023 годы было принято 748 нормативно-правовых актов, регулирующих вопросы информационной безопасности, обработки персональных данных, IT и цифровой экономики. В 2023 году было принято 187 документов, касающихся регулирования ИБ, что на 31% меньше, чем в 2022 году.

Особенно выделяются нормативные акты, регулирующие персональные данные, доля которых составила 25% от всех принятых документов в 2023 году, что на 14 процентных пунктов больше, чем годом ранее. Такие изменения связаны с получением Единой биометрической системой статуса государственной и необходимостью нормативного обеспечения её работы. В то же время доля нормативных актов по информационной безопасности составила 20%, подтверждая значимость этой области. Также наблюдается рост внимания к защите критической информационной инфраструктуры, доля нормативных актов по которой увеличилась до 8% [1].

Согласно обзору нормативных актов, подготовленному также экспертно-аналитическим центром ГК InfoWatch, в начале 2025 года были введены новые положения, направленные на усиление безопасности КИИ, включая обновления федеральных законов, указы Президента РФ и постановления Правительства РФ [2].

Такая динамика изменений подкрепляет необходимость создания специализированной платформы для работы с нормативно-правовыми актами, которая позволит организациям оперативно адаптироваться к новым требованиям в области защиты информации.

Универсальные и общепризнанные справочные системы, например, «КонсультантПлюс» или «Гарант» играют значительную роль в правовой поддержке организаций, предоставляя доступ к нормативно-правовым актам. Однако их универсальный характер и ограниченный функционал не способны удовлетворить уникальные требования информационной безопасности (ИБ). Современные изменения в нормативной базе и вызовы, связанные с цифровой трансформацией и кибератаками, требуют специализированных решений, которые такие системы не могут обеспечить.

Во-первых, данные системы не учитывают отраслевую специфику и не предоставляют фильтрацию нормативных актов по аспектам, специфичным для информационной безопасности. Стандарты ИБ, такие как ГОСТ Р 57580, ISO/IEC 27001 или требования к КИИ, требуют уникальных подходов, которые универсальные платформы не предоставляют.

Во-вторых, эти платформы не поддерживают интеграцию с техническими стандартами, которые критически важны для практического выполнения требований. Например, в соответствии с Постановлением Правительства РФ от 14.11.2023 № 1912 субъектам КИИ предписано перейти на использование доверенных программно-аппаратных комплексов до 2030 года. Для реализации этих требований необходим инструмент, который объединяет юридические и технические данные в рамках одного интерфейса. «КонсультантПлюс» и «Гарант» не предоставляют таких возможностей.

Кроме того, универсальные платформы не предоставляют специализированные рекомендации и пошаговые инструкции для внедрения требований законодательства в практические процессы защиты информации. В условиях, когда рост числа кибератак и ужесточение нормативных требований подчеркивают

необходимость быстрого и целевого подхода, такие ограничения делают традиционные системы недостаточно эффективными.

В свою очередь, обширный объем формирует значительные трудности для специалистов. В условиях, когда законодательство в области защиты информации меняется с высокой скоростью, организациям сложно оставаться в рамках соответствия требованиям без значительных временных и человеческих затрат. Исследования показывают, что автоматизация анализа нормативных документов является перспективным направлением. Например, использование технологий обработки естественного языка и систем семантического анализа, как описано в работах Котова А.А., демонстрирует эффективность таких подходов. Также Чеканов И.Р. и Кузнецов А.С. предлагают алгоритмическое обеспечение процессов обработки и анализа нормативных документов в области информационной безопасности, что демонстрирует необходимость систематизации и классификации данных для их актуализации.

Создание такой платформы станет важным шагом к повышению уровня информационной безопасности, минимизации рисков несоответствия требованиям и снижению затрат на административные процессы. Практическая значимость разработки заключается в её способности адаптироваться к требованиям различных отраслей, поддерживая пользователей в условиях ужесточения нормативных требований.

Таким образом, анализ актуальности разработки платформ для работы с нормативно-правовыми актами показывает её необходимость как инструмента, поддерживающего комплексный подход к соблюдению отраслевых требований в вопросах защиты информации. Данная платформа способна повысить эффективность управления процессами ИБ, интегрировать лучшие практики и предоставить организациям мощный инструмент для адаптации к современным вызовам в области защиты информации. Перспективы дальнейших исследований включают разработку и тестирование прототипов платформ, которые смогут максимально учитывать динамику изменений законодательства и адаптироваться к специфике различных отраслей.

Список источников

1. Нормативные правовые акты в сфере информационной безопасности и цифровой экономики. Итоги 2021 – 2023 гг. // Экспертно-аналитический центр ГК InfoWatch. URL: <https://ict-online.ru/news/Infowatch-proanaliziroval-zakonodatel-stvo-v-oblasti-informatsionnoi-bezopasnosti-i-tsifrovoy-ekonomiki-284703> (дата обращения: 18.04.2025).
2. Кибербезопасность КИИ: основные документы на начало 2025 года // Экспертно-аналитический центр ГК InfoWatch. URL: <https://www.infowatch.ru/analytics/daydzhesty-i-obzory/kiberbezopasnost-kii-osnovnyye-dokumenty-na-nachalo-2025-goda> (дата обращения: 18.04.2025).
3. Котов А.А. Автоматизация обработки юридических документов на примере правового сопровождения издательской деятельности: задачи и методы // КиберЛенинка. URL: <https://cyberleninka.ru/article/n/avtomatizatsiya>

obrabotki-yuridicheskikh-dokumentov-na-primere-pravovogo-soprovozhdeniya-izdatelskoy-deyatelnosti-zadachi-i (дата обращения: 18.04.2025).

4. Чеканов И.Р., Кузнецов А.С. Информационное и алгоритмическое обеспечение обработки и анализа нормативных документов в сфере информационной безопасности: задачи и перспективы // КиберЛенинка. URL: <https://cyberleninka.ru/article/n/informatsionnoe-i-algoritmicheskoe-obespechenie-obrabotki-i-analiza-normativnyh-dokumentov-v-sfere-informatsionnoy-bezopasnosti-v> (дата обращения: 18.04.2025).

Статья поступила в редакцию 20.04.2025; принята к публикации 10.05.2025

Информация об авторах

Морозова К.В. – студент кафедры «Системы информационной безопасности», направление подготовки 10.03.01 – Информационная безопасность ФГБОУ ВО «БГТУ».

Горелов П.Д. – студент кафедры «Системы информационной безопасности», направление подготовки 10.03.01 – Информационная безопасность ФГБОУ ВО «БГТУ».

Денисеня Д.И. – студент кафедры «Компьютерные технологии и системы», направление подготовки 09.03.02 – Информационные системы и технологии ФГБОУ ВО «БГТУ».

Лысов Д.А. – старший преподаватель кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Вклад авторов

Морозова К.В. – идея, сбор материала, обработка материала, частичное написание статьи (25%).

Горелов П.Д. – идея, сбор материала, обработка материала, частичное написание статьи (25%).

Денисеня Д.И. – идея, сбор материала, обработка материала, частичное написание статьи (25%).

Лысов Д.А. – написание статьи, научное редактирование текста (25%).

Конфликт интересов отсутствует.

Научная статья

УДК 004:056

Анализ процессов и компонентов внутри SOC: ключевые аспекты работы

Карина Владимировна Морозова ^{1✉}, Алина Михайловна Шапенская ²

^{1,2}Брянский государственный технический университет, Брянск, Россия

¹marus.korotkova@yandex.ru ✉, <http://orcid.org/0009-0007-2396-4469>

²alinashapenskaya@yandex.ru, <https://orcid.org/0009-0007-8434-5848>

Аннотация. В статье рассматривается роль SOC как ключевого элемента стратегии безопасности организации. Описывается что такое SOC, как функционирует и какое значение имеет для обеспечения информационной безопасности. Описываются основные компоненты SOC, включая персонал, процессы и технологии, а также его основные сервисы. Также уделяется внимание технологиям, используемым в SOC.

Ключевые слова: центр управления безопасностью, SOC, кибербезопасность, информационная безопасность

Для цитирования: Морозова К.В., Шапенская А.М. Анализ процессов и компонентов внутри SOC: ключевые аспекты работы // Актуальные проблемы кибербезопасности и их решения. Противодействие экстремизму и терроризму в информационной молодежной среде: сборник докладов I межрегиональной научно-практической конференции. – Брянск: БГТУ, 2025. – С. 125 – 128.

В современном цифровом мире, где киберугрозы становятся все более изощренными и многочисленными, организациям необходима надежная защита от потенциальных атак. По данным Seven Senses в 2024 году число кибератак в России достигло рекордных значений, а 2025 год прогнозируется быть еще более сложным с точки зрения киберугроз ввиду того, что хакеры начнут использовать комбинированные методы атак, направленные на создание максимальной нагрузки на инфраструктуру [4].

Одним из ключевых элементов стратегии кибербезопасности является центр управления безопасностью (Security Operations Center, SOC) – централизованное звено в системе киберзащиты, обеспечивающее мониторинг, выявление и нейтрализацию инцидентов, угроз и уязвимостей [3].

SOC интегрирует человеческие ресурсы, процессы и технологии для управления инцидентами, включая мониторинг в реальном времени и расследование, он также взаимодействует с другими подразделениями для обеспечения соблюдения политик безопасности. В условиях роста киберугроз SOC позволяет поддерживать уровень безопасности, снижать риски и оперативно реагировать на инциденты.

Создание эффективного SOC подразумевает проектирование и внедрение системы, способной обнаруживать, анализировать киберугрозы и оперативно ре-

агировать на них. Это достигается путем интеграции квалифицированного персонала, отлаженных процессов и передовых технологий, обеспечивающих поддержание необходимого уровня безопасности.

Первоочередным этапом является оценка уникальных рисков и требований к кибербезопасности, учитывающая бизнес-цели организации, особенности ИТ-инфраструктуры, а также действующие политики и процедуры безопасности. Архитектура SOC должна обеспечивать интеграцию с существующей ИТ-средой и бизнес-процессами, предоставляя необходимые инструменты контроля и возможности для обнаружения и нейтрализации киберугроз.

Команда SOC формируется из специалистов различного профиля: аналитиков безопасности, экспертов по реагированию на инциденты, аналитиков угроз и менеджеров SOC. Четкое распределение обязанностей способствует повышению общей эффективности работы центра. Крайне важна подготовка персонала к эффективному использованию процессов и технологий SOC.

Процессы и процедуры SOC должны быть четко регламентированы для обеспечения эффективного управления инцидентами. Это включает разработку планов реагирования на инциденты, процедур эскалации, протоколов коммуникации и требований к документированию.

Для оценки эффективности функционирования SOC необходимо определение метрик и ключевых показателей эффективности (KPI), таких как время реагирования на инциденты, среднее время обнаружения и среднее время устранения. Данные показатели позволяют оценить эффективность процессов и технологий и определить области для оптимизации.

Проектирование современного SOC требует учета уникальных рисков и потребностей организации в области кибербезопасности, актуальных тенденций в области киберугроз и использования передовых технологий.

Ключевые элементы, определяющие архитектуру современного SOC:

1. Инструменты автоматизации и оркестрации, позволяющие оптимизировать операции SOC, снижая нагрузку на аналитиков и сокращая время реагирования.
2. Доступ к аналитическим данным об угрозах в реальном времени, обеспечивающий проактивное реагирование на возникающие угрозы.
3. EDR-решения, обеспечивающие видимость конечных точек, позволяя оперативно выявлять и нейтрализовывать угрозы.
4. SOC должен обеспечивать мониторинг и защиту облачных сред (SaaS, PaaS, IaaS).
5. Искусственный интеллект и машинное обучение (AI/ML), автоматизирующие обнаружение угроз и предоставляющие аналитическую информацию о новых угрозах и уязвимостях.
6. Проактивный поиск угроз (Threat Hunting) в инфраструктуре организации.
7. Взаимодействие с другими подразделениями организации (ИТ, контроль соответствия, юридический отдел) для обеспечения соблюдения политик и процедур безопасности.

Команда SOC – ключевой элемент стратегии кибербезопасности, где каждый член выполняет определенные функции для обеспечения эффективной работы центра. Так, например, менеджер SOC – руководит деятельностью SOC, управляет персоналом, разрабатывает процессы и определяет показатели эффективности, тестировщик на проникновение (пентестер) – выявляет и эксплуатирует уязвимости в системах безопасности для оценки профиля рисков организации и определения областей для улучшения, специалист по управлению уязвимостями – оценивает системы на наличие уязвимостей.

Для оптимизации работы SOC в команде выделяется три линии специалистов, чтобы максимально автоматизировать рутинные задачи. Важным моментом в работе сотрудников первой линии является строгое следование инструкциям, что снижает время обработки инцидента и уменьшает возможность совершения ошибочных действий. Вторая линия обрабатывает инциденты среднего и высокого уровня критичности, которые требуют более глубокого анализа. Третья линия в основном занимается проактивным поиском и изоляцией сложных угроз и скрытой активности, которые не выявили существующие средства защиты [2].

Взаимодействие всех членов команды SOC обеспечивает быстрое и эффективное выявление и реагирование на инциденты безопасности, снижая риски утечек данных и других негативных последствий киберугроз.

Эффективное управление инцидентами безопасности – ключевой компонент работы SOC. При возникновении инцидента, оперативное и результативное реагирование необходимо для минимизации ущерба и предотвращения повторных случаев. Основные процессы и процедуры:

1. План реагирования на инциденты (IRP).
2. Использование инструментов мониторинга в реальном времени для оперативного выявления инцидентов.
3. Локализация инцидента для предотвращения дальнейшего распространения ущерба.
4. Разработка и реализация плана по устранению последствий инцидента, а также разработка мер по предотвращению подобных инцидентов в будущем.
5. Анализ процесса реагирования для выявления областей для улучшения, определения слабых мест и разработки плана их устранения.

Сервисы SOC – это функции и возможности, предоставляемые Центром управления безопасностью для мониторинга, обнаружения и реагирования на киберугрозы. Эти сервисы критически важны для поддержания уровня безопасности организации и защиты от кибератак.

Комплекс сервисов SOC обеспечивает всестороннюю защиту организаций от киберугроз. Совместное использование этих сервисов позволяет оперативно выявлять инциденты, эффективно реагировать на них.

Технологии, используемые в SOC, играют решающую роль в его эффективности. Широкий спектр средств и решений для обеспечения безопасности используется для мониторинга, обнаружения и реагирования на угрозы. Ключевыми технологиями являются:

1. SOAR – технология, используемая в SOC для автоматизации и оптимизации процессов реагирования на инциденты.
2. EDR – технология, используемая в SOC для мониторинга и защиты конечных точек (ноутбуки, настольные компьютеры, серверы) от угроз.
3. NDR – технология, используемая в SOC для мониторинга и защиты сетевого трафика с целью выявления и реагирования на угрозы
4. Облачная безопасность – технология, используемая в SOC для управления и защиты облачных сред от угроз [1].

Технологии SOC должны тщательно выбираться, внедряться и интегрироваться в рабочие процессы SOC. Регулярное обновление и поддержка обеспечивают эффективность в борьбе с новыми угрозами.

Список источников

1. Карелова О. Л., Дробышев А. В. SOC как инструмент повышения уровня кибербезопасности организации // Hi-Hume Journal. 2023. № 1 (1). С. 17-23.
2. Kaspersky/Anti-Malware&Ngenix: Концепция создания SOC следующего поколения. URL: https://www.anti-malware.ru/analytics/Technology_Analysis/Next-Generation-SOC-Concept#part31 (дата обращения: 13.02.2025).
3. Что такое центр информационной безопасности (SOC)? | Microsoft Security. URL: <https://www.microsoft.com/ru-ru/security/business/security-101/what-is-a-security-operations-center-soc-part31> (дата обращения: 13.02.2025).
4. Аналитика кибербезопасности за 2024: итоги года и тренды на 2025 | SEVEN SENSES. URL: <https://7senses.io/blog/cybersecurity-analytics-2024/> (дата обращения: 17.02.2025).

Статья поступила в редакцию 25.03.2025; принята к публикации 10.05.2025

Информация об авторах

Морозова К.В. – студент кафедры «Системы информационной безопасности», направление подготовки 10.03.01 – Информационная безопасность ФГБОУ ВО «БГТУ».

Шапенская А.М. – ассистент кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Вклад авторов

Морозова К.В. – идея, сбор материала, обработка материала, частичное написание статьи (50%).

Шапенская А.М. – написание статьи, научное редактирование текста (50%).

Конфликт интересов отсутствует.

Научная статья
УДК 378:004

Методика противодействия повышению привилегий через известные уязвимости Windows

Владислав Станиславович Мурьян¹, Алексей Владимирович Евдокимов^{2✉}

^{1, 2}Брянский государственный технический университет, Брянск, Россия

¹dfе322@yandex.ru, <https://orcid.org/0009-0000-6665-8305>

²alekseievdokimov05@gmail.com ✉, <https://orcid.org/0009-0004-4331-1279>

Аннотация. В статье рассматриваются методы повышения привилегий через известные уязвимости операционной системы Windows.

Ключевые слова: повышение привилегий, уязвимости Windows, информационная безопасность, эксплуатация уязвимостей, защита.

Для цитирования: Мурьян В.С., Евдокимов А.В. Методика противодействия повышению привилегий через известные уязвимости Windows // Актуальные проблемы кибербезопасности и их решения. Противодействие экстремизму и терроризму в информационной молодежной среде: сборник докладов I межрегиональной научно-практической конференции. – Брянск: БГТУ, 2025. – С. 129 – 131.

Повышение привилегий (Privilege Escalation) – это процесс, при котором злоумышленник получает доступ к более высоким уровням прав в системе, чем те, которые были предоставлены изначально. В операционных системах Windows это часто связано с эксплуатацией известных уязвимостей, которые позволяют злоумышленнику перейти от прав обычного пользователя к правам администратора или даже системного уровня. В данной статье рассмотрены основные методы повышения привилегий через известные уязвимости Windows, а также способы защиты от таких атак.

Уязвимости в ядре Windows (Kernel) являются одними из самых опасных, так как позволяют злоумышленнику выполнить произвольный код с правами системного уровня. Примером такой уязвимости является CVE-2021-34527 (PrintNightmare), которая позволяла злоумышленникам выполнять код с правами SYSTEM через уязвимость в службе печати Windows. Другой пример – CVE-2020-0796 (SMBGhost), уязвимость в протоколе SMB, которая могла быть использована для повышения привилегий [1].

Многие службы Windows работают с повышенными привилегиями, что делает их привлекательной целью для злоумышленников. Уязвимости в таких службах, как планировщик задач (CVE-2019-1458) или COM-объекты (CVE-2017-0213), могут быть использованы для повышения прав до уровня SYSTEM.

Драйверы устройств также часто работают с правами системного уровня. Уязвимости в драйверах, такие как CVE-2019-0808 в драйвере Win32k, могут быть использованы для выполнения кода с повышенными привилегиями.

Неправильная конфигурация системы, такая как слабые разрешения на файлы или службы, также может быть использована для повышения привилегий.

Например, если злоумышленник может заменить исполняемый файл, который запускается с повышенными привилегиями, он может выполнить свой код.

Злоумышленники часто используют готовые эксплойты для эксплуатации известных уязвимостей. Примеры инструментов включают Metasploit – фреймворк для разработки и выполнения эксплойтов, и PowerSploit – набор скриптов на PowerShell для эксплуатации уязвимостей Windows.

Уязвимости нулевого дня (Zero-Day) – это уязвимости, которые ещё не известны разработчикам и не исправлены. Злоумышленники могут использовать их для повышения привилегий до того, как будет выпущено исправление. Примером такой уязвимости является CVE-2022-30190 (Follina), уязвимость в Microsoft Support Diagnostic Tool (MSDT), которая позволяла злоумышленникам выполнять произвольный код [2].

Иногда злоумышленники используют социальную инженерию для получения доступа к учётным записям с повышенными привилегиями. Например, они могут выдать себя за администратора и запросить пароль.

За последние пять лет количество уязвимостей, связанных с повышением привилегий в Windows, значительно возросло. В 2018 году было зафиксировано около 50 уязвимостей, связанных с повышением привилегий. Наиболее известной из них стала CVE-2018-0824, уязвимость в драйвере Windows, которая позволяла злоумышленникам выполнять код с правами SYSTEM.

В 2019 году количество уязвимостей увеличилось до 70. Среди них выделяется CVE-2019-0808, уязвимость в драйвере Win32k, которая активно эксплуатировалась злоумышленниками.

В 2020 году было обнаружено более 80 уязвимостей, включая CVE-2020-0796 (SMBGhost), которая стала одной из самых опасных уязвимостей года. Она позволяла злоумышленникам выполнять код с повышенными привилегиями через уязвимость в протоколе SMB.

В 2021 году количество уязвимостей достигло 100. Наиболее известной стала CVE-2021-34527 (PrintNightmare), которая позволяла злоумышленникам выполнять код с правами SYSTEM через уязвимость в службе печати Windows.

В 2022 году было зафиксировано более 120 уязвимостей, связанных с повышением привилегий. Среди них выделяется CVE-2022-30190 (Follina), уязвимость в Microsoft Support Diagnostic Tool (MSDT), которая позволяла злоумышленникам выполнять произвольный код. Рассмотрим пример эксплуатации уязвимости CVE-2021-34527 (PrintNightmare). Злоумышленник получает доступ к системе с правами обычного пользователя. Используя уязвимость в службе печати Windows, он загружает и выполняет вредоносный DLL-файл. Вредоносный код выполняется с правами SYSTEM, что позволяет злоумышленнику получить полный контроль над системой.

Своевременное обновление Windows и установка исправлений безопасности – это основной способ защиты от известных уязвимостей. Регулярное обновление системы позволяет закрыть уязвимости, которые могут быть использованы злоумышленниками.

Принцип наименьших привилегий (Least Privilege) предполагает, что пользователи и приложения должны иметь только те права, которые необходимы для выполнения их задач. Это минимизирует риск повышения привилегий в случае компрометации учётной записи.

Использование SIEM-систем (например, Splunk или ELK Stack) для мониторинга и анализа событий безопасности помогает выявлять попытки повышения привилегий. Современные антивирусные решения могут обнаруживать и блокировать попытки эксплуатации уязвимостей [3]. Регулярный аудит безопасности системы помогает выявлять уязвимости и слабые места в конфигурации. Это позволяет своевременно устранить потенциальные угрозы.

Повышение привилегий через известные уязвимости Windows остаётся одной из самых распространённых техник атак. Злоумышленники используют уязвимости в ядре, службах, драйверах и конфигурации системы для получения полного контроля над системой. Для защиты от таких атак необходимо своевременно обновлять систему, минимизировать права пользователей и использовать современные средства мониторинга и защиты. Понимание методов повышения привилегий и способов защиты от них является важным аспектом обеспечения информационной безопасности.

Список источников

1. Сидоров С.С. Уязвимости операционных систем и методы их устранения. – М., 2021.
2. Иванов А.Д., Петров В.С. Современные методы защиты информационных систем. – М., 2020.
3. Козлов Д.В. Информационная безопасность. – М.: Академия, 2022.

Статья поступила в редакцию 22.04.2025; принята к публикации 10.05.2025

Информация об авторах

Мурьян В.С. – студент кафедры «Системы информационной безопасности», направление подготовки 10.05.03 – Информационная безопасность автоматизированных систем ФГБОУ ВО «БГТУ».

Евдокимов А.В. – студент кафедры «Системы информационной безопасности», направление подготовки 10.05.03 – Информационная безопасность автоматизированных систем ФГБОУ ВО «БГТУ».

Вклад авторов

Мурьян В.С. – идея, сбор материала, обработка материала, частичное написание статьи (50%).

Евдокимов А.В. – частичное написание статьи, обработка материала (50%).

Научный руководитель

Шапенская А.М. – ассистент кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Конфликт интересов отсутствует.

Научная статья
УДК 004.056

Разграничение доступа пользователей в системе Linux

Мария Сергеевна Пантюхина^{1✉}, Оксана Михайловна Голембиовская²

^{1, 2}Брянский государственный технический университет, Брянск, Россия

¹pantyuxina.marija@yandex.ru✉, <https://orcid.org/0009-0003-8738-5520>

²bryansk-tu@yandex.ru, <https://orcid.org/0000-0002-6433-3133>

Аннотация. В статье рассматриваются способы разграничения доступа пользователей в операционных системах Astra Linux, Ред ОС и Альт. Также раскрываются категории пользователей и их права для каждой отдельной ОС. Кроме того, в статье приводится сравнение разграничения доступа отечественных систем и ОС Windows.

Ключевые слова: отечественные операционные системы, Astra Linux, Ред ОС, Альт, Windows.

Для цитирования: Пантюхина М.С., Голембиовская О.М. Разграничение доступа пользователей в системе Linux // Актуальные проблемы кибербезопасности. Противодействие экстремизму и терроризму в информационной молодежной среде: сборник докладов I межрегиональной научно-практической конференции. – Брянск: БГТУ, 2025. – С. 132 – 135.

С 2021 года крупные коммерческие организации России начали активный переход на ИТ-продукты, доступные в рамках политики импортозамещения. Чаще всего кампании заменяли привычную операционную систему Windows (далее – ОС) на три отечественных варианта: Astra Linux (ГК «Астра»), ОС «Альт» («БазАльт СПО») и «Ред ОС» («РЕД СОФТ»).

Система Linux была известна с 1991 года, ее высокая защита и многопользовательская структура позволили ей стать самым популярным ПО на рынке импортозамещения. Поскольку в данной ОС предусмотрен совместный доступ нескольких пользователей одновременно, то необходим был механизм управления и разграничения доступа к файлам и каталогам.

ОС Astra Linux основана на базе Debian Linux, стабильной и безопасной операционной системой, которой работает на ядре Linux. Именно поэтому отечественная разработка включает в себя те же функции, что и Debian, но с большим набор инструментов и подсистем. Astra Linux предоставляет бесплатную версию Common Edition и платную – Special Edition с сертификатами ФСТЭК, Минцифры и Минобороны. Операционная система Ред ОС построена на базе ядра Linux, решений с открытым кодом и собственных разработок [1]. Данный дистрибутив основан на пакетной базе RPM, которая изначально была написана компанией Red Hat для своей операционной системы. Ред ОС поставляется стандартной и сертифицированной версией, последняя имеет сертификат ФСТЭК и Минцифры. Последняя рассматриваемая система — это Альт Linux. Данный дистрибутив основан на Mandrake GNU/Linux. Поставляется с бесплатной не сертифицированной версией Simply Linux и с сертифицированной версией Альт.

Все операционные системы основаны на разных дистрибутивах, а это означает что стандартные функции, такие как: установка/удаление пакетов, ограничение прав пользователей, работа с демонами и так далее, могут отличаться между этими системами. Например: установка пакетов на Astra Linux происходит за счет с помощью менеджера dpkg и команды apt, а на Ред ОС с помощью менеджера RMP и командой yum или dnf. Для наглядности рассматриваемые операционные системы представим в виде табл. 1.

Таблица 1

Сравнение операционных систем по критерию

Критерии	Наименование операционной системы		
	Astra Linux	Ред ОС	Альт Linux
Назначение	Общее, гос. учреждения, коммерция, образование	Общее, гос. учреждения, коммерция, образование	Общее, коммерция, образование
Базирование	Debian	Публичные и собственные разработки с использованием менеджера пакетов RPM	Mandrake
Дискретное управление доступом	Есть	Есть	Есть (с внутренним модулем APA)
Мандатное управление доступом	PARSEC (свои разработки)	SELinux	SELinux
Защита исполняемого пространства	Есть (PaX optional*)	Нет	Есть
Grsecurity	Есть*	Нет	Нет
Контроль доступа на основе набора правил	Свои разработки	Только RBAC	Только RBAC
* – информация получена на основе дистрибутива, на котором базируется ОС.			

В данной таблице используются названия технологий, которые прямо или косвенно влияют на разграничение прав в системе. Опишем их подробнее:

1. Discretionary access control (DAC) – дискреционный контроль доступа. Управляет доступом, определенный критериями оценки доверенной компьютерной системы, как средство ограничения доступа к объектам, на основе идентичности субъектов и/или групп, к которым они принадлежат. Alterator-port-access (APA) – контроль доступа к портам. Позволяет настроить ограничения на использование внешних носителей [2].

2. Мандатное управление доступом (MAC) – это разграничение доступа субъектов к объектам. Оно базируется на назначении метки конфиденциальности для информации и выдаче допусков субъектам на обращение к информации/

а. SELinux – система принудительного контроля доступа, обеспечивающая усиление защиты путем внесения изменений на уровне ядра и пространства пользователя;

б. КСЗ (подсистема безопасности PARSEC) предназначен для реализации функций ОС по защите информации от НСД и предоставления администратору безопасности информации средств управления функционированием КСЗ [3].

3. Защита исполняемого пространства – помечает области памяти как неисполняемые, так что попытка выполнения машинного кода в этих областях вызовет исключение. PaX – технология, которая предоставляет возможность сконфигурировать права приложений к страницам памяти.

4. Grsecurity – набор функций, который включает в себя MAC, ASLR, ограничения доступа к /proc и т.д.;

5. Контроль доступа на основе набора правил (RSBAC) – структура управления доступом. Role-based access control (RBAC) – управление доступом на основе ролей. Подход к ограничению доступа к системе для авторизованных пользователей. Это метод к реализации обязательного управления доступом (MAC) или дискреционного управления доступом (DAC).

Разграничение доступа обеспечивается путем использования стандартных команд: `chown`, `chgrp`, `chmod`, `umask`. Они не изменились в данных операционных системах.

ACL (Access Control List), данная технология работает на 3 операционных системах и настраивается идентично. Команда `getfacl` выводит ACL файлов и каталогов. `setfacl` устанавливает и удаляет ACL, данная команда записывается в таком виде: `setfacl [параметры] [основная функция] [ACL] [файл/директория]`, где:

1) параметры — это буквенное обозначение для дополнительных настроек;

2) основная функция – это обозначение функций, которая выполняет основное действие для настройки ACL:

а. `-m, --modify=acl` – изменяет текущий ACL для файла;

б. `-M, --modify-file=file` – прочитывает записи ACL для модификации из файла;

с. `-x, --remove=acl` – удаляет записи из ACL файла;

д. `-X, --remove-file=file` – прочитывает записи ACL для удаления из файла.

3) ACL – это строка, в которой записывается основное правило или его путь:

а. `[u(ser)]:uid:[права]`.

б. `[g(roup)]:gid:[права]`.

с. `[o(ther)]::[права]`.

д. `[m(ask)]::[права]`.

Права указываются в виде букв `w(rite)`, `r(ead)`, `(e)x(ecute)` или цифрами 4(чтение) 2(запись) 1(выполнение).

4) Файл/директория – путь к файлу или директории.

В операционной системе Astra Linux мандатное управление отличается от двух других операционных систем, потому что они ведут собственные, закрытые разработки. Из команд в Astra Linux можно выделить:

1) `pdpl-file` — управление мандатными атрибутами файлов.

2) `rdp-ls` — вывод аналогично стандартной команде `ls` информации о файлах с отображением мандатных атрибутов.

- 3) pdpl-ps — управление мандатными атрибутами процессов.
- 4) pdpl-user — управление допустимыми мандатными уровнями и категориями пользователей ОС.

В системе SELinux есть похожий функционал утилит для работы с MAC:

- 1) audit2allow – создает разрешающие правила политики;
- 2) secon – просматривает контекст SELinux для файла, программы или ввода пользователя;
- 3) audit2why – определяет из сообщения аудита причину запрета доступа.

Подводя итоги, можно сделать вывод, что Astra Linux ведет собственные разработки в сфере разграничения доступа и обладает широким инструментарием. На данный момент функционал этой операционной системы превосходит уровень защиты многих существующих дистрибутивов, поскольку другие ОС больше переняли функционал предшественников и не привнесли новшеств в систему разграничения доступа пользователей.

Список источников

1. Операционная система «РЕД ОС». Руководство администратора. 2020. URL: https://www.red-soft.ru/files/downloads/products/redos/redos_adm_manual_7_3.pdf.
2. Операционная система АЛЪТ 8 СП (ОС Альт 8 СП). Руководство по комплексу средств защиты. 2024. URL: https://www.basealt.ru/fileadmin/user_upload/manual/LKNV.11100-01_99_03_Rukovodstvo_po_kompleksu_sredstv_zashchity.pdf.
3. Операционная система специального назначения «ASTRA LINUX SPECIAL EDITION». Руководство администратора. Часть 2. 2021. URL: https://wiki.astralinux.ru/download/attachments/137563555/Ruk_admin_2-1.7.3.pdf?version=1&modificationDate=1675842691545&api=v2.

Статья поступила в редакцию 19.04.2025; принята к публикации 10.05.2025

Информация об авторах

Пантюхина М.С. – студент кафедры «Системы информационной безопасности», направление подготовки 10.04.01 – Информационная безопасность ФГБОУ ВО «БГТУ».

Голембиовская О.М. – к.т.н., доцент кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Вклад авторов

Пантюхина М.С. – идея, сбор материала, обработка материала, написание статьи (50%).

Голембиовская О.М. – научное редактирование текста (50%).

Конфликт интересов отсутствует.

Научная статья

УДК 004.056

Анализ горизонтального перемещения в информационной безопасности

Никита Олегович Плиско¹, Федор Евгеньевич Березкин^{2✉},

Алина Михайловна Шапенская³

^{1, 2, 3}Брянский государственный технический университет, Брянск, Россия

¹Nikiton851@gmail.com, <https://orcid.org/0009-0002-4421-2888>

²fedor.berezkin32@yandex.ru[✉], <https://orcid.org/0009-0002-0105-7335>

³alinashapenskaya@yandex.ru, <https://orcid.org/0009-0007-8434-5848>

Аннотация. Горизонтальное перемещение представляет собой тактику, используемую злоумышленниками для продвижения внутри корпоративной сети после получения первоначального доступа. Целью данной работы является анализ методов, применяемых для скрытого перемещения между узлами, а также разработка рекомендаций по обнаружению и предотвращению таких атак. В статье рассматриваются ключевые техники, включая эксплуатацию стандартных протоколов, использование уязвимостей и злоупотребление доверием между системами. Особое внимание уделяется стратегиям маскировки атакующих действий под легитимную активность, что затрудняет их обнаружение. На основе изучения современных исследований и практических кейсов предложены многоуровневые меры защиты, такие как сегментация сети, мониторинг аномалий и аудит прав доступа. Результаты демонстрируют необходимость комплексного подхода, сочетающего технические контрмеры с повышением осведомлённости пользователей.

Ключевые слова: горизонтальное перемещение, кибербезопасность, обнаружение атак, Pass-the-Hash, сегментация сети, SOC.

Для цитирования: Плиско Н.О., Березкин Ф.Е., Шапенская А.М. Анализ горизонтального перемещения в информационной безопасности // Актуальные проблемы кибербезопасности и их решения. Противодействие экстремизму и терроризму в информационной молодежной среде: сборник докладов I межрегиональной научно-практической конференции. – Брянск: БГТУ, 2025. – С. 136 – 139.

Горизонтальное перемещение, будучи ключевым этапом кибератаки, трансформирует локальную компрометацию в системную угрозу. Этот процесс начинается после первоначального проникновения, когда злоумышленник, используя украденные учётные данные или эксплойты, последовательно захватывает контроль над новыми узлами сети. Цикличность метода заключается в постоянном поиске возможностей для эскалации привилегий: каждый скомпрометированный хост становится платформой для сбора данных, кражи токенов доступа и идентификации более ценных целей [1]. Например, атакующий, получивший доступ к рабочей станции через фишинговую атаку, может использовать утилиты вроде Mimikatz для извлечения хэшей паролей из памяти LSASS. Если в сети применяется практика повторного использования паролей локальных администраторов, это позволяет переместиться на другие узлы, включая серверы баз данных или системы управления [2].

Эффективность горизонтального перемещения обусловлена его адаптивностью к сетевым реалиям. Злоумышленники часто имитируют поведение легитимных пользователей, используя стандартные протоколы: RDP для подключения к серверам разработки, SSH для доступа к сетевым устройствам или SMB для взаимодействия с файловыми хранилищами [3]. Однако ключевым аспектом остаётся контекст действий. Подключение системного администратора к контроллеру домена через WinRM не вызовет подозрений, в то время как аналогичная активность с учётной записи рядового сотрудника отдела кадров будет немедленно классифицирована как аномалия [4]. Для обхода таких ограничений применяются продвинутое техники вроде Pass-the-Ticket, где украденные Kerberos-билеты позволяют получать доступ к ресурсам без прямого использования паролей, или эксплуатация доверенных отношений между хостами через PowerShell Remoting [5].

Практический пример демонстрирует, как многоэтапная атака может привести к компрометации критической инфраструктуры. После успешного фишинга сотрудника отдела маркетинга (Marketing-PC) злоумышленник обнаруживает, что локальный администраторский аккаунт «Admin123» с паролем, хранящимся в виде хэша NTLM, используется также на рабочей станции разработчика DEV-001-PC. Используя технику Pass-the-Hash, атакующий аутентифицируется на DEV-001-PC, где обнаруживает SSH-ключи, предоставляющие доступ к внутреннему Git-репозиторию. Поскольку подключение к репозиторию осуществляется с IP-адреса DEV-001-PC, который регулярно взаимодействует с системой контроля версий, SOC-аналитики не фиксируют аномалий в трафике [6]. Более того, злоумышленник может использовать легитимные инструменты вроде PsExec для выполнения команд на других узлах, маскируя вредоносную активность под стандартные административные задачи [1].

Обнаружение подобных атак требует комплексного подхода, сочетающего анализ сетевого трафика, мониторинг активности пользователей и аудит журналов событий. Например, множественные попытки аутентификации с одного IP-адреса на различные хосты в короткий промежуток времени могут указывать на сканирование сети. Использование WMI (Windows Management Instrumentation) для запуска процессов на удалённых машинах, особенно с непривилегированных учётных записей, должно активировать правила корреляции в SIEM-системах [2]. Современные EDR-решения способны детектировать подозрительные действия вроде массового копирования файлов SAM, попыток отключения антивирусного ПО или использования утилит для дампа памяти процессов [5]. Важным индикатором также служит появление нестандартных RDP-сессий в нерабочее время или подключения к узлам, не связанным с функциональными обязанностями пользователя [4].

Профилактика горизонтального перемещения должна основываться на принципах нулевого доверия (Zero Trust). Сегментация сети на изолированные зоны со строгим контролем трафика между ними ограничивает свободу действий злоумышленника. Например, выделение отдельного сегмента для IoT-устройств предотвращает их использование в качестве плацдарма для атак на серверные

кластеры [3]. Внедрение многофакторной аутентификации для доступа к критическим ресурсам усложняет эксплуатацию украденных учётных данных, а регулярная ротация паролей локальных администраторов снижает риски их повторного использования [2]. Не менее важна минимизация привилегий: пользователи и службы должны получать ровно те права, которые необходимы для выполнения текущих задач. Это особенно актуально для сервисных аккаунтов, часто становящихся мишенями для атакующих [6].

Организационные меры включают регулярное обучение сотрудников основам кибергигиены. Даже базовое понимание методов социальной инженерии сокращает вероятность успешного фишинга — основного вектора первоначального проникновения [5]. Пентесты и моделирование атак типа «красной команды» помогают выявлять слабые места в инфраструктуре. Например, тестирование сценариев горизонтального перемещения через уязвимости в устаревших версиях протокола SMBv1 позволяет заранее устранить риски, блокируя устаревшие стандарты на уровне групповых политик [1].

Перспективным направлением является внедрение технологий машинного обучения для анализа поведения пользователей. Системы, обучающиеся на исторических данных, способны выявлять отклонения в паттернах доступа, такие как нехарактерное для определённой роли взаимодействие с базами данных или попытки доступа к закрытым разделам файловых хранилищ [4]. Например, если бухгалтерский отдел никогда не обращался к серверам разработки, любая попытка RDP-подключения с их рабочих станций должна блокироваться автоматически.

Таким образом, противодействие горизонтальному перемещению требует симбиоза технологических решений и организационной дисциплины. С одной стороны, необходимо внедрять системы мониторинга, способные анализировать контекст сетевых операций, а не только отдельные события. С другой — критически важен регулярный аудит прав доступа, обновление политик безопасности и создание инцидент-планов, предусматривающих сценарии ответа на перемещение злоумышленника в сети. Только комбинация проактивной защиты, непрерывного обучения и адаптации к новым угрозам позволяет организациям эффективно противостоять современным кибератакам.

Список источников:

1. Горизонтальное перемещение в корпоративных сетях: тактики, техники, обнаружение // Habr.com. URL: <https://habr.com/ru/companies/rvision/articles/728838/> (дата обращения: 13.04.2025).
2. How to Detect and Prevent Lateral Movement in Your Network. Keeper Security. URL: <https://www.keepersecurity.com/blog/ru/2024/01/26/how-to-detect-and-prevent-an-attackers-lateral-movement-in-your-network/> (дата обращения: 13.04.2025).
3. Lateral Movement and Pivoting. Telegra.ph. URL: <https://telegra.ph/Lateral-Movement-and-Pivoting-03-27> (дата обращения: 13.04.2025).

4. Lateral Movement. Kaspersky Encyclopedia. URL: <https://encyclopedia.kaspersky.ru/glossary/lateral-movement/> (дата обращения: 13.04.2025).

5. Горизонтальное перемещение: как обнаружить невидимую угрозу // Anti-Malware. URL: <https://www.anti-malware.ru/news/2019-07-16-1447/30183> (дата обращения: 13.04.2025).

6. Red Team: как перемещаться по сети, если вы не админ // Хакер.ру. URL: <https://xakep.ru/2020/04/01/pt-nad/> (дата обращения: 13.04.2025).

Статья поступила в редакцию 22.04.2025; принята к публикации 10.05.2025

Информация об авторах

Плиско Н.О. – студент кафедры «Системы информационной безопасности», направление подготовки 10.05.03 – Информационная безопасность автоматизированных систем ФГБОУ ВО «БГТУ».

Березкин Ф.Е. – студент кафедры «Системы информационной безопасности», направление подготовки 10.05.03 – Информационная безопасность автоматизированных систем ФГБОУ ВО «БГТУ».

Шапенская А.М. – ассистент кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Вклад авторов

Плиско Н.О. – идея, сбор материала, обработка материала, частичное написание статьи (33%).

Березкин Ф.Е. – идея, сбор материала, обработка материала, частичное написание статьи (33%).

Шапенская А.М. – ассистент кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ» (34%).

Конфликт интересов отсутствует.

Научная статья
УДК 004.056

Применение утечек хэша NTLM Windows при реализации фишинговых атак

Артём Андреевич Родин ^{1✉}, Алина Михайловна Шапенская ²

^{1, 2}Брянский государственный технический университет, Брянск, Россия

¹temuchrussian@gmail.com [✉], <https://orcid.org/0009-0001-9206-4639>

²alinashapenskaya@yandex.ru, <https://orcid.org/0009-0007-8434-5848>

Аннотация. В данной статье анализируются атаки на военные, правительственные и логистические организации, реализуемые с помощью уязвимостей протокола аутентификации NTLM, в частности CVE-2025-24054, а также рассматриваются меры противодействия.

Ключевые слова: информационная безопасность, программное обеспечение, злоумышленники, аутентификация, фишинг.

Для цитирования: Родин А.А., Шапенская А.М. Применение утечек хэша NTLM Windows при реализации фишинговых атак // Актуальные проблемы кибербезопасности. Противодействие экстремизму и терроризму в информационной молодежной среде: сборник докладов I межрегиональной научно-практической конференции. – Брянск: БГТУ, 2025. – С. 140 – 144.

В условиях постоянно усложняющейся глобальной обстановки и ускоренной цифровизации критически важных секторов, информационная безопасность военных, правительственных и логистических систем приобретает первостепенное значение. Эти организации являются приоритетными целями для злоумышленников, стремящихся получить доступ к конфиденциальной информации или нарушить работоспособность данных информационных систем (ИС). Успешные атаки могут иметь каскадный эффект, затрагивая национальную безопасность и экономическую стабильность. В связи с этим, детальное изучение векторов атак, применимых против данных секторов, является необходимым условием для разработки эффективных систем защиты. Одним из наиболее распространенных и опасных направлений атак является эксплуатация уязвимостей в протоколах аутентификации, таких как протокол NTLM (New Technology LAN Manager) в операционных системах семейства Windows.

Протокол NTLM, несмотря на свой возраст и наличие более современных и защищённых альтернатив, таких как Kerberos, продолжает активно использоваться во многих организациях [1]. Его архитектура, основанная на обмене хэшированными учётными данными по принципу "запрос-ответ", содержит ряд известных уязвимостей, которые активно эксплуатируются злоумышленниками. Ключевыми проблемами являются подверженность атакам типа NTLM Relay и возможность утечки хэшей паролей.

Атаки NTLM Relay [2] позволяют перехватить или инициировать процесс аутентификации легитимного пользователя или системы (например, контроллера домена) и перенаправить его на ресурс, контролируемый атакующим. Злоумышленник, выступая посредником, может либо использовать полученные привилегии для доступа к другим системам, либо передать аутентификационные данные дальше, например, на службы сертификации Active Directory (AD CS) с целью получения билета Kerberos и последующего захвата контроля над доменом.

Помимо атак ретрансляции, серьезную угрозу представляет прямая утечка NTLM-хэшей. Исторически известны методы, когда взаимодействие пользователя с вредоносным веб-контентом или файлом, содержащим ссылку на удаленный SMB-ресурс атакующего, приводило к автоматической попытке Windows аутентифицироваться на этом ресурсе, отправляя имя пользователя и хэш его пароля. Злоумышленнику остается лишь перехватить этот хэш. Хотя сам пароль не передаётся в открытом виде, полученный хэш может быть использован в атаках типа Pass-the-Hash для аутентификации на других системах от имени пользователя, либо злоумышленник может попытаться восстановить исходный пароль методом перебора, что особенно эффективно при использовании пользователями слабых паролей. Уязвимость, зарегистрированная как CVE-2025-24054, является ярким примером такого рода угроз. Она связана с недостатком типа CWE-73 (External Control of File Name or Path), который позволяет неавторизованному пользователю инициировать спуфинг, приводящий к раскрытию NTLM-хэша [3].

Эксплуатация CVE-2025-24054 требует минимального взаимодействия со стороны пользователя. Злоумышленник может создать специально подготовленный файл, например, файл библиотеки Windows (".library-ms"), который является легитимным типом файла, используемым для агрегации контента из различных расположений. Вредоносный файл ".library-ms" содержит внутри себя путь к SMB-ресурсу, контролируемому атакующим. Когда пользователь взаимодействует с этим файлом – даже просто выделяет его в проводнике, просматривает его свойства или выполняет другое действие, отличное от прямого открытия или запуска – операционная система пытается подключиться к указанному SMB-ресурсу для получения метаданных. Эта попытка подключения инициирует процесс NTLM-аутентификации, в ходе которого хэш пароля пользователя отправляется на сервер злоумышленника.

Наблюдения показывают, что данная уязвимость начала активно эксплуатироваться в фишинговых атаках, нацеленных на правительственные учреждения и частные компании. В некоторых зафиксированных атаках вредоносные файлы ".library-ms" распространялись через ZIP-архивы, отправляемые по электронной почте или через ссылки на облачные хранилища, такие как Dropbox. Примечательно, что позже были обнаружены кампании, где файлы ".library-ms" распространялись напрямую, без архивации, что свидетельствует об адаптации злоумышленниками своих методов для повышения шансов на успех.

Получение NTLM-хэша или успешное проведение NTLM Relay атаки часто является лишь первым шагом для злоумышленника. Дальнейшие действия обычно направлены на закрепление в системе, повышение привилегий и достижение конечных целей. После получения первоначального доступа или компрометации учётных данных, атакующие могут развернуть на зараженном устройстве дополнительное вредоносное программное обеспечение, такое как трояны удаленного доступа (RAT). Подобные инструменты предоставляют широкий спектр возможностей: хищение локальных данных из браузеров (пароли, cookie-файлы, история), доступ к реестру системы, развёртывание программ-шифровальщиков, регистрация нажатий клавиш и движений мыши, получение доступа к веб-камере и микрофону, создание скриншотов экрана, а также загрузка и запуск дополнительных модулей или полезной нагрузки. Коммуникация с командными серверами (Control and Command, C2) и экфильтрация данных часто маскируются под легитимный трафик с использованием общедоступных API, таких как Telegram Bot API или облачные сервисы типа Firebase Realtime, что усложняет их обнаружение сетевыми средствами защиты. Кроме того, современное вредоносное ПО часто включает в себя механизмы противодействия анализу, такие как проверка на запуск в виртуальной среде или использование обфускации кода.

Военные, правительственные и логистические организации представляют особую ценность для атакующих из-за характера обрабатываемой ими информации и критической роли, которую они играют. Успешная компрометация сетей таких организаций через уязвимости NTLM может привести к утечке таких данных с ограниченным доступом, как планов операций, персональных данных сотрудников, нарушению управления войсками, сбоем в работе государственных сервисов или параличу логистических цепочек поставок. Атаки на логистические компании могут быть направлены не только на кражу данных о грузах или клиентах, но и на нарушение физических процессов доставки, что может иметь серьёзные экономические последствия. Использование относительно простых в эксплуатации уязвимостей, таких как CVE-2025-24054, требующих минимального взаимодействия с пользователем, делает фишинговые атаки с использованием вредоносных файлов ".library-ms" эффективным инструментом для проникновения в целевые сети.

Для противодействия угрозам, связанным с эксплуатацией уязвимостей NTLM, организациям необходимо применять комплексный подход к защите. Первоочередной мерой является своевременное применение обновлений безопасности, выпускаемых производителем ПО, для устранения известных уязвимостей, включая CVE-2025-24054. Однако, учитывая сохраняющиеся риски, связанные с самим протоколом NTLM, необходимы дополнительные шаги по усилению конфигурации систем [4]. Крайне рекомендуется ограничить или полностью отключить исходящий NTLM-трафик к удаленным серверам с помощью групповых политик или настроек реестра операционной системы. В средах, где полное отключение NTLM невозможно из-за проблем совместимости, следует использовать списки исключений для разрешения NTLM-аутентификации

только с доверенными серверами. Важными мерами для противодействия NTLM Relay являются включение подписи SMB (SMB signing), использование расширенной защиты аутентификации (Extended Protection for Authentication, EPA), отключение неиспользуемых служб, которые могут быть использованы для принудительной аутентификации, и применение RPC-фильтров или межсетевых экранов для блокировки нелегитимных RPC-вызовов к контроллерам домена и серверам AD CS.

Полный переход на более безопасные протоколы аутентификации, такие как Kerberos, и отключение NTLM, где это возможно, является стратегической целью. Помимо технических мер, необходимо уделять внимание повышению осведомлённости пользователей об угрозах фишинга и правилах безопасного обращения с файлами из недоверенных источников. Сетевой мониторинг для выявления аномального SMB-трафика и использование надёжных парольных политик в сочетании с многофакторной аутентификацией также являются важными элементами комплексной системы защиты.

Таким образом, атаки, эксплуатирующие слабости протокола NTLM, продолжают представлять серьёзную угрозу для критически важных организаций. Уязвимость CVE-2025-24054, связанная с раскрытием NTLM-хэшей через специально созданные файлы, демонстрирует, как даже минимальное взаимодействие пользователя может привести к компрометации учётных данных. Активная эксплуатация этой уязвимости в атаках на государственные и коммерческие структуры подчёркивает необходимость постоянной бдительности, своевременного обновления систем и применения проактивных мер по усилению конфигурации. Комплексный подход, сочетающий технические средства защиты, административные политики и обучение пользователей, является ключом к обеспечению устойчивости военных, правительственных и логистических организаций перед лицом современных киберугроз.

Список источников

1. Windows NTLM hash leak flaw exploited in phishing attacks on governments. URL: <https://www.bleepingcomputer.com/news/security/windows-ntlm-hash-leak-flaw-exploited-in-phishing-attacks-on-governments/> (дата обращения: 10.04.2025).
2. New DFSCoerce NTLM Relay attack allows Windows domain takeover. URL: <https://www.bleepingcomputer.com/news/microsoft/new-dfsc coerce-ntlm-relay-attack-allows-windows-domain-takeover/> (дата обращения: 11.04.2025).
3. NTLM Hash Disclosure Spoofing Vulnerability. URL: <https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2025-24054> (дата обращения: 10.04.2025).
4. Microsoft deprecates Windows NTLM authentication protocol. URL: <https://www.bleepingcomputer.com/news/microsoft/microsoft-deprecates-windows-ntlm-authentication-protocol/> (дата обращения: 11.04.2025).

Статья поступила в редакцию 20.04.2025; принята к публикации 10.05.2025

Информация об авторах

Родин А.А. – студент кафедры «Системы информационной безопасности», направление подготовки 10.05.03 – Информационная безопасность автоматизированных систем, профиль «Безопасность автоматизированных систем» ФГБОУ ВО «БГТУ».

Шапенская А.М. – ассистент каф. «СИБ» ФГБОУ ВО «БГТУ».

Вклад авторов

Родин А.А. – идея, сбор материала, обработка материала, частичное написание статьи (50%).

Шапенская А.М. – научное редактирование текста, частичное написание статьи (50%).

Конфликт интересов отсутствует.

Научная статья
УДК 658.7:004.056

Управление киберрисками в экосистеме цифровых цепочек поставок: уязвимости, последствия и стратегии повышения защищенности

Никита Александрович Руденко¹, Федор Евгеньевич Березкин^{2✉}

^{1, 2}Брянский государственный технический университет, Брянск, Россия

¹Rudenkonikita889@gmail.com, <https://orcid.org/0009-0001-8726-3836>

²fedor.berezkin32@yandex.ru[✉], <https://orcid.org/0009-0002-0105-7335>

Аннотация. В статье исследуется проблема обеспечения кибербезопасности современных глобальных цепочек поставок.

Ключевые слова: кибербезопасность, цепочка поставок, управление киберрисками, риски третьих сторон, атака на цепочку поставок, киберустойчивость.

Для цитирования: Руденко Н.А., Березкин Ф.Е. Управление киберрисками в экосистеме цифровых цепочек поставок: уязвимости, последствия и стратегии повышения защищенности // Актуальные проблемы кибербезопасности. Противодействие экстремизму и терроризму в информационной молодежной среде: сборник докладов I межрегиональной научно-практической конференции. – Брянск: БГТУ, 2025. – С. 145 – 150.

Современная глобальная экономика немыслима без сложной и разветвленной сети взаимосвязей, известной как цепочка поставок. Эта система, охватывающая поставщиков сырья, производителей, логистические компании, дистрибьюторов и розничных продавцов, обеспечивает движение товаров и услуг от точки зарождения до конечного потребителя. Цифровизация и интеграция информационных технологий коренным образом трансформировали эти цепочки, повысив их эффективность и прозрачность, но одновременно породив новые, значительные риски. Уязвимости в области кибербезопасности перестали быть проблемой отдельных организаций; они превратились в системную угрозу для всей экосистемы поставок, где компрометация одного звена может вызвать каскадный эффект, затрагивающий множество участников. Злоумышленники все чаще осознают, что атака на менее защищенного партнера в цепочке может стать ключом к проникновению в целевую, более крупную и лучше защищенную организацию, что меняет парадигму угроз и требует пересмотра подходов к управлению рисками [1].

Уязвимость современных цепочек поставок обусловлена их фундаментальными характеристиками: взаимозависимостью и сложностью. Каждая организация в цепи полагается на данные, системы и процессы своих партнеров. Это создает обширную поверхность атаки, простирающуюся далеко за пределы традиционного периметра безопасности отдельной компании. Недостаточная видимость и контроль над практиками кибербезопасности у сторонних поставщиков и подрядчиков являются критической проблемой. Уровень зрелости кибербезопасности может значительно варьироваться между участниками цепочки, от

крупных корпораций с выделенными отделами безопасности до малых предприятий с ограниченными ресурсами [3]. Эта неоднородность создает слабые звенья, которые активно ищут и эксплуатируют злоумышленники. Интеграция информационных технологий (ИТ) с операционными технологиями (ОТ) в производственных и логистических процессах добавляет еще один слой сложности, поскольку системы ОТ часто имеют иные протоколы безопасности и более длительные жизненные циклы, что затрудняет их своевременное обновление и защиту.

Данные, циркулирующие в цепочках поставок, сами по себе представляют огромную ценность и являются привлекательной целью для киберпреступников. Речь идет не только о конфиденциальной коммерческой информации, интеллектуальной собственности или персональных данных клиентов и сотрудников. Критически важными становятся и операционные данные, такие как информация о маршрутах перевозок, графиках поставок, складских остатках и статусах заказов [2]. Получение несанкционированного доступа к этим данным может позволить злоумышленникам не только похитить ценную информацию для продажи или шантажа, но и нарушить логистические операции, вызвать сбои в производстве, перенаправить грузы или даже осуществить физические диверсии. Успешная атака может подорвать доверие между партнерами и нанести серьезный ущерб репутации всех вовлеченных сторон. Таким образом, обеспечение конфиденциальности, целостности и доступности данных на всех этапах цепочки поставок становится первостепенной задачей [1, 2].

Спектр кибератак, нацеленных на цепочки поставок, весьма разнообразен и постоянно эволюционирует. Одним из наиболее распространенных и опасных векторов является компрометация поставщиков программного обеспечения. Злоумышленники внедряют вредоносный код в легитимные программные продукты или обновления, которые затем распространяются среди многочисленных клиентов поставщика [5]. Пользователи, доверяя источнику, устанавливают зараженное ПО, предоставляя атакующим доступ к своим системам. Подобные атаки, известные как "supply chain attacks", могут иметь разрушительные последствия, как продемонстрировали инциденты с SolarWinds и Kaseya, затронувшие тысячи организаций по всему миру. Другой вектор связан с компрометацией аппаратного обеспечения на этапе производства или транспортировки, хотя такие атаки сложнее в исполнении, они могут обеспечить глубокий и труднообнаруживаемый уровень доступа [4].

Помимо атак на программное и аппаратное обеспечение, злоумышленники активно используют более традиционные методы для проникновения в системы участников цепочки поставок. Фишинговые атаки, направленные на сотрудников компаний-партнеров, остаются эффективным способом получения учетных данных для доступа к корпоративным сетям или облачным сервисам. Эксплуатация уязвимостей в веб-приложениях, API-интерфейсах, используемых для обмена данными между партнерами, или в системах управления логистикой также является распространенной тактикой [2, 3]. Уязвимости могут существовать как

в системах самой организации, так и в платформах сторонних поставщиков логистических или облачных услуг. Часто целью атаки становится не сама крупная корпорация, а ее менее защищенный поставщик или подрядчик, через системы которого злоумышленники получают плацдарм для дальнейшего продвижения по цепочке [1, 5]. Особую опасность представляют атаки на поставщиков управляемых услуг (MSP), поскольку компрометация одного MSP может открыть доступ к сетям десятков или сотен его клиентов.

Последствия кибератак на цепочки поставок могут быть катастрофическими и многогранными. Прямые финансовые потери включают расходы на восстановление систем, выплату выкупов в случае атак программ-вымогателей, устранение последствий утечки данных, возможные штрафы за нарушение регуляторных требований и судебные издержки. Однако косвенный ущерб часто оказывается значительно выше. Нарушение операционной деятельности – остановка производства, срыв поставок, невозможность обработки заказов – может привести к потере доходов, неустойкам по контрактам и утрате доли рынка [3]. Ярким примером являются атаки на крупные порты или логистические компании, способные парализовать движение товаров на региональном или даже глобальном уровне [2].

Репутационный ущерб от успешной кибератаки на цепочку поставок трудно переоценить. Утрата доверия со стороны клиентов, партнеров и инвесторов может иметь долгосрочные негативные последствия для бизнеса. Компании, ставшие жертвой или источником компрометации в цепочке, рискуют потерять контракты и столкнуться с трудностями в привлечении новых партнеров [1]. Кража интеллектуальной собственности или конфиденциальной коммерческой информации может лишить компанию конкурентных преимуществ. Кроме того, следует учитывать каскадный эффект: инцидент у одного поставщика может вызвать цепную реакцию, затрагивая его клиентов, которые, в свою очередь, могут столкнуться с собственными операционными проблемами и финансовыми потерями. Это подчеркивает взаимозависимость участников и системный характер рисков в современных цепочках поставок [5].

Противодействие киберугрозам в цепочках поставок требует комплексного и проактивного подхода, выходящего за рамки традиционных мер безопасности отдельной организации. Центральным элементом стратегии защиты должно стать управление рисками третьих сторон (Third-Party Risk Management, TPRM) [1]. Это включает в себя тщательную проверку (due diligence) потенциальных и существующих поставщиков и партнеров на предмет их практик кибербезопасности перед установлением деловых отношений. Необходимо оценивать их политики безопасности, процедуры реагирования на инциденты, наличие сертификатов и результаты аудитов. Важно не ограничиваться формальной проверкой, а стремиться к глубокому пониманию реального уровня защищенности партнера. Результаты такой оценки должны учитываться при принятии решений о сотрудничестве и влиять на условия контрактов.

Контрактные обязательства играют ключевую роль в установлении требований к кибербезопасности для всех участников цепочки поставок. В договоры

с поставщиками и партнерами следует включать четкие положения, касающиеся стандартов безопасности, которым они должны соответствовать, процедур уведомления об инцидентах, права на проведение аудита и ответственности за нарушения безопасности [3]. Эти требования должны быть адаптированы к уровню риска, связанного с конкретным поставщиком и характером его доступа к системам и данным. Однако одних лишь контрактных обязательств недостаточно. Необходимо непрерывный мониторинг состояния безопасности партнеров и поставщиков на протяжении всего жизненного цикла сотрудничества. Это может включать использование специализированных платформ для оценки рисков третьих сторон, анализ внешней поверхности атаки партнеров и регулярные пересмотры их практик безопасности [1, 4].

Повышение осведомленности о киберугрозах и обучение персонала являются критически важными компонентами защиты. Это касается не только сотрудников самой организации, но и, по возможности, персонала ключевых партнеров. Регулярные тренинги по распознаванию фишинговых атак, безопасному использованию корпоративных ресурсов и основам кибергигиены могут значительно снизить риск человеческой ошибки, которая часто становится отправной точкой для успешной атаки [3]. Разработка и внедрение безопасных практик на всех этапах жизненного цикла разработки программного обеспечения (Secure Software Development Lifecycle, SSDLC) особенно важны для поставщиков ПО, чтобы минимизировать риск внедрения уязвимостей или вредоносного кода в их продукты [5]. Организациям, использующим стороннее ПО, следует тщательно проверять его безопасность и своевременно устанавливать обновления и патчи.

Технические меры защиты также играют важную роль. Сегментация сети позволяет изолировать критически важные системы и ограничить потенциальный ущерб в случае компрометации одного сегмента. Использование многофакторной аутентификации (MFA), надежных методов шифрования данных при передаче и хранении, систем обнаружения и предотвращения вторжений (IDPS), а также решений для защиты конечных точек (EDR) помогает укрепить оборону. Важно иметь четкий и протестированный план реагирования на инциденты, который бы учитывал специфику атак на цепочку поставок и предусматривал координацию действий с затронутыми партнерами [4]. Обмен информацией об угрозах и индикаторах компрометации между участниками цепочки поставок, возможно, через отраслевые центры обмена и анализа информации (ISACs), может значительно повысить коллективную устойчивость к атакам.

Несмотря на понимание важности проблемы, эффективное управление киберрисками в цепочках поставок сталкивается с рядом серьезных вызовов. Глобальный характер многих цепочек, включающих партнеров из разных стран с различными законодательными и регуляторными требованиями, усложняет стандартизацию подходов к безопасности и обеспечение соответствия. Недостаток прозрачности и видимости вглубь цепочки поставок, особенно на уровне поставщиков второго и третьего уровней, затрудняет полноценную оценку рисков [1]. Стоимость внедрения и поддержания надежных мер кибербезопасности мо-

жет быть непосильной для малых и средних предприятий, которые часто являются неотъемлемой частью цепочек поставок крупных корпораций. Нахождение баланса между обеспечением высокого уровня безопасности и сохранением операционной эффективности и гибкости цепочки поставок также представляет собой сложную задачу [3].

Будущее кибербезопасности цепочек поставок будет определяться дальнейшей цифровизацией, ростом сложности взаимосвязей и постоянной эволюцией тактик злоумышленников. Появление новых технологий, таких как Интернет вещей (IoT), искусственный интеллект (AI) и блокчейн, с одной стороны, открывает новые возможности для оптимизации цепочек поставок, а с другой – создает новые векторы атак и уязвимости, требующие адаптации стратегий защиты. Геополитическая напряженность и кибервойны могут привести к увеличению числа атак, спонсируемых государствами и нацеленных на критическую инфраструктуру и ключевые отрасли, включая их цепочки поставок [5]. Регуляторное давление, вероятно, будет усиливаться, требуя от организаций большей ответственности за безопасность всей своей экосистемы поставок.

В заключение, киберугрозы в цепочках поставок представляют собой одну из наиболее серьезных и сложных проблем современной кибербезопасности. Они затрагивают организации любого размера и отрасли, неся риски значительных финансовых потерь, операционных сбоев и репутационного ущерба. Эффективное противодействие этим угрозам требует перехода от изолированной защиты отдельных организаций к комплексному, экосистемному подходу, основанному на управлении рисками третьих сторон, тесном сотрудничестве между партнерами, внедрении надежных технических и организационных мер, а также постоянной бдительности и адаптации к меняющемуся ландшафту угроз. Обеспечение киберустойчивости цепочек поставок является не просто технической задачей, а стратегическим императивом для поддержания непрерывности бизнеса и стабильности глобальной экономики в цифровую эпоху.

Список источников

1. How to Manage Cyber Risks in the Supply Chain // Alibaba Reads. URL: <https://reads.alibaba.com/ru/how-to-manage-cyber-risks-in-the-supply-chain/> (дата обращения: 18.04.2024).
2. Почему данные о перевозках стали объектом пристального внимания киберпреступников? // Logistic Tools Blog. URL: <https://logistic.tools/ru/blog/tpost/9fr8kgu3s1-pochemu-dannie-o-perevozkah-stali-obekto> (дата обращения: 18.04.2024).
3. Why Cybersecurity Is a Supply Chain Problem in 2023 // Logos3PL Blog. URL: <https://www.logos3pl.com/ru/blog/why-cybersecurity-is-a-supply-chain-problem-in-2023/> (дата обращения: 18.04.2024).
4. Риски в цепочке поставок: от теории к практике // Pentect. URL: <https://pentect.ru/article/postrisk/> (дата обращения: 18.04.2024).

5. Атака на цепочку поставок (Supply Chain Attack) // Anti-Malware.ru.
URL: https://www.anti-malware.ru/analytics/Threats_Analysis/Supply-Chain-Attack
(дата обращения: 18.04.2024).

Статья поступила в редакцию 22.04.2025; принята к публикации 10.05.2025

Информация об авторах

Руденко Н.А. – студент кафедры «Системы информационной безопасности», направление подготовки 10.03.01 – Информационная безопасность, профиль «Организация защиты информации» ФГБОУ ВО «БГТУ».

Березкин Ф.Е. – студент кафедры «Системы информационной безопасности», направление подготовки 10.05.03 – Информационная безопасность автоматизированных систем ФГБОУ ВО «БГТУ».

Вклад авторов

Руденко Н.А. – идея, сбор материала, обработка материала, частичное написание статьи (50%).

Березкин Ф.Е. – идея, сбор материала, обработка материала, частичное написание статьи (50%).

Научный руководитель

Шапенская А.М. – ассистент кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Конфликт интересов отсутствует.

Научная статья
УДК 378:004

Анализ методик идентификации и эксплуатации уязвимостей

Никита Александрович Руденко ¹, Алексей Владимирович Евдокимов ²✉

^{1, 2}Брянский государственный технический университет, Брянск, Россия

¹rudenkonikita889@gmail.com, <https://orcid.org/0009-0001-8726-3836>

²alekseievdokimov05@gmail.com ✉, <https://orcid.org/0009-0004-4331-1279>

Аннотация. В данной статье мы рассмотрим актуальные методики идентификации и эксплуатации уязвимостей, а также статистику, доказывающую эффективность этих методик.

Ключевые слова: информационная безопасность, идентификация уязвимостей, эксплуатация уязвимостей.

Для цитирования: Руденко Н.А., Евдокимов А.В. Анализ методик идентификации и эксплуатации уязвимостей // Актуальные проблемы кибербезопасности и их решения. Противодействие экстремизму и терроризму в информационной молодежной среде: сборник докладов I межрегиональной научно-практической конференции. – Брянск: БГТУ, 2025. – С. 151 – 153.

В цифровом мире, где информация становится одним из самых ценных активов, аудит информационной безопасности играет ключевую роль. Он помогает организациям оценить, насколько эффективно защищены их данные, и выявить потенциальные уязвимости. С учетом растущих киберугроз, понимание процесса идентификации и эксплуатации уязвимостей становится особенно важным для обеспечения безопасности информационных систем. В данной статье будут рассмотрены этапы идентификации и эксплуатации уязвимостей в системе защиты информации.

Рассмотрим методику идентификация уязвимостей. Существуют различные способы, используемые для выявления слабых мест в системах:

1. Использование автоматизированных сканеров уязвимостей - такие инструменты работают как виртуальные детективы, быстро находя известные проблемы, как устаревшие версии программного обеспечения или неправильные настройки. Они помогают сэкономить время и усилия. Согласно исследованию, проведенному в 2024 году компанией "Лаборатория Касперского", более 60% организаций, использующих автоматизированные сканеры, обнаружили уязвимости в своих системах в течение первых 30 дней. Это подтверждает эффективность таких инструментов в быстром выявлении слабых мест [2].
2. Проведение пентеста – специалисты эмулируют атаки на систему, чтобы выявить уязвимости, которые могут быть использованы злоумышленниками. Это позволяет не только обнаружить слабые места, но и понять, как они могут повлиять на организацию. По данным отчета "Касперского", 68% российских компаний, проводивших пентестационное

тестирование, нашли уязвимости, которые не были выявлены другими методами [2]. Это подчеркивает важность эмуляции атак для полноценного обзора состояния безопасности системы.

3. Анализирование кода – данный процесс потребует глубоких познаний в программировании. Ревизия исходного кода приложений помогает выявить уязвимости, такие как SQL-инъекции или XSS. В какой-то степени, это напоминает поиск иголки в стоге сена, но может предотвратить серьезные проблемы в будущем. Исследование, проведенное в 2021 году, показало, что более 75% уязвимостей веб-приложений в России связано с проблемами в исходном коде. Регулярный анализ кода может снизить вероятность возникновения таких уязвимостей на 35% [3].
4. Проведение оценки конфигураций – анализ настроек серверов, сетевых устройств и приложений помогает обнаружить неправильные конфигурации, которые могут привести к уязвимостям. По данным "ИнфоТеКС", неправильные конфигурации составляют до 25% всех уязвимостей в системах. Оценка конфигураций помогает выявить критические проблемы, и 45% организаций, проводивших такие оценки, смогли устранить уязвимости [4].

После того, как уязвимости были выявлены, следующим важным шагом является их эксплуатация. Этот процесс позволяет понять, насколько серьезными могут быть последствия и какие данные могут оказаться под угрозой. Рассмотрим основные аспекты эксплуатации уязвимостей более подробно:

1. Оценка рисков – на данном этапе важно определить уровень риска, связанного с каждой уязвимостью. Это помогает понять, какие проблемы требуют своевременного внимания. Уязвимости с высоким уровнем риска могут привести к значительным потерям, поэтому их следует устранять в первую очередь. Согласно отчету "Альт Тек", более 70% кибератак в России связаны с известными, но не устраненными уязвимостями. Оценка рисков позволяет определить приоритеты и понять, какие проблемы требуют немедленного внимания [2].
2. Разработка сценариев атак – разработка различных сценариев, в которых уязвимости могут быть использованы, помогает оценить потенциальный ущерб и последствия для бизнеса. Это как создание "учебных" атак, которые показывают, как злоумышленники могут воспользоваться найденными уязвимостями. Исследование, проведенное в 2023 году, показало, что 80% организаций, разработавших сценарии атак, смогли значительно улучшить свои меры безопасности. Это помогает оценить потенциальный ущерб и подготовить команду к реальным угрозам [1].
3. Составление документации и ведение отчетности – необходимо своевременно документировать все найденные уязвимости и методы их эксплуатации. Это поможет в дальнейшем анализе, и является основой для разработки стратегий по улучшению безопасности. Качественно подготовленная документация позволяет командам быстрее реагировать на угрозы и улучшать защиту. По данным исследования "Роскачества", 75%

организаций с тщательной документацией по уязвимостям могут быстрее реагировать на угрозы. Это подчеркивает важность систематического подхода к документированию и отчетности [4].

Подводя итоги, идентификация и эксплуатация уязвимостей – это неотъемлемая часть обеспечения информационной безопасности. Данные процессы помогают организациям не только выявлять слабые места в своих системах, но и разрабатывать эффективные стратегии для их устранения. В условиях постоянно меняющихся угроз важно регулярно проводить аудит и обновлять меры безопасности, чтобы защитить информацию и сохранить доверие клиентов, особенно потому, что безопасность – это не просто задача, а постоянный процесс, который требует внимания и ресурсов.

Список источников

1. Системы классификации и оценки уязвимостей и угроз информационных систем: какие они бывают и зачем нужны. URL: <https://habr.com/ru/companies/bastion/articles/706884/>.
2. Отчеты о состоянии киберугроз и безопасности информационных систем в России. URL: <https://ics-cert.kaspersky.ru/publications/reports/>.
3. Результаты расследования инцидента утечки БД пользователей сайта ИнфоТеКС. URL: <https://infotecs.ru/press-center/publications/rezultaty-rassledovaniya-intsidenta-utechki-bd-polzovateley-sayta-infotecs/>.
4. Документация и отчетность. URL: <https://roskachestvo.gov.ru>.

Статья поступила в редакцию 22.04.2025; принята к публикации 10.05.2025

Информация об авторах

Руденко Н.А. - студент кафедры «Системы информационной безопасности», направление подготовки 10.03.01 – Информационная безопасность ФГБОУ ВО «БГТУ».

Евдокимов А.В. – студент кафедры «Системы информационной безопасности», направление подготовки 10.05.03 – Информационная безопасность автоматизированных систем ФГБОУ ВО «БГТУ».

Вклад авторов

Руденко Н.А. - идея, сбор материала, обработка материала, частичное написание статьи (50%).

Евдокимов А.В. – частичное написание статьи, обработка материала (50%).

Научный руководитель

Шапенская А.М. – ассистент кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Конфликт интересов отсутствует.

Научная статья
УДК 001.891.57

Актуальность высококачественной обработки информации в регионах Российской Федерации

Михаил Юрьевич Рытов^{1✉}, Виталий Александрович Шкаберин^{2✉}

^{1, 2}Брянский государственный технический университет, Брянск, Россия

¹rmy@tu-bryansk.ru[✉]

²vash@tu-bryansk.ru[✉]

Аннотация. В статье оценивается важность обеспечения качества обработки информации в регионе, как основном элементе системы управления Российской Федерацией. Рассмотрена типовая региональная система управления.

Ключевые слова: региональное управление, качество обработки информации, сложно-организованные системы.

Для цитирования: Рытов М.Ю., Шкаберин В.А. Актуальность высококачественной обработки информации в регионах Российской Федерации // Актуальные проблемы кибербезопасности. Противодействие экстремизму и терроризму в информационной молодежной среде: сборник докладов I межрегиональной научно-практической конференции. – Брянск: БГТУ, 2025. – С. 154 – 157.

Задачи государства в современных условиях сложны и многогранны. Россия, следуя путем эволюционного развития, последовательно осуществляет глубокие преобразования политической, социально – экономической систем нашего государства, направленные на обеспечение эффективного функционирования и всестороннего развития общества, его сохранение, удовлетворение интересов и потребностей граждан.

Особое значение для современной России, страны с огромной территорией и чрезвычайно разнообразными географическими, природно-климатическими и экономическими условиями производства и жизни людей, является поступательное социально-экономическое развитие регионов [2].

Регионы Российской Федерации, являясь неотъемлемой частью государства, непосредственно участвуют в реализации государственных задач, направляют усилия на обеспечение достойного уровня жизни населения, повышение его благосостояния и безопасности. Именно они являются тем звеном государственного управления, развитие которого определяет все социально-экономическое развитие страны.

Современное понимание определения «регион» изложено в Указе Президента Российской Федерации от 3 июня 1996 г. за № 803 «Об основных положениях региональной политики в Российской Федерации»: «Под **регионом** понимается часть территории Российской Федерации, обладающая общностью природных, социально-экономических, национально-культурных и иных условий. Регион может совпадать с границами территории субъекта Российской Федерации либо объединять территории нескольких субъектов Российской Федерации».

Федерации». Поэтому в настоящее время сложилось представление о регионе как о самоуправляемой территории, то есть как о субъекте Российской Федерации. Под регионом подразумевается субъект Российской Федерации – республика, край, область [3].

Таким образом, регион является структурным элементом в системе административно-территориального устройства государственной власти как система представляет собой:

часть территории, где существует система связи между хозяйственными субъектами;

подсистему всего социально-экономического комплекса страны;

сложный территориально-экономический комплекс со своей структурой связи с внешней и внутренней средой.

В целом, регион рассматривается как сложное соединение многочисленных звеньев производственных систем и социальной инфраструктуры, объединенных единой территорией, хозяйственной организацией и соответствующими управленческими структурами.

Регион как единое целое выступает в системе государственного управления в качестве объектной подсистемы и одновременно в качестве самоуправляемой системы (субъектной), организующей процессы социального, экономического и экологического развития на конкретной территории.

Регион как объект государственного управления испытывает на себе воздействие федеральных органов власти и управления, которые сосуществуют с регионом в единой законодательной среде, одновременно он является подсистемой Федерации, которая состоит из отдельных элементов, призванных обеспечить собственную жизнедеятельность региона.

В тоже время регион выступает в качестве субъекта самоуправления на уровне собственной жизнедеятельности в пределах компетенции, определенной законодательством Российской Федерации о разграничении полномочий между субъектами Российской Федерации и центром.

Регион как объект государственного управления представляет собой сложную открытую систему. Модель структуры социально-экономической системы региона представлена на рис.1.

Высшим уровнем структурной организации региона является система управления. Субъектами управления в регионе являются территориальные органы федеральных органов государственной власти, органы управления субъектом Федерации и органы местного самоуправления, которые зачастую имеют пересекающиеся, но не всегда совпадающие интересы. В результате система управления регионом приобретает довольно сложную структуру.

Субъекты территориального (регионального) управления (управляющая системарегиона) включает в себя законодательный и исполнительный органы государственной власти, хозяйственные, коммерческие и общественные структуры.

Объектом управления в регионе является весь его хозяйственный и социально-экономический комплекс, который формируется независимо от выбора набора отраслей, ведомственной подчиненности и форм собственности предпри-

ятий, сосредоточенных на данной территории, то есть объектами управления выступают материально-вещественные, финансово-кредитные, трудовые и информационные потоки в общественной системе.

Субъект федерации имеет собственный бюджет, утверждаемый законодательно на региональном уровне [1].

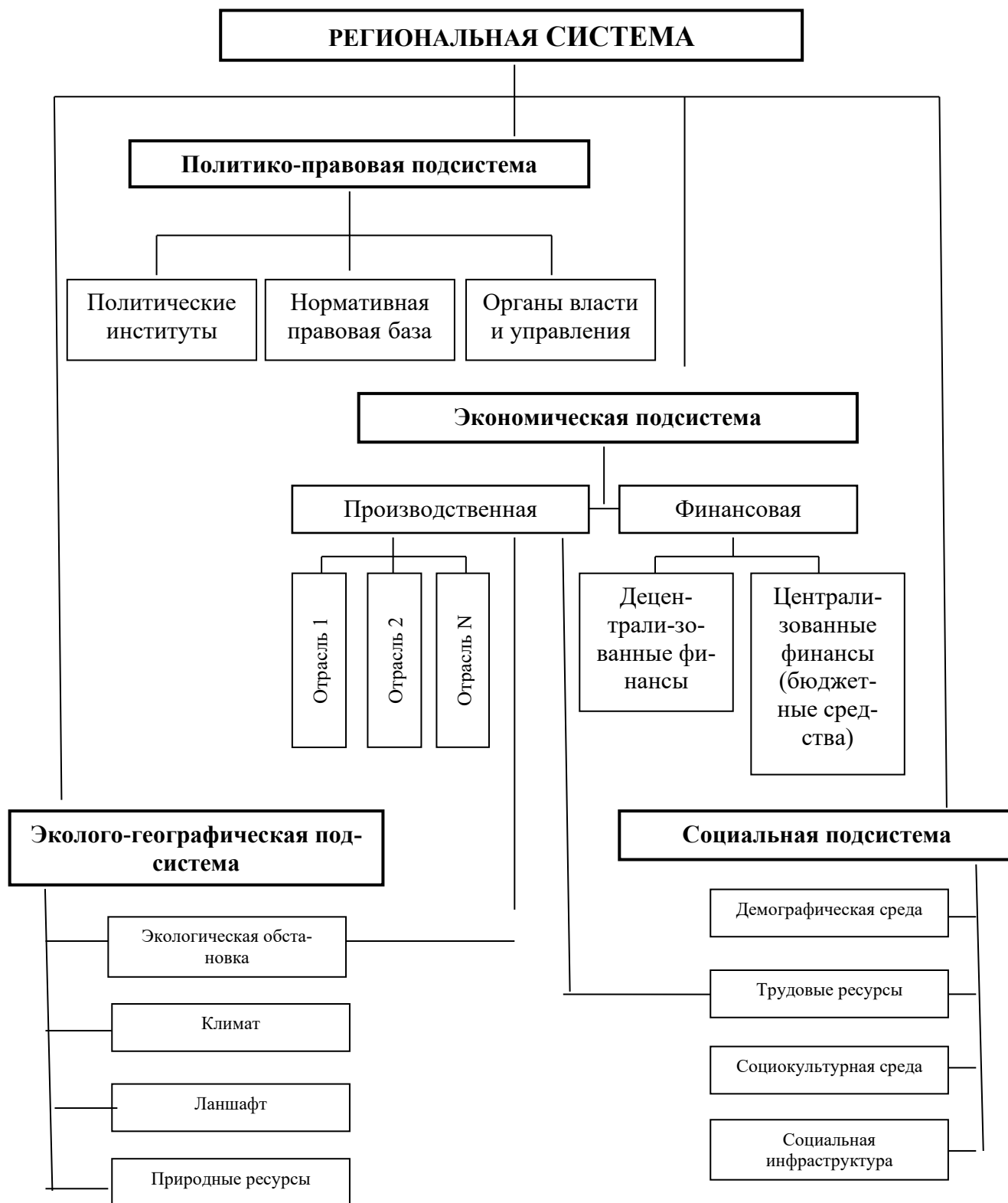


Рис.1. Модель структуры социально-экономической системы региона

Таким образом, основываясь на проведенном исследовании можно сделать вывод о том, что регион представляет собой сложноорганизованную систему управления, характеризующуюся значительным набором свойств и обладающих множеством связей образующих элементов. Общеизвестно, что взаимодействие структурных элементов любой системы управления осуществляется посредством обмена информацией. Следовательно, эффективное функционирование и развитие региона находится в прямой зависимости от знания, своевременности, полноты и качества информации, умения использовать ее в процессе управления. Особую роль в данном процессе играет возможность эффективной, качественной обработки информации, необходимой для принятия обоснованных решений в условиях неопределенности, неполноты и противоречивости исходных данных, в том числе и по вопросам обороны и безопасности в современных условиях.

Список источников

1. Рытов М. Ю. Информационное обеспечение региональных структур исполнительной власти с учетом деструктивных воздействий в мирное и военное время: монография / М.Ю. Рытов, Ю.Ю. Громов // ФГБОУ ВО «ВГЛУ». 2023. - Инв № 81. - 390 с. – Секретно.
2. Рытов М. Ю. Актуальные проблемы управления процессами обработки информации в среде информационных порталов региональных органов исполнительной власти: монография / М.Ю. Рытов, В.Т. Еременко – Тирасполь: Изд-во Приднестр. ун-та, 2017. – 256 с.
3. Рытов М.Ю. Теоретические основы управления обменом данными в среде корпоративного портала промышленного предприятия: монография / М.Ю. Рытов, К.А. Мегаев, С.В. Еременко. – Брянск: БГТУ, 2014. – 196 с.

Информация об авторах

Рытов М.Ю. - д.т.н., доцент, заведующий кафедрой «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Шкаберин В.А. - к.т.н., доцент, первый проректор по учебной работе и цифровизации ФГБОУ ВО «БГТУ».

Вклад авторов

Рытов М.Ю. - идея, сбор материала, обработка материала (60%).

Шкаберин В.А. - написание статьи, научное редактирование текста (40%).

Конфликт интересов отсутствует.

Научная статья

УДК 004.056

Методы обеспечения безопасности информации при передаче данных

Даниил Геннадьевич Таран^{1✉}, Артём Сергеевич Мартынов²,

Александр Сергеевич Шабардин³

^{1,2,3} Межвидовой центр подготовки и боевого применения (учебный и испытательный),

Тамбов, Россия

^{1, 2, 3}nauchnajarota@yandex.ru✉

Аннотация. Статья рассматривает основные концепции и методы обеспечения информационной безопасности при передаче данных. Представлена классификация угроз, возникающих при обработке информации, и описаны подходы к защите данных с применением криптографических алгоритмов и специализированных протоколов. Подчеркивается важность интеграции технических, организационных и правовых мер для эффективного противодействия рискам нарушения конфиденциальности, целостности и доступности информации.

Ключевые слова: информационная безопасность, угрозы информационной безопасности, методы защиты информации, криптографические алгоритмы.

Для цитирования: Таран Д.Г., Мартынов А.С., Шабардин А.С. Методы обеспечения безопасности информации при передаче данных // Актуальные проблемы кибербезопасности. Противодействие экстремизму и терроризму в информационной молодежной среде: сборник докладов I межрегиональной научно-практической конференции. – Брянск: БГТУ, 2025. – С. 158 – 164.

Современное общество характеризуется высокой степенью цифровизации всех сфер жизни, что повышает значимость вопросов информационной безопасности. Обеспечение надежной защиты данных стало необходимым условием успешного функционирования государственных учреждений, коммерческих предприятий и частных лиц. Передача информации через глобальные сети создает новые риски, связанные с возможностью несанкционированного доступа, модификации или утраты важных данных.

Данная работа направлена на изучение ключевых аспектов информационной безопасности, выявление существующих угроз и ознакомление с современными методами защиты информации при ее передаче. Рассматриваются базовые понятия, особенности построения систем защиты и практические рекомендации по выбору оптимальных защитных мер, позволяющих минимизировать риски и обеспечить эффективную защиту данных.

1. Понятие информационной безопасности

Информационная безопасность представляет собой сложный и многокомпонентный механизм, состоящий из множества инструментов и методов, разработанных специально для эффективной защиты цифровой и аналоговой информации. Этот процесс охватывает значительный круг областей информационно-технологического спектра, начиная от инфраструктуры и заканчивая вопросами сетевой безопасности, аудитом и тестированием систем. Среди широко распро-

странённых способов реализации такой защиты выделяются технологии идентификации и авторизации, предназначенные для строгого контроля над правами доступа пользователей и минимизации случаев несанкционированного проникновения к приватным сведениям [1]. Подобные меры обеспечивают снижение вероятности негативных последствий, вызванных нарушением конфиденциальности, повреждением данных или утратой ценных документов.

В широком смысле информационная безопасность затрагивает важные аспекты общественной и профессиональной деятельности, объединяя их в единое целое. Так, одним из ключевых элементов выступает состояние защищенности самого информационного пространства, благодаря которому оно развивается и функционирует в интересах граждан, организаций и государства. Другой важный элемент касается состояния используемой инфраструктуры, в частности уровня защищенности аппаратных и программных комплексов, обеспечивающих обработку и хранение информации, причём такая инфраструктура должна функционировать исключительно в предусмотренных целях и не оказывать отрицательного влияния на рабочие процессы. Третьим ключевым элементом является непосредственно сама информация, которая должна оставаться защищённой от внешних посягательств, включая попытки её взлома, фальсификации или потери. В дополнение к этому существуют экономические компоненты информационной безопасности, подразумевающие наличие специализированных управляющих систем и аналитических платформ, нацеленных на поддержку устойчивости производственного сектора, промышленного комплекса, транспортной отрасли и энергетических сетей. Наконец, существенную роль играет финансовая сторона вопроса, предполагающая создание безопасной среды для взаимодействия денежных потоков, защиты банков и поддержания стабильности международных и внутренних платежей.

Формально обеспечение информационной безопасности начинается с выявления всех участников процесса, взаимодействующих с соответствующими информационными ресурсами, и оценки их интересов. Обычно интересы делятся на три основные группы: доступность (способность оперативно получать необходимые услуги), целостность (поддержка достоверности и неизменности данных) и конфиденциальность (предотвращение несанкционированного ознакомления). Все перечисленное позволяет сформулировать общее определение информационной безопасности как способности защищать объекты безопасности от вредоносных действий, которые могли бы негативно повлиять на характеристики информации и инфраструктуры, задействованной в её обработке.

При практическом подходе важно учитывать структуру компьютерной безопасности, состоящую из совокупности технических и административных мер, необходимых для защиты ресурсов персонального компьютера и другой ИТ-инфраструктуры. Здесь ключевую роль играют вопросы обеспечения доступности, целостности и конфиденциальности хранящихся и обрабатываемых данных. Помимо прочего, особое значение приобретает проблема безопасности самих коммуникационных каналов, решаемая путём внедрения специальных методов и приёмов, препятствующих раскрытию конфиденциальных сведений в процессе их передачи. Политика безопасности, формирующаяся в организациях, строится на тщательном анализе вероятных угроз и разработке адекватных

контрмер, регламентирующих поведение сотрудников и взаимодействие с информацией.

Под угрозой информационной безопасности понимается любые события или действия, способные исказить, уничтожить или нанести ущерб ценным информационным ресурсам, связанным с управлением системами, а также используемым программным и техническим инструментариям. Ответ на подобные угрозы даёт комплекс мероприятий по защите информации, направленный на сохранение важнейшей характеристики данных – их целостности, доступности и конфиденциальности. Основные направления подобной деятельности связаны с охраной государственной тайны, коммерческих секретов, личных данных граждан и объектов интеллектуальной собственности.

Эффективность функционирования любой системы защиты информации определяется наличием четкого набора компонентов, обеспечивающих её работоспособность. Одним из них является правовая база, включающая нормативные документы, правила и инструкции, создающие юридический фундамент защиты. Организационное обеспечение предусматривает выделение конкретных подразделений, занимающихся решением проблем безопасности, таких как отделы безопасности и режимных мероприятий. Аппаратное обеспечение обеспечивает техническую сторону дела, используя специализированные устройства и оборудование для мониторинга и охраны информации. Не менее значима роль информационного компонента, представляющего собой базу данных, необходимую для поддержки работы системы защиты. Программное обеспечение реализует выполнение проверок и защиты данных, выступая основным инструментом защиты информации. Математическое обеспечение связано с разработкой алгоритмов, помогающих оценивать степень уязвимости оборудования и выбирать подходящие стратегии защиты. Эргономическое обеспечение способствует удобству работы пользователей с инструментами защиты, повышая общую эффективность всей системы.

Таким образом, информационная безопасность представляет собой сложную конструкцию, включающую разнообразные элементы и уровни, гармонично интегрированные между собой и направленные на решение главной задачи – сохранение ценности и функциональности информации в современном обществе.

2. Классификация угроз информационной безопасности

Под угрозой понимается внешний или внутренний фактор, который способен дестабилизировать работу автоматизированной системы. Современный перечень угроз информационной безопасности автоматизированных систем весьма широк и насчитывает десятки видов потенциально опасных ситуаций [2].

Классификация угроз проводится с учетом особенностей архитектуры современных систем обработки информации. Каждая категория угроз соответствует одному из общих требований к защитным механизмам системы, позволяя детально раскрыть специфику каждой конкретной проблемы.

Поскольку разнообразие факторов, влияющих на накопленную, сохранённую и обработанную информацию, крайне велико, создать исчерпывающий список всех угроз практически невозможно. Поэтому принято выделять классы угроз, сформированных на основании ряда типичных признаков.

Исходя из природы происхождения, угрозы информационной безопасности могут возникать вследствие двух групп факторов:

- Естественных факторов (катастроф природного характера, таких как пожары, наводнения, землетрясения, молнии и прочие стихийные явления).
 - Человеческого фактора.
- Человеческий фактор делится на две подгруппы:
- Случайные, непреднамеренные угрозы, возникающие в результате ошибок в ходе подготовки, обработки и передачи информации (например, неверное оформление документации, ошибки разработчиков ПО, неисправности оборудования из-за низкого качества сборки, ошибки персонала из-за низкой квалификации или неправильных действий операторов).
 - Преднамеренные, осознанные угрозы, инициированные людьми с преступными намерениями. Они могут включать передачу, изменение или уничтожение ценной научной и технологической информации, перехват телефонных переговоров и других деловых обсуждений, организацию нелегального экспорта знаний и компетенций, получение незаконного доступа к компьютерным ресурсам и хранилищам данных путем подключения к вычислительным устройствам и линиям связи, похищение материальных носителей информации (дискет, печатных материалов).

Преднамеренные угрозы условно разделяют на два типа:

- Активные угрозы: представляют собой целенаправленные атаки, направленные на прямое вмешательство в работу системы и нарушение нормальной работы инфраструктуры. Примерами активных угроз могут служить повреждение линий связи, отключение компьютеров, внесение ложных записей в базы данных, распространение вирусов и вредоносных программ.
- Пассивные угрозы: заключаются в попытках скрытого наблюдения за информацией, циркулирующей внутри системы, например, незаконное прослушивание каналов связи с целью перехвата сообщений.

Эти классификации позволяют лучше понять природу и возможные последствия угроз информационной безопасности, что помогает правильно выбрать эффективные защитные мероприятия и обеспечить должный уровень защиты автоматизированных систем.

3. Методы защиты информации

Средства и механизмы информационной безопасности включают в себя процессы и процедуры ограничения доступа, сокрытие информации, создание избыточных данных и избыточных информационных систем (для хранения, обработки и передачи данных), а также применение надежных методов хранения, преобразования и передачи информации. Нормативно-правовые и административные меры стимулирования и контроля также важны для повышения уровня безопасности.

Практически используемые современные технологии защиты информации строятся на основе нескольких базовых сервисов, таких как аутентификация, поддержка целостности данных, контроль доступа и т.д., а также применяются различные механизмы обеспечения безопасности, включая шифрование, цифро-

вые подписи и управление маршрутизацией данных. Но одних только технических средств недостаточно — необходима дополнительная организационная и управленческая деятельность по обеспечению информационной безопасности. Это направление входит в состав четырех ключевых составляющих комплексной системы защиты информации вместе с разработкой специализированного программного обеспечения, производством и эксплуатацией аппаратных средств, а также улучшением криптографических (математических) методов защиты.

Помимо этого, особая задача возникает при защите данных, передающихся по электронным каналам связи, например, через электронную почту, для чего требуются специальные меры защиты.

Примером данного метода является программа Pretty Good Privacy. Программа служит для кодирования файлов, основывается на алгоритме RSA (Rivest-Shamir-Adelman), использующем 2 ключа – открытого и секретного. Открытый ключ распространяется окружению, секретный имеется только у владельца.

В некоторых случаях ключ шифрования показан как линейный массив. Слова состоят из 4 байтов, которые находятся в одном столбце (при представлении в виде прямоугольного массива).

Таблица 1

Представление четырёх байтового ключа шифрования

$a_{0.0}$	$a_{0.1}$	$a_{0.2}$	$a_{0.3}$	$a_{0.4}$	$a_{0.5}$
$a_{1.0}$	$a_{1.1}$	$a_{1.2}$	$a_{1.3}$	$a_{1.4}$	$a_{1.5}$
$a_{2.0}$	$a_{2.1}$	$a_{2.2}$	$a_{2.3}$	$a_{2.4}$	$a_{2.5}$
$a_{3.0}$	$a_{3.1}$	$a_{3.2}$	$a_{3.3}$	$a_{3.4}$	$a_{3.5}$

Входные данные для шифра обозначаются как байты состояния в порядке: $a_{0.0}, a_{1.0}, a_{3.0}, a_{0.1}, a_{3.1} \dots$ Число циклов обозначено как Nr и зависит от значений Nb и Nk.

Таблица 2

Число циклов как функция от длины ключа и длины блока

Nr	Nb = 4	Nb = 6	Nb = 8
Nk = 4	10	12	14
Nk = 6	12	12	14
Nk = 8	14	14	14

Цикловое преобразование состоит из четырёх различных преобразований.
 Round (State, RoundKey)

```
{
ByteSub (State); // замена байт
ShiftRow (State); // сдвиг строк
MixColumn (State); // замешивание столбцов
AddRoundKey (State, RoundKey); // добавление циклового ключа
}
```

В последнем цикле будет отсутствовать функция MixColumn. Преобразование ByteSub представляет собой нелинейную замену байт, выполняемую независимо с каждым байтом состояния.

Таблица 3

Действие ByteSub на каждый бит состояния

$a_{0.0}$	$a_{0.1}$	$a_{0.2}$	$a_{0.3}$	$a_{0.4}$	$a_{0.5}$	$k_{0.0}$	$k_{0.1}$	$k_{0.2}$	$k_{0.3}$
$a_{1.0}$	$a_{1.1}$	$a_{1.2}$	$a_{i,j}$	$a_{1.4}$	$a_{1.5}$	$k_{1.0}$	$k_{1.1}$	$b_{i,j}$	$k_{1.3}$
$a_{2.0}$	$a_{2.1}$	$a_{2.2}$	$a_{2.3}$	$a_{2.4}$	$a_{2.5}$	$k_{2.0}$	$k_{2.1}$	$k_{2.2}$	$k_{2.3}$
$a_{3.0}$	$a_{3.1}$	$a_{3.2}$	$a_{3.3}$	$a_{3.4}$	$a_{3.5}$	$k_{3.0}$	$k_{3.1}$	$k_{3.2}$	$k_{3.3}$

Несмотря на это, модели показали способность различать классы, что позволит улучшить результаты в дальнейшем.

Функция ShiftRow предполагает что последние 3 строки состояния циклически сдвигаются на различное число байт. Строка 1 сдвигается на C1 байт, строка 2 на C2 байт и строка 3 на C3 байт. Значения сдвигов C1,C2,C3 зависят от длины блока Nb. Их величины приведены в таблице 4.

Таблица 4

Величина сдвига для разной длины блоков

Nb	C1	C2	C3
4	1	2	3
6	1	2	3
8	1	3	4

Функция MixColumn преобразует столбцы замешивая их. Столбцы рассматриваются как многочлены и умножаются по модулю $4x+1$ на многочлен $s(x)$, выглядящий следующим образом:

$$s(x) = '03'x^3 + '01'x^2 + '01'x + '02'$$

b_0	02	02	02	02	a_0
b_1	01	02	02	02	a_1
b_2	01	02	02	02	a_2
b_3	03	02	02	02	a_3

Применение этой операции ко всем четырём столбцам состояния обозначено как MixColumn(State).

Таблица 5

Представление действия функции MixColumn на столбцы состояния

$a_{0.0}$	$a_{0.1}$	$a_{0.2}$	$a_{0,j}$	$a_{0.4}$	$a_{0.5}$	$k_{0.0}$	$k_{0.1}$	$b_{0,j}$	$k_{0.3}$
$a_{1.0}$	$a_{1.1}$	$a_{1.2}$	$a_{1,j}$	$a_{1.4}$	$a_{1.5}$	$k_{1.0}$	$k_{1.1}$	$b_{1,j}$	$k_{1.3}$
$a_{2.0}$	$a_{2.1}$	$a_{2.2}$	$a_{2,j}$	$a_{2.4}$	$a_{2.5}$	$k_{2.0}$	$k_{2.1}$	$b_{2,j}$	$k_{2.3}$
$a_{3.0}$	$a_{3.1}$	$a_{3.2}$	$a_{3,j}$	$a_{3.4}$	$a_{3.5}$	$k_{3.0}$	$k_{3.1}$	$b_{3,j}$	$k_{3.3}$

В статье были рассмотрены теоретические основы и практические подходы к обеспечению информационной безопасности при передаче данных. Описаны ключевые понятия и принципы информационной безопасности, классифицированы потенциальные угрозы и представлены основные методы защиты информации.

Проведенный обзор показывает, что успешная реализация мер информационной безопасности требует комплексного подхода, сочетающего применение технических средств защиты, организационных процедур и правового регулирования. Особое внимание уделено современным методам криптографической защиты, таким как алгоритм RSA и протокол PGP, доказавшие свою эффективность в обеспечении конфиденциальности и целостности передаваемых данных.

Таким образом, разработка и внедрение эффективных механизмов защиты информации становятся приоритетными задачами для любых организаций, работающих с чувствительными данными, поскольку надежность и безопасность данных гарантируют стабильное функционирование бизнеса и минимизацию рисков утечки информации.

Список источников

1. Ясенев В.Н., Дорожкин А.В., Сочков А.Л., Ясенев О.В. Информационная безопасность: учебное пособие. - Нижний Новгород: Нижегородский госуниверситет им. Н.И. Лобачевского, 2017. - 198 с.
2. Ломакин П., Шрейн Д. Антихакинг. - М.: Майор, 2002. - 512 с.

Статья поступила в редакцию 19.04.2025; принята к публикации 10.05.2025

Информация об авторах

Таран Д.Г. - старший оператор научной роты войск РЭБ.

Мартынов А.С. - оператор научной роты войск РЭБ.

Шабардин А.С. - оператор научной роты войск РЭБ.

Вклад авторов

Таран Д.Г. - идея, сбор материала, обработка материала, написание статьи (50%).

Мартынов А.С. - написание статьи, научное редактирование текста (30%).

Шабардин А.С. - написание статьи (20%).

Конфликт интересов отсутствует.

Научная статья
УДК 378:004

Исследование средств взлома паролей Hashcat и Patator

Дмитрий Витальевич Устюшенков^{1✉}, Алина Михайловна Шапенская²

^{1, 2}Брянский государственный технический университет, Брянск, Россия

¹dima.ustyushenkov@mail.ru[✉], <https://orcid.org/0009-0005-2376-4200>

²alinashapenskaya@yandex.ru, <https://orcid.org/0009-0007-8434-5848>

Аннотация. В статье анализируются особенности современных инструментов используемых для взлома паролей и методы защиты от них.

Ключевые слова: информационная безопасность, взлом паролей, защита от утечек данных, методы защиты информации, методы взлома паролей.

Для цитирования: Устюшенков Д.В., Шапенская А.М. Исследование средств взлома паролей Hashcat и Patator // Актуальные проблемы кибербезопасности и их решения. Противодействие экстремизму и терроризму в информационной молодежной среде: сборник докладов I межрегиональной научно-практической конференции. – Брянск: БГТУ, 2025. – С. 165 – 168.

В современном мире информационная безопасность играет ключевую роль в защите данных как отдельных пользователей, так и крупных организаций. Одной из наиболее актуальных проблем в этой области является взлом паролей. Пароли остаются основным методом аутентификации, несмотря на их уязвимость к различным атакам. В данной статье мы рассмотрим инструменты для взлома паролей, такие как Hashcat и Patator, а также обсудим, как специалисты пытаются решить эту проблему.

Брутфорс (перебор всех возможных комбинаций) – это метод, при котором злоумышленник пытается подобрать пароль, перебирая все возможные комбинации символов. Этот метод требует значительных вычислительных ресурсов и времени, но может быть эффективен против слабых паролей.

Атака по словарю – в этом случае злоумышленник использует список распространенных паролей или слов из словаря для попытки подбора. Этот метод эффективен против пользователей, которые используют простые и предсказуемые пароли.

Радужные таблицы – это предварительно вычисленные таблицы хэшей, которые позволяют быстро находить соответствия между хэшами и паролями. Этот метод эффективен против коротких паролей.

Социальная инженерия – злоумышленник может попытаться получить пароль через манипуляции с пользователем, например, через фишинговые атаки [1].

Существуют различные инструменты для взлома паролей, в данной статье остановим своё внимание на Hashcat и Patator.

Hashcat – это один из самых мощных инструментов для взлома паролей. Он поддерживает множество алгоритмов хэширования и может работать на CPU и GPU. Hashcat позволяет проводить атаки методом брутфорса, по словарю, а также использовать радужные таблицы. Этот инструмент активно используется как злоумышленниками, так и специалистами по безопасности для тестирования устойчивости паролей [2].

Hashcat широко используется, не только для взлома паролей, но и для их защиты.

В 2021 году компания Have I Been Pwned использовала Hashcat для анализа утечек данных и проверки, насколько легко можно взломать пароли из публичных баз данных. Результаты показали, что более 30% паролей могли быть взломаны за несколько минут.

В 2020 году исследователи из Kaspersky Lab использовали Hashcat для демонстрации уязвимости паролей в IoT-устройствах. Они показали, что большинство устройств используют пароли по умолчанию, которые могут быть взломаны за секунды.

Patator – это универсальный инструмент для проведения атак на различные протоколы аутентификации, такие как SSH, FTP, SMTP и другие. Patator позволяет проводить атаки методом перебора паролей и логинов, что делает его опасным инструментом в руках злоумышленников [3].

Patator широко используется специалистами по информационной безопасности для:

- Тестирования устойчивости систем аутентификации в корпоративных сетях.
- Проведения аудита безопасности и выявления слабых паролей на серверах.
- Восстановления доступа к системам в случае утери пароля (например, в криминалистике).

Hashcat входит в топ-5 самых используемых инструментов для тестирования на проникновение (по данным исследований портала Exploit Database).

Согласно опросу, проведенному среди специалистов по кибербезопасности на платформе GitHub, Hashcat используется более чем 60% респондентов для проведения аудита безопасности и тестирования устойчивости паролей.

На GitHub репозиторий Hashcat имеет более 20 000 звезд и активно поддерживается сообществом, что свидетельствует о его популярности и востребованности.

Согласно исследованиям компании Verizon, около 80% утечек данных связаны с слабыми или украденными паролями. Исследование компании SplashData показало, что самые популярные пароли в 2022 году – это "123456", "password" и "123456789". Такие пароли могут быть взломаны за считанные секунды с использованием инструментов, таких как Hashcat.

Также исследования показывают, что использование двухфакторной аутентификации (2FA) значительно снижает вероятность успешного взлома паролей. Однако, даже с 2FA, слабые пароли остаются уязвимыми к атакам.

На GitHub репозиторий Patator имеет более 4 000 звезд, что свидетельствует о его популярности среди специалистов по кибербезопасности, но при этом он всё же уступает Hashcat.

Согласно опросу, проведенному среди специалистов по безопасности на платформе Reddit, Patator используется более чем 30% респондентов для тестирования уязвимостей в системах аутентификации.

Согласно исследованию компании Rapid7, в 2022 году более 40% успешных атак на SSH-серверы были связаны с использованием инструментов для перебора паролей, таких как Patator.

Вместо простых алгоритмов, таких как MD5 или SHA-1, которые легко взломать с помощью современных инструментов вроде Hashcat, сейчас используются более сложные алгоритмы, например, bcrypt, Argon2, PBKDF2.

Двухфакторная аутентификация повсеместно используется для повышения безопасности учетных записей. Даже если пароль будет взломан, злоумышленнику потребуется второй фактор (например, код из SMS или приложения-аутентификатора) для доступа к системе.

Для предотвращения атак методом перебора (brute-force) были разработаны следующие меры: ограничение количества попыток входа, CAPTCHA, Задержки между попытками входа.

Биометрическая аутентификация (отпечатки пальцев, распознавание лица, сканирование радужной оболочки глаза) становится все более популярной. Она используется в смартфонах, ноутбуках и других устройствах, что снижает зависимость от традиционных паролей [1].

Компании, такие как Apple (Face ID, Touch ID) и Samsung, активно внедряют биометрические методы аутентификации.

Взлом паролей остается серьезной угрозой для информационной безопасности, особенно с учетом доступности инструментов, таких как Hashcat и Patator, которые упрощают этот процесс для злоумышленников. Эти инструменты позволяют быстро и эффективно проводить атаки на пароли, что делает необходимыми меры по защите. Для снижения рисков важно обучать пользователей созданию сложных и уникальных паролей, внедрять многофакторную аутентификацию, а также регулярно проводить аудит безопасности и тестирование на уязвимости. Кроме того, использование систем мониторинга и обнаружения аномалий может помочь своевременно выявлять подозрительную активность. Комплексный подход, включающий эти меры, может значительно повысить уровень защиты и минимизировать угрозы, связанные с кибератаками.

Список источников

1. Кнут Д.Е. Взлом паролей: методологии, инструменты и практика. Москва: Наука.
2. Station X. URL: <https://www.stationx.net/hashcat/> (дата обращения: 06.02.2025).
3. Инструменты Kali Linux. URL: <https://kali.tools/?p=269> (дата обращения: 07.02.2025).

Статья поступила в редакцию 25.03.2025; принята к публикации 10.05.2025

Информация об авторах

Устюшенков Д.В. – студент кафедры «Системы информационной безопасности», направление подготовки 10.05.03 – Информационная безопасность автоматизированных систем ФГБОУ ВО «БГТУ».

Шапенская А.М. – ассистент кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Вклад авторов

Устюшенков Д.В. – идея, сбор материала, обработка материала, частичное написание статьи (50%).

Шапенская А.М. – научное редактирование текста, частичное написание статьи (50%).

Конфликт интересов отсутствует.

Научная статья
УДК 621.376

Исследование возможности модуляции хаотического колебания информационным сигналом для повышения информационной безопасности

Александр Сергеевич Шабардин^{1✉}, Артём Сергеевич Мартынов²,
Даниил Геннадьевич Таран³

^{1,2,3} Межвидовой центр подготовки и боевого применения (учебный и испытательный),
Тамбов, Россия

^{1, 2, 3} nauchnajarota@yandex.ru✉

Аннотация. В данной статье рассматривается возможность применения хаотических колебаний для модуляции их информационным сигналом с целью увеличения устойчивости работы систем связи, а также сокрытия передаваемой информации.

Ключевые слова: модуляция, динамический хаос, генераторы хаотических колебаний, системы связи.

Для цитирования: Шабардин А.С., Мартынов А.С., Таран Д.Г. Исследование возможности модуляции хаотического колебания информационным сигналом для повышения информационной безопасности // Актуальные проблемы кибербезопасности. Противодействие экстремизму и терроризму в информационной молодежной среде: сборник докладов I межрегиональной научно-практической конференции. – Брянск: БГТУ, 2025. – С. 169 – 175.

Открытие нерегулярных хаотических колебаний в детерминированных нелинейных динамических системах различной природы (физических, механических, радиотехнических и других) стало одной из крупнейших научных сенсаций прошлого века [1].

Всего несколько десятилетий назад возникновение хаотических колебаний в технических системах считалось «паразитным», то сейчас явление динамического хаоса - научно обоснованное явление фундаментальной значимости.

Открытие явления динамического хаоса дало исследователям множество идей, где можно использовать хаотические колебания.

Одним из быстро развивающихся направлений в области защиты информации является когерентная цифровая связь на основе детерминированного хаоса. Использование хаотической динамики для генерации сигналов позволяет получить несущие сигналы, похожие на шум по спектральным и статистическим характеристикам, что обеспечивает высокую скрытность передачи данных, а детерминизм порождающей их системы повышает устойчивость к перекрестной помехе.

Появление хаоса в системах обусловлено собственной динамикой нелинейной системы, а не шумами и внешними факторами, поэтому возможно применение хаотических колебаний при создании новых технологий, в частности,

применение хаотических колебаний в качестве несущих для передачи информации.

1. Основы модуляции сигналов

Модуляцией называется изменение одного из параметров высокочастотного несущего колебания по закону модулирующего информационного сигнала. Модуляция применяется для повышения помехоустойчивости передаваемого сигнала (для передачи информационного сигнала по каналам связи с шумами) [1].

Формулу гармонического колебания можно записать в виде:

$$U(t) = U_m * \cos(\omega_0 t + \varphi_0), \quad (1)$$

где U_m – амплитуда, ω_0 – угловая частота, φ_0 – начальная фаза.

При модуляции один или несколько параметров (U_m, ω_0, φ_0) становятся функциями от времени, то есть с течением времени изменяется их значение по закону модулирующего информационного сигнала.

При изменении параметра $U_m(t)$ модуляция называется амплитудной (АМ), при изменении $\omega_0(t)$ – частотной (ЧМ), а $\varphi_0(t)$ – фазовой (ФМ). Существует множество других видов модуляций, например, импульсно-кодовая, широтно-импульсная, квадратурная и т.д. Каждая из них нашла свое применение в областях связи [2].

2. Введение в теорию хаоса

Динамический хаос – явление, состоящее в возникновении в нелинейных динамических системах (объектах любой природы, состояние которых изменяется во времени в соответствии с некоторым динамическим законом) сложных непериодических колебаний с непрерывным спектром [3].

С математической точки зрения устойчивость динамической системы определяется знаками показателя Ляпунова в каждой точке фазовой траектории, которые полностью определяются математической моделью динамической системы и ее текущим состоянием, то есть координатами фазовой точки.

Показатель Ляпунова определяется по формуле:

$$\lambda = \lim_{t \rightarrow \infty} \frac{1}{t - t_0} \ln \frac{d(t)}{d(t_0)}, \quad ((2)$$

где $d(t_0)$ – расстояние между фазовыми траекториями в некоторый момент времени t_0 ; $d(t)$ – в момент времени t .

Хаотические колебания возникают в неустойчивых динамических системах, то есть при положительном показателе Ляпунова.

При описании поведения динамических систем используется понятие фазового пространства (множество всех теоретически возможных состояний динамической системы), в котором состояние системы изображается точкой, а изменение этого состояния во времени – фазовой траекторией, вдоль которой перемещается изображающая точка.

Так как динамические переменные в данном случае являются величинами, а не функциями и число их конечно, фазовое пространство имеет конечную размерность, а математические модели описываются системами дифференциальных уравнений.

Динамический хаос обладает многими свойствами случайных процессов такими, как сплошной спектр мощности, экспоненциально спадающая автокорреляционная функция; непредсказуемость на большие интервалы времени.

Простейшие хаотические системы с непрерывным временем описываются системой, состоящей из трех дифференциальных уравнений. Некоторые хаотические системы представляют собой генераторы, построенные путем добавления одного или нескольких элементов в стандартные генераторы регулярных колебаний. Другие источники хаоса не так просто связать с традиционными электронными генераторами, однако, они также могут быть реализованы с помощью современной элементной базы. Типичными примерами источников хаоса с полутора степенями свободы являются следующие системы.

3. Применение хаотических колебаний в качестве несущей при модуляции сигнала

Существует несколько способов введения полезного информационного сигнала в хаотическое несущее колебание, что значительно повышает степень защиты системы связи, предотвращает перехват передаваемой информации несанкционированным абонентом даже при условии отсутствия шифрующего устройства.

Традиционно используемые в современной телекоммуникационной сфере гармонические волны подвергаются модуляции информационного сигнала посредством изменения амплитуды, частоты либо фазы (подробности см. раздел 1). Приемник, соответственно, занимается обратным процессом — извлечением исходной информации.

Подобным образом возможно осуществить модуляцию и хаотического сигнала полезным информационным сообщением. Основное отличие заключается в следующем: в гармонических сигналах управляемыми параметрами являются лишь амплитуда, частота и фаза, тогда как хаотический сигнал обладает повышенной чувствительностью ко многим другим параметрам, даже небольшие вариации которых приводят к значительным изменениям характеристик волновых процессов.

Возьмем генератор Рёсслера в качестве примера, иллюстрирующего потенциал хаотических колебаний:

$$\begin{cases} \dot{x} = -y - z \\ \dot{y} = d \times x - a \times y \\ \dot{z} = b + z \times (x - c) \end{cases}, \quad (3)$$

Его работа основана на системе дифференциальных уравнений, определяющих движение точки в фазовом пространстве. Параметры a , b , c , d оказывают существенное влияние на форму траектории, и малейшие отклонения этих значений вызывают кардинальные изменения поведения аттракторов, как показано на рис. 1.

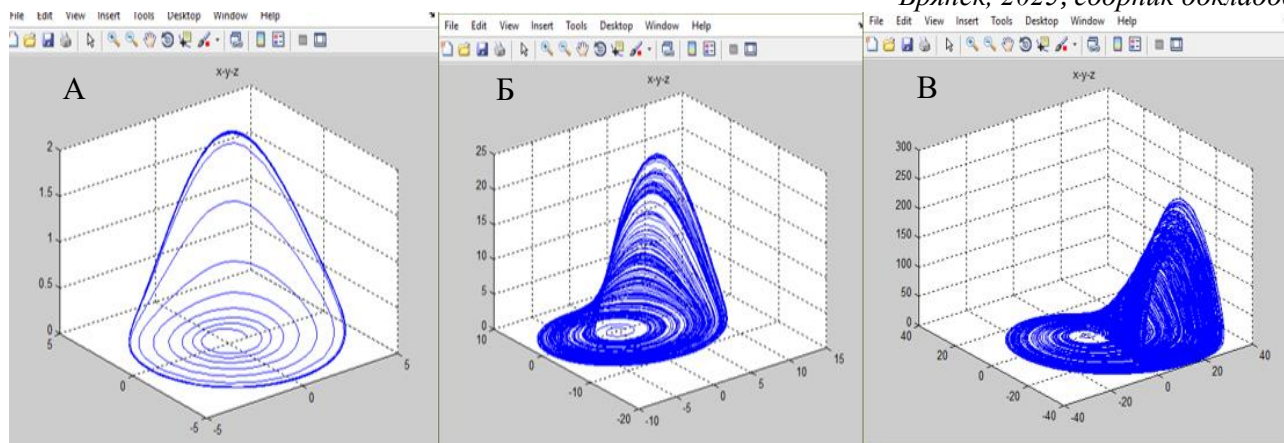


Рис. 1. Изменение аттрактора Рёсслера в зависимости от параметров (рисунок 1-А – $a=0.1$, $b=0.098$, $c=2.5$; рисунок 1-Б – $a=0.2$, $b=0.19995$, $c=5.7$; рисунок 1-В – $a=0.38$, $b=0.368$, $c=14$)

Это значит, что нарушителю потребуется точно восстановить значения параметров a , b , c , d , поскольку любая ошибка здесь ведет к серьезным отклонениям и искажению сигнала.

Однако внедрение хаотических методов коммуникации сопряжено с рядом трудностей:

- Генерация хаотических колебаний должна соответствовать нужной частоте в пределах необходимого диапазона ЭМ-спектра.
- Необходимо разработать способы эффективного внесения информационной нагрузки в хаотический сигнал на передаче и её последующего выделения на приеме.

Кроме того, возникает проблема точности электронных компонентов: любые различия в значениях элементов негативно сказываются на характеристиках системы, затрудняя восстановление оригинального сигнала среди помех хаотической несущей.

Предлагаемый путь преодоления указанных сложностей включает:

- 1) Формирование высокочастотного хаотического сигнала с использованием специально разработанной хаотической динамической системы, чьи свойства оптимизированы под нужды конкретной информационной среды.
- 2) Процесс модуляции подготовленного хаотического сигнала данным полезным информационным сигналом.
- 3) Передача сформированного модулированного сигнала по линии связи.
- 4) Демодуляция принятого сигнала на приемной стороне для извлечения первоначальной информации.

При проектировании хаотической динамической системы важно выбрать область параметров, гарантирующую стабильность и однородность хаотического процесса, учитывая специфику спектральной характеристики формируемого хаотического сигнала.

Структурная схема передающего и принимающего устройств представлена на рис. 2.

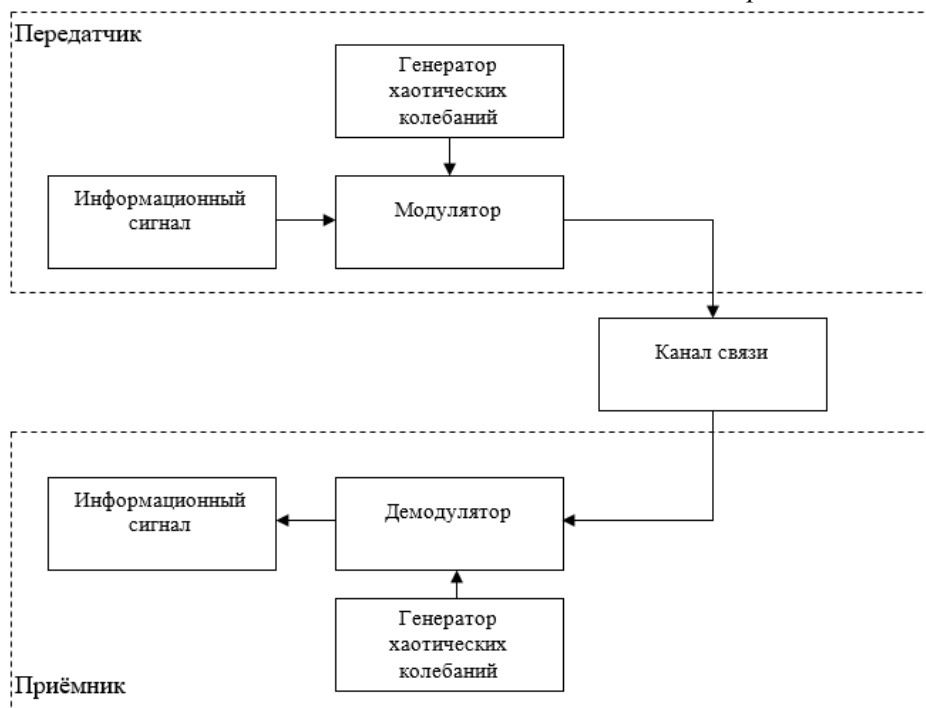


Рис. 2. Структурная схема передатчика и приемника

Сегодня активно исследуются технологии прямого использования хаотических сигналов в беспроводных сетях. Вместо классических непрерывных несущих применяются последовательности хаотичных импульсов, каждый из которых модулируется согласно информационному сигналу, задавая длительность и интервалы следования. Преобразование такого сигнала осуществляется приёмником, синхронизированным с аналогичной динамической системой передатчика.

Альтернативным решением служит использование динамической автоколебательной системы, включающей специальные регуляторы для тонкой настройки режимов генерации широкополосных хаотических сигналов и радиооптических импульсов.

Генераторы хаотических колебаний играют ключевую роль в формировании основных качеств системы, включая статистические, корреляционные и спектральные особенности сигнала.

Современные разработки в области хаотических генераторов основаны на компонентах вроде биполярных и полевых транзисторов, операционных усилителях, диодах с зарядовым накоплением, варикаторах, диодах Чуа и др., позволяющих формировать разнообразные типы хаотических колебаний.

Важным преимуществом хаотических систем является возможность гибкого управления колебаниями за счёт небольших изменений параметров, что обеспечивает быструю модуляцию сигналов и снижает энергопотребление.

Широкая спектрограмма хаотических сигналов позволяет передавать информационные потоки почти равные самой ширине полосы спектра хаотиче-

ского сигнала, сохраняя неизменной ширину и форму спектра. Это упрощает создание не только широкополосных, но и сверхширокополосных (СШП) систем связи.

Такие сверхширокополосные сети идеально подходят для короткодистанционного обмена информацией в промышленных цехах, шахтах и иных ограниченных пространствах с плохими условиями распространения сигнала, а также там, где каналы сильно загружены.

Главным достоинством сверхширокополосных технологий является низкая потребляемая мощность передатчиков, благодаря чему возможна скрытая передача данных. Например, такие сигналы воспринимаются как слабый фоновый шум, делая их незаметными для прослушивания посторонними лицами.

По сравнению с прочими методами сверхширокополосной связи, решение на основе хаотических сигналов демонстрирует высокий уровень безопасности благодаря собственной сложности, непредсказуемым спектральным характеристикам и большому числу степеней свободы, создающим дополнительные трудности для взломщиков.

С помощью модуляции хаотического сигнала может быть осуществлена маскировка передаваемой информации. При правильном выборе способа организации передачи сигнала с помощью модуляции им несущего хаотического колебания выделение полезной составляющей в приемнике может быть осуществлено даже при условии, что хаотическая несущая находится ниже уровня шумов (это позволяет не просто маскировать информацию, а факт ее передачи).

Модуляционная техника хаотических сигналов эффективно скрывает передаваемую информацию, позволяя извлекать полезный сигнал даже в условиях низкого отношения сигнал/шум. Даже если подобный сигнал удастся обнаружить, точное воспроизведение требует знания детальных характеристик используемого генератора хаотических колебаний и метода модуляции, что представляет собой чрезвычайно сложную задачу.

Область практического применения хаотических несущих пока недостаточно изучена, и соответствующие широкополосные системы остаются экспериментальными проектами.

Подводя итог, одним из способов маскировки информационного сигнала может служить модуляция им хаотического колебания, которое в эфире будет выглядеть как незначительный рост шума.

Список источников

1. Куликов Г.В., Нгуен Ван Зунг, Кулагин В.П., Лелюх А.А. Помехоустойчивость приема многопозиционных сигналов М-ФМ и М-КАМ в канале связи с нефлуктуационными помехами // Надежность и качество: труды международного симпозиума. 2020. Т. 2. С. 333–336.
2. Кузина А.В., Шнайдер А.Д., Надырбеков Г.Ж., Лысенко А.В., Аброськин Н.С. Области применения радиосвязи в настоящее время // Надежность и качество: труды международного симпозиума. 2018. Т. 2. С. 317–319.

3. Шахтарин Б.И., Сидоркина Ю.А., Кондратьев А.В., Митин С.В. Генераторы хаотических колебаний: учебное пособие. - М.: Гелиос АРВ, 2007. 248 с.

4. Кармалина В.А. Цифровая обработка случайных колебаний. - М.: Машиностроение, 1986. 80 с.

Статья поступила в редакцию 19.04.2025; принята к публикации 10.05.2025

Информация об авторах

Шабардин А.С. - оператор научной роты войск РЭБ.

Мартынов А.С. - оператор научной роты войск РЭБ.

Таран Д.Г. - старший оператор научной роты войск РЭБ.

Вклад авторов

Шабардин А.С. - идея, сбор материала, обработка материала, написание статьи (50%).

Мартынов А.С. - написание статьи, научное редактирование текста (30%).

Таран Д.Г. - написание статьи (20%).

Конфликт интересов отсутствует.

Научная статья

УДК 004.056

Исследование видов атак на Wi-Fi, осуществляемых при помощи MitM и DoS/DDoS, и способы противодействия им

Александр Александрович Шауло ¹, Артём Андреевич Родин ^{2✉}

^{1, 2}Брянский государственный технический университет, Брянск, Россия

¹a-shaulo@mail.ru, <https://orcid.org/0009-0007-2420-2896>

²temuchrussian@gmail.com [✉], <https://orcid.org/0009-0001-9206-4639>

Аннотация. В статье рассмотрены такие основные виды атак на беспроводные локальные сети (Wi-Fi), как атака типа "Человек посередине" (Man in the Middle), DoS и DDoS-атаки, а также проанализированы основные методы борьбы с ними.

Ключевые слова: информационная безопасность, беспроводная локальная сеть, Wi-Fi, Man in the Middle, Denial-of-Service, шифрование.

Для цитирования: Шауло А.А., Родин А.А. Исследование видов атак на Wi-Fi, осуществляемых при помощи MitM и DoS/DDoS, и способы противодействия им // Актуальные проблемы кибербезопасности. Противодействие экстремизму и терроризму в информационной молодежной среде: сборник докладов I межрегиональной научно-практической конференции. – Брянск: БГТУ, 2025. – С. 176 – 178.

Беспроводные сети Wi-Fi очень распространены в современном мире, обеспечивая доступ к сети Интернет в частных домах, корпоративных зонах и общественных местах. Безопасность таких сетей подвергается угрозам со стороны злоумышленников, применяющих различные типы атак, включая атаки типа Man-in-the-Middle (MitM), отказа в обслуживании (DoS) и распределенные атаки отказа в обслуживании (DDoS). Каждая из таких атак может привести к утечке данных, потере доступа или нарушению работы критически важных систем.

Среди распространенных угроз можно выделить атаки через подмену точки доступа, известные как "evil twin", когда злоумышленники создают фальшивую сеть с именем, идентичным легитимной, чтобы перехватить трафик подключающихся пользователей. Также актуальны атаки, реализуемые методом подбора паролей (brute force, dictionary attack), особенно эффективные против сетей со слабыми паролями или устаревшими протоколами безопасности. Перехват трафика, или "сниффинг", с использованием специализированного оборудования позволяет злоумышленникам получать доступ к незашифрованным или слабо зашифрованным данным, передаваемым по сети.

Атаки типа "человек посередине" (Man-in-the-Middle, MitM) представляют особую опасность, так как позволяют злоумышленнику не только прослушивать трафик, но и активно вмешиваться в сеанс связи, изменяя или подделывая передаваемые данные. Такие атаки могут осуществляться с целью кражи

информации, перехвата сессий, получения несанкционированного доступа к информационным ресурсам, искажения данных или внедрения вредоносного контента. Эффективная борьба с MitM-атаками на сетевом уровне требует применения надёжных алгоритмов шифрования а также создания сложных паролей.

Атаки типа "отказ в обслуживании" (Denial of Service, DoS) и их распределённый вариант (DDoS) нацелены не на кражу данных, а на нарушение доступности сетевых ресурсов. Злоумышленники перегружают сеть, операционную систему или приложение жертвы избыточным трафиком, делая сервисы недоступными для реальных пользователей. По данным QRATORLABS, в 2024 году наблюдается значительный рост DDoS-атак – на 53% по сравнению с 2023 годом, причем самая длительная атака продолжалась более 19 дней [1]. Предотвратить такие атаки сложно и часто требуется фильтрация вредоносного трафика, идущего к защищаемой сети.

Недавние исследования выявили более глубокие уязвимости, связанные с тем, как точки доступа Wi-Fi управляют потоками передачи данных при использовании механизмов энергосбережения [2]. Злоумышленники могут манипулировать флагами состояния энергосбережения в заголовках кадров (протокол 802.11). Это позволяет обмануть точку доступа и заставить её передавать кадры из очереди либо в незашифрованном виде, либо зашифрованными с использованием общего группового ключа, что фактически обходит индивидуальное шифрование для конкретного клиента [3].

Данные уязвимости, связанные с манипуляцией очередями сетевых кадров, также открывают новые векторы для атак отказа в обслуживании. Заставляя точку доступа помещать в очередь критически важные управляющие кадры, злоумышленник может вызвать тайм-ауты и срыв соединения клиента, даже если информационная сеть использует современные стандарты защиты, такие как WPA3 и Management Frame Protection (MFP).

Последствия таких атак весьма серьёзны. Они позволяют перехватывать пользовательский трафик, включая веб-трафик, что может привести к краже cookie-файлов или отслеживанию посещаемых сайтов по IP-адресам, осуществлять перехват TCP-соединений с последующим внедрением вредоносных данных, а также проводить эффективные атаки типа DoS/DDoS.

Таким образом, для защиты от всего спектра угроз необходим комплексный подход. Использование современных протоколов безопасности, таких как WPA3, является обязательным базовым уровнем. Однако выявленные уязвимости показывают необходимость более строгих правил управления очередями сетевых кадров. В сетях типа хот-спот следует применять механизмы, предотвращающие немедленное переподключение устройства-клиента под тем же MAC-адресом без дополнительной проверки подлинности пользователя. Фильтрация MAC-адресов может служить дополнительным барьером, но неэффективна против атак с подменой адреса. Для защиты от DoS/DDoS атак стоит использовать балансировщики нагрузки, системы фильтрации трафика и специализированные сервисы защиты. Наконец, критически важным остаётся

применение сквозного шифрования (например, TLS/HTTPS) на уровне приложений для защиты данных независимо от безопасности Wi-Fi соединения.

Список источников

1. DDoS-атаки, боты и BGP-инциденты в 2024 году: статистика и тренды. URL: https://blog.grator.net/ru/ddos-boty-i-bgp-incidenty-v-2024-godu-statistika-i_210/ (дата обращения: 20.04.2025).
2. Framing Frames: Bypassing Wi-Fi Encryption by Manipulating Transmit Queues. URL: <https://papers.mathyvanhoef.com/usenix2023-wifi.pdf> (дата обращения: 20.04.2025).
3. Уязвимость в протоколе Wi-Fi IEEE 802.11 позволяет перехватывать сетевой трафик. URL: <https://xakep.ru/2023/03/29/ieee-802-11-flaw/> (дата обращения: 11.04.2025).

Статья поступила в редакцию 20.04.2025; принята к публикации 10.05.2025

Информация об авторах

Шауло А.А. – студент кафедры «Системы информационной безопасности», направление подготовки 10.03.01 – Информационная безопасность, профиль «Организация защиты информации» ФГБОУ ВО «БГТУ».

Родин А. А. – студент кафедры «Системы информационной безопасности», направление подготовки 10.05.03 – Информационная безопасность автоматизированных систем, профиль «Безопасность автоматизированных систем» ФГБОУ ВО «БГТУ».

Вклад авторов

Шауло А.А. – идея, сбор материала, обработка материала, частичное написание статьи.

Родин А.А. – идея, сбор материала, обработка материала, частичное написание статьи.

Научный руководитель

Шапенская А.М. – ассистент кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Конфликт интересов отсутствует.

Научная статья

УДК 004.056.53

Анализ уязвимостей Docker-образов с использованием инструмента Trivy

Илья Сергеевич Шишкин¹✉, Денис Александрович Вислобоков²,

Евгений Сергеевич Маленков³

^{1,2}Тамбовский государственный технический университет, Тамбов, Россия

³Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации, Москва, Россия

¹ilya.shis@yandex.ru ✉, <https://orcid.org/0009-0004-6413-8364>

²denis.vislobokov@mail.ru, <https://orcid.org/0009-0006-6986-4132>

³z.malenkov@yandex.ru, <https://orcid.org/0009-0005-9416-1167>

Аннотация. В статье рассмотрены проблемы безопасности docker-образов, связанные с ростом популярности контейнерных технологий и увеличением числа кибератак на контейнерные среды. Представлена классификация уязвимостей docker-образов. Рассмотрен сканер уязвимостей docker-образов Trivy, который выявляет уязвимости разного уровня.

Ключевые слова: Docker; безопасность; технология контейнеризации; контейнеры.

Для цитирования: Шишкин И.С., Вислобоков Д.А., Маленков Е.С. Анализ уязвимостей Docker-образов с использованием инструмента Trivy // Актуальные проблемы кибербезопасности. Противодействие экстремизму и терроризму в информационной молодежной среде: сборник докладов I межрегиональной научно-практической конференции. – Брянск: БГТУ, 2025. – С. 179 – 183.

За последние несколько лет использование технологии контейнеризации обрела большую популярность из-за потребности в сокращении циклов разработки, экономии вычислительных средств и изоляции среды. Контейнерные технологии обеспечивают производительность близкую к нативной и позволяют изолировать каждый контейнер друг от друга, что позволяет избежать конфликта зависимостей [1]. Такая популярность увеличила количество атак на контейнеры из-за чего возникла необходимость в обеспечении безопасности контейнерных сред.

Самой популярной технологией контейнеризации является Docker. Термин Docker имеет несколько значений. Во-первых, это спецификация образов контейнеров и среды выполнения, включая Dockerfiles, позволяющие воспроизводить процесс сборки. Во-вторых, это программное обеспечение, реализующее эту спецификацию, общедоступный репозиторий, который называется DockerHub, где разработчики могут загружать свои образы и делиться ими [2].

Анализ уязвимостей Docker-образов

Угрозы безопасности системы могут появиться ещё в процессе запуска первого контейнера, а именно, скачивание образов docker из сторонних репозиториях. Как показал анализ четырех миллионов общедоступных docker-образов на DockerHub от компании Prevasio, более половины образов имеют критические

уязвимости, а несколько тысяч образов содержат вредоносный код или потенциально опасные элементы [3]. Вне зависимости от первоначальных намерений, если сотрудник какой-либо компании воспользуется DockerHub, а затем запустит образ с майнером на работе, существует высокая вероятность того, что ресурсы компании будут использованы не так, как предполагалось изначально. Системный администратор может счесть такие образы контейнеров нежелательными для корпоративной среды или даже потенциально опасными. Также во время исследования были обнаружены образы с динамическими полезными нагрузками, то есть сам исходный образ не содержал ничего вредоносного, однако позже исходный код майнера загружался, компилировался и выполнялся специальным скриптом.

Уязвимости в docker-образах можно разделить на четыре варианта [4]:

- OS Vulnerabilities – уязвимости базового образа и системных пакетов, включённых в этот образ;
- Dependencies – уязвимости в сторонних зависимостях;
- Software Vulnerabilities – уязвимости непосредственно в коде приложений, которые запускаются в контейнерах;
- Dockerfile – небезопасные инструкции для сборки образа.

Эксплуатация уязвимостей docker-образов может привести к серьезным рискам для безопасности и стабильности всей информационной системы организации:

- нарушение безопасности компонента инфраструктуры: уязвимый образ может стать точкой входа для злоумышленника для получения несанкционированного доступа к другим контейнерам или к основной системе, так как контейнер запускается от привилегированного пользователя, у злоумышленника будет полный доступ к системе;
- заражение вредоносным ПО: в скомпрометированный образ злоумышленник может подкинуть вредоносное ПО, которое будет заражать инфраструктуру или приложения организации. Это может привести к потере данных, нарушению работы критически важных сервисов или неавторизованному задействованию вычислительных мощностей в посторонних целях, что ведет к деградации рабочих процессов и дополнительным финансовым потерям.

Для минимизации рисков, связанных с уязвимыми docker-образами, критически важно внедрять инструменты автоматизированного сканирования на этапах сборки и развёртывания контейнеров. Современные сканеры уязвимостей, такие как Anchore, Clair или Trivy, анализируют содержимое образов, проверяя их на соответствие стандартам безопасности, наличие известных CVE (Common Vulnerabilities and Exposures) и небезопасных конфигураций.

Сканер уязвимостей docker-образов Trivy

Одним из наиболее гибких и популярных инструментов для анализа docker-образов является Trivy-open-source сканер, разработанный Aqua Security. Его ключевые преимущества:

- хорошая документация, содержащая примеры;

- возможность вывода не только на экран, но и в json файл, при этом фильтрую уязвимости по критичности;
- универсальность: поддерживает сканирование не только образов, но и файловых систем, конфигураций Kubernetes, IaC-шаблонов (Terraform, CloudFormation);
- простота интеграции: работает через CLI или встраивается в CI/CD-пайплайны (GitHubActions, GitLab CI, Jenkins);
- актуальность данных: использует компактную и постоянно обновляемую базу уязвимостей, включая данные из NVD (National Vulnerability Database) и репозитории безопасности ОС.

Для проверки докер образа достаточно выполнить команду `trivyimage<название-образа> [4]`. Trivy выведет количество и список уязвимостей с указанием уровня критичности (CRITICAL, HIGH, MEDIUM), их описания и рекомендаций по исправлению.

Например, был просканирован образ самого популярного веб сервера на DockerHub под названием `nginx`. Для этого была введена команда `trivy-imagenginx:stable-perl` после чего начинается процесс сканирование образа (рис. 1).

```
2025-03-20T16:31:45Z INFO [vuln] Vulnerability scanning is enabled
2025-03-20T16:31:45Z INFO [secret] Secret scanning is enabled
2025-03-20T16:31:45Z INFO [secret] If your scanning is slow, please try '--scanners vuln' to disable secret scanning
2025-03-20T16:31:45Z INFO [secret] Please see also https://trivy.dev/v0.60/docs/scanner/secret#recommendation for faster secret detection
2025-03-20T16:31:51Z INFO [javadb] Downloading Java DB...
2025-03-20T16:31:51Z INFO [javadb] Downloading artifact... repo="mirror.gcr.io/aquasec/trivy-java-db:1"
```

Рис. 1. начало процесса сканирования

После завершения сканирования можно увидеть количество уязвимостей (рис. 2).

Report Summary			
Target	Type	Vulnerabilities	Secrets
nginx:stable-perl (debian 12.10)	debian	157	-

Рис. 2. Доклад после завершения сканирования

Также будет отчет об уровнях обнаруженных уязвимостей (рис. 3).

```
Total: 157 (UNKNOWN: 1, LOW: 103, MEDIUM: 36, HIGH: 15, CRITICAL: 2)
```

Рис. 3. Количество уязвимостей разного уровня

И подробный отчет о каждой обнаруженной уязвимости, например, об уязвимости в пакете `libao3`, которой присвоен уровень CRITICAL (рис. 4).

libabsl20220623	CVE-2025-0838	MEDIUM		20220623.1-1		abseil-cpp: Heap Buffer overflow in Abseil https://avd.aquasec.com/nvd/cve-2025-0838
libaom3	CVE-2023-6879	CRITICAL		3.6.0-1+deb12u1		aom: heap-buffer-overflow on frame size change https://avd.aquasec.com/nvd/cve-2023-6879
	CVE-2023-39616	HIGH	will_not_fix			ADMedia v3.0.0 to v3.5.0 was discovered to contain an invalid read mem... https://avd.aquasec.com/nvd/cve-2023-39616

Рис. 4. Отчет о каждой обнаруженной уязвимости

После завершения сканирования docker-образа с использованием инструментов Trivy, начинается этап детального анализа полученных результатов.

Использование docker-образов для ускорения разработки и закрытия конфликтов зависимостей также вызывает риск инцидента безопасности. Анализ показал, что более половины образов в открытом доступе содержат уязвимости. Основными угрозами считаются: уязвимости базового образа; образы, запущенные с правами привилегированного пользователя и заранее инфицированные образы. Для избежание данных угроз необходимо использовать сканеры уязвимостей, которые способны обнаружить уязвимый образ до начала его эксплуатации.

Рассмотренное решение Trivy формирует отчет, который содержит информацию об уровне критичности каждой уязвимости (CRITICAL, HIGH, MEDIUM), её описании, включая тип угрозы, затронутые версии программного обеспечения, а также рекомендации по устранению. Необходимо определить приоритет уязвимостей для компании, выявить системы, на которые влияет каждая уязвимость, а также предоставление информации о ее серьезности, влиянии и основных причинах. Составить руководства и инструкции по устранению уязвимостей. Автоматизация контроля безопасности docker-образов является неотъемлемой частью защиты современных информационных систем.

Список источников

1. Docker: что это такое и как работать с контейнерами. URL: <https://selectel.ru/blog/what-is-docker/>.
2. To Docker or Not to Docker: A Security Perspective. URL: https://www.researchgate.net/profile/Roberto-Pietro/publication/309965523_To_Docker_or_Not_to_Docker_A_Security_Perspective/links/5bd2f7c1a6fdcc3a8da6c5.
3. Анализ 4 000 000 Docker-образов показал, что половина из них содержит критические уязвимости. URL: <https://xakep.ru/2020/12/03/docker-hub-analysis/>.
4. Docker в опасности, или Как искать уязвимости в образах контейнеров. URL: <https://habr.com/ru/companies/nixys/articles/735544/>.

Статья поступила в редакцию 19.04.2025; принята к публикации 10.05.2025

Информация об авторах

Шушкин И.С. – аспирант кафедры «Информационные системы и защита информации», направление подготовки 2.3.6 – Методы и системы защиты информации, информационная безопасность ФГБОУ ВО «ТГТУ».

Вислобоков Д.А. – аспирант кафедры «Информационные системы и защита информации», направление подготовки 2.3.6 – Методы и системы защиты информации, информационная безопасность ФГБОУ ВО «ТГТУ».

Маленков Е.С. – магистрант кафедры «Государственное и муниципальное управление», направление подготовки 38.04.04 – Государственное управление социально-экономическим развитием ФГБОУ ВО «РАНХиГС».

Вклад авторов

Все авторы внесли эквивалентный вклад в подготовку публикации.

Конфликт интересов отсутствует.

СЕКЦИЯ 2. КОМПЬЮТЕРНАЯ КРИМИНАЛИСТИКА

Научная статья

УДК 004:056

Внедрение предмета «Компьютерная криминалистика» в образовательную программу студентов направления «Информационная безопасность»

Максим Михайлович Голембиовский¹, Татьяна Вячеславовна Васина²✉

^{1,2}Брянский государственный технический университет, Брянск, Россия

¹maksim32region@yandex.ru

²tata.vasina.666@gmail.com✉

Аннотация. В статье рассматривается актуальность подготовки специалистов в области компьютерной криминалистики в современных условиях роста киберугроз и информационных преступлений.

Ключевые слова: компьютерная криминалистика, информационные технологии, информационная безопасность.

Для цитирования: Голембиовский М.М., Васина Т.В. Внедрение предмета «Компьютерная криминалистика» в образовательную программу студентов направления «Информационная безопасность» // Актуальные проблемы кибербезопасности. Противодействие экстремизму и терроризму в информационной молодежной среде: сборник докладов I межрегиональной научно-практической конференции. – Брянск: БГТУ, 2025. – С. 184 – 186.

Сегодня информационные технологии являются неотъемлемой частью повседневной жизни общества. Кибератаки, хищение конфиденциальных данных, фишинг-мошенничество, распространение вирусов и другие формы противоправных действий становятся всё более распространёнными явлениями. Эти обстоятельства делают крайне актуальной необходимость подготовки квалифицированных специалистов, обладающих глубокими познаниями в области цифровой криминалистики.

В связи с ростом числа случаев преступных деяний, связанных с применением высоких технологий, возрастает потребность в специалистах, способных проводить полноценные экспертные исследования электронных носителей информации, устанавливать источник нарушений и защищать интересы потерпевших сторон.

Студенческая программа по направлению «Информационная безопасность», дополненная дисциплиной «Компьютерная криминалистика», способна существенно повысить уровень профессиональной подготовки выпускников образовательных учреждений высшего профессионального образования и обеспечить их конкурентными преимуществами на рынке труда.

Цель освоения студентами образовательной программы по специальности «Информационная безопасность» состоит в формировании компетенций, позволяющих успешно решать профессиональные задачи в области предотвращения и реагирования на инциденты информационной безопасности.

Изучение курса «Компьютерная криминалистика» направлено на достижение нескольких основных целей:

- изучение методов и инструментов сбора и анализа цифровых доказательств;
- обучение проведению исследований различных типов цифровых устройств и сетей;
- овладение приёмами анализа вредоносного программного обеспечения и устранения последствий киберинцидентов;
- ознакомление с правовыми основами и процедурами осуществления экспертиз в рамках уголовных дел.

Задачи курса заключаются в следующем:

- освоение методики сохранения целостности и достоверности цифровых доказательств;
- умение пользоваться специализированным программным обеспечением для криминалистического анализа;
- получение навыков идентификации и оценки риска утечки персональных данных;
- анализ современных тенденций развития компьютерной криминалистики и перспектив её применения.

Учебная дисциплина «Компьютерная криминалистика» предусматривает изучение ряда ключевых вопросов, включающих следующие темы:

1. Основы теории судебной информатики и законодательства, регламентирующего проведение экспертиз цифровых доказательств.
2. Методы извлечения и анализа информации с жёстких дисков, SSD-накопителей, мобильных телефонов и планшетов.
3. Особенности проведения онлайн-исследования цифровых сетевых следов (анализ журналов серверов, выявление источников несанкционированного доступа).
4. Методы установления личности пользователей путём анализа метаданных документов и фотографий.
5. Работа с виртуализацией и образами операционных систем для фиксации состояния компьютера на момент инцидента.
6. Выявление скрытых каналов передачи данных и способов обхода средств защиты.
7. Оценка рисков возникновения новых видов киберугроз и разработка мер противодействия.

Для практического изучения приёмов анализа и обработки цифровой информации, студенты могут воспользоваться такими программами, как EnCase Forensic, FTK Imager, Autopsy, X-Ways Forensics и другие, которые широко используются специалистами по всему миру.

Рассматривая перспективы внедрения новой дисциплины, можно отметить, что подготовка студентов по данному профилю позволит готовить кадры высокого уровня компетенции, способных быстро адаптироваться к новым условиям ведения

бизнеса и обеспечивать должный уровень защиты информации во всех сферах жизнедеятельности российского общества.

Для успешной реализации проекта необходимо привлечение опытных преподавателей-практиков, обладающих необходимым уровнем знаний и опыта в проведении судебных экспертиз и консультационной деятельности в области информационной безопасности.

Введение такого важного компонента образовательной программы значительно повысит качество подготовки специалистов и обеспечит дальнейшее развитие научно-технического потенциала России в условиях глобальной конкуренции на мировом уровне.

Таким образом, интеграция дисциплины «Компьютерная криминалистика» в учебный процесс играет ключевую роль в обеспечении эффективного функционирования системы информационной безопасности нашей страны и готовит новое поколение экспертов, способных уверенно отвечать на современные вызовы в области цифровых технологий.

Список источников

1. Цифровая криминалистика: учебник для вузов / под ред. В.Б. Вехова, С.В. Зуева. - М.: Юрайт, 2021.
2. Федотов Н.Н. Форензика – компьютерная криминалистика. – М.: Юридический мир, 2007. – 432 с.

Статья поступила в редакцию 23.04.2025; принята к публикации 10.05.2025

Информация об авторах

Голембиовский М.М. – ассистент кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Васина Т.В. – магистрант кафедры «Системы информационной безопасности», направление подготовки 10.04.01 – Информационная безопасность ФГБОУ ВО «БГТУ».

Вклад авторов

Голембиовский М.М. – идея, сбор материала, обработка материала, научное редактирование текста (60%).

Васина Т.В. – написание статьи, сбор материала обработка материала (40%).

Конфликт интересов отсутствует.

СЕКЦИЯ 3. ИНЦИДЕНТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Научная статья

УДК 004

Исследование важности роли метаданных в инцидентах информационной безопасности

Карина Владимировна Морозова^{1✉}, Павел Дмитриевич Горелов^{2✉},
Диана Игоревна Денисеня^{3✉}, Дмитрий Андреевич Лысов^{4✉}

^{1, 2, 3, 4}Брянский государственный технический университет, Брянск, Россия

¹marus.korotkova@yandex.ru✉, <https://orcid.org/0009-0007-2396-4469>

²pashkayr@yandex.ru✉, <https://orcid.org/0009-0008-7487-6124>

³d.diana1519@gmail.com✉, <https://orcid.org/0009-0004-6440-7632>

⁴lysovdmitriia@gmail.com✉, <https://orcid.org/0009-0003-9666-7191>

Аннотация. Статья посвящена исследованию значимости метаданных в инцидентах информационной безопасности. Рассматриваются различные аспекты использования метаданных, такие как административные, дескриптивные, технические и метаданные цифрового сохранения. Приводятся конкретные примеры реальных инцидентов, связанных с нарушением конфиденциальности и целостности метаданных, демонстрируя необходимость повышенного внимания к защите и управлению метаданными.

Ключевые слова: инцидент информационной безопасности, информационная безопасность, метаданные, стандарт, DeepSeek, io.net, MTC RED SOC.

Для цитирования: Морозова К.В., Горелов П.Д., Денисеня Д.И., Лысов Д.А. Исследование важности роли метаданных в инцидентах информационной безопасности // Актуальные проблемы кибербезопасности. Противодействие экстремизму и терроризму в информационной молодежной среде: сборник докладов I межрегиональной научно-практической конференции. – Брянск: БГТУ, 2025. – С. 187 – 192.

Метаданные – это данные, которые описывают свойства ресурсов, используемых в информационных технологиях. К числу таких ресурсов относятся, в частности, структуры данных и базы данных, программные продукты, веб-сайты и веб-серверы, электронные библиотеки, каталоги и классификаторы содержащихся в них информационных объектов и сами эти объекты, онтологии предметных областей и др. [11].

Необходимо отметить, что в различных стандартах дается разное определение термина «метаданные»:

1. Согласно определению из ГОСТ Р 57668-2017 «Пространственные данные. Метаданные. Часть 1. Основные положения», метаданные – это информация о ресурсе, а ресурс – это идентифицируемый аспект или средства, которые соответствуют требованиям [1].

2. Также исходя из определения, содержащемся в ГОСТ Р 7.0.95-2015 «Национальный стандарт российской федерации. Система стандартов по инфор-

мации, библиотечному и издательскому делу», метаданные – это структурированные данные, описывающие контекст, содержание и структуру электронного документа, предназначенные для его идентификации и поиска, а также процессы управления на протяжении всего жизненного цикла документа [2].

3. Основываясь на определении, данным стандартом ГОСТ Р ИСО 15489-1-2019 "Система стандартов по информации, библиотечному и издательскому делу. Информация и документация. Управление документами. Часть 1. Понятия и принципы", метаданные документов – это структурированная или полуструктурированная информация, которая позволяет создавать, управлять и использовать документы в разное время и в различных областях деятельности. [3].

4. Также в ГОСТ Р ИСО/МЭК 11179-1-2010 «Национальный стандарт Российской Федерации. Информационная технология. Регистры метаданных (РМД). Часть 1. Основные положения» дается более подробное определение метаданных: метаданные – данные, которые определяют и описывают другие данные, при этом в стандарте также даются определения элемента метаданных (экземпляр объекта метаданных), объекта метаданных (тип объекта, определяемый метамоделью), метамодели (модель данных, которая определяет одну или несколько других моделей данных) и модели данных (графическое и/или словесное представление данных, задающее их структуру и взаимосвязи). В данной статье дальнейшее исследование важности роли метаданных в инцидентах информационной безопасности будет проводиться на основе определения данного пункта [4].

Возможны различные подходы к классификации метаданных – по их функциям, по уровням семантической абстрактности, по их свойствам, по уровням информационной архитектуры, к которым относятся описываемые ресурсы, а также по ряду других критериев. Далее приводится один из вариантов классификации метаданных по их назначению:

1. Административные метаданные. Служат для обеспечения управления и администрирования ресурсами данных, а также для поддержки выполнения аналогичных функций по отношению к другим ресурсам информационных технологий.

2. Дескриптивные метаданные. К этому классу относятся, например, схемы баз данных, средства идентификации и описания свойств коллекций информационных ресурсов и отдельных составляющих их ресурсов, каталожные записи электронных библиотек и информация для помощи при поиске в них, индексы DOI публикаций, профили авторов, издателей и пользователей.

3. Метаданные цифрового сохранения. Предназначены для управления сохранением информационных ресурсов. Метаданные этого класса описывают физические условия сохранения ресурсов, предпринятые действия для физического сохранения, сведения о цифровых версиях ресурсов, об изменениях, которые были произведены во время их оцифровки и сохранения.

4. Технические метаданные. Включают, в частности, описание процесса функционирования систем, информацию о технологии проведенной оцифровки

документов, данные аутентификации и обеспечения информационной безопасности (ключи шифрования, пароли).

5. Метаданные об использовании. Описывают характер использования ресурсов, в том числе возможность повторного использования, версии ресурсов, авторские права на ресурсы, включают журнал регистрации доступа пользователей и прочее [5, 11].

Известно большое количество инцидентов информационной безопасности, которые касаются как минимум одного вида метаданных согласно данной классификации.

Так, известен инцидент информационной безопасности, связанный с делом американской юридической фирмы Venable, когда в ходе юридической экспертизы по делу о хищении конфиденциальной информации бывшим сотрудником компании-истца было установлено несоответствие между временными отметками последнего сохранения и даты печати файла: согласно метаданным документа, последний раз файл сохранялся ранее, чем была произведена его последняя печать – ситуация, которую обе стороны признали невозможной. Дело в том, что информация о дате последнего вывода на печать является частью метаданных программы и фиксируется в файле исключительно при его сохранении. Соответственно, если файл был распечатан, но после этого не сохранился заново, сведения о новой дате печати в нём не обновляются. Ещё одним свидетельством фальсификации стало несоответствие метаданных создания файла на корпоративном сервере с фактическим началом судебного процесса: документ появился там уже после старта разбирательств. Дополнительно было выявлено вмешательство в данные о последних изменениях файлов формата OLM, также содержавших признаки манипуляций с датировками.

На основании представленных доказательств суд признал вину ответчиков и обязал их выплатить компенсацию истцу в размере \$20 миллионов вместе с судебными расходами [6].

Также известен случай, когда в апреле 2024 года компания AT&T, один из крупнейших операторов связи в США, выплатила хакеру сумму в размере \$370 тыс., чтобы тот уничтожил похищенную базу метаданных пользователей. Преступники получили несанкционированный доступ к детализированному учёту телефонных разговоров и SMS-сообщений свыше 100 миллионов клиентов оператора за период с 1 мая по 31 октября 2022 года. Уточняется, что украденные данные включают лишь техническую информацию: список номеров, используемых абонентами, количество совершенных звонков и отправленных сообщений, а также суммарную длительность переговоров. Несмотря на отсутствие среди похищенных материалов личных данных вроде имён, адресов проживания или реквизитов банковских счетов, специалисты предупреждают, что имеющейся информации достаточно для выявления другой персональной информации [7].

Эксперты американского IT-стартапа Wiz, специализирующегося на решениях в области облачной безопасности, проанализировали китайскую платформу DeepSeek на уязвимости. В итоге они наткнулись на открытую базу данных с 976

тысячами строк логов, включающую конфиденциальную информацию пользователей – как оказалось, она была просто оставлена «без присмотра».

При тестировании платформы исследователи нашли два открытых сетевых порта (8123 и 9000), обеспечивающих прямой доступ к хранилищу данных, даже не защищённому паролем: к нему можно было обращаться с помощью текстовых команд. После нескольких запросов специалистам удалось извлечь из неё журнал `log_stream`, содержащий 976 тысяч строк. Среди наиболее важной информации были:

- логи с 6 января 2025 года, включающие время сеансов работы;
- текстовые журналы с историей чатов, ключами API, сведениями о серверной части и метаданными;
- данные о происхождении запросов журнала, содержащие историю чатов, ключи API, структуры каталогов и журналы метаданных чат-бота [8].

Используя найденную уязвимость, потенциальные злоумышленники могли бы получить конфиденциальные данные пользователей, включая их сообщения в чате в формате обычного текста, а также похитить пароли, локальные файлы с серверов компании и прочие сведения, относящиеся к метаданным, что повлекло бы серьезные репутационные и финансовые убытки платформы DeepSeek.

Io.net, децентрализованная сеть физической инфраструктуры (DePIN), недавно подверглась взлому. Злоумышленники использовали открытые токены идентификаторов пользователей для выполнения атаки с внедрением языка запросов системы (SQL), которая привела к несанкционированному изменению метаданных устройств в сети графических процессоров (GPU) на уровне пользователя [9].

Несмотря на то, что данный инцидент информационной безопасности не повлек каких-либо критических проблем для компании и пользователей услуг компании, этот случай подчеркнул важность защиты от SQL-инъекций и необходимость тщательного управления идентификационными токенами. Компания Io.net оперативно отреагировала на атаку, применив меры по усилению безопасности: были проведены обновления программного обеспечения, введены дополнительные механизмы авторизации и проверки подлинности запросов, а также проведена внутренняя проверка всей инфраструктуры на наличие аналогичных уязвимостей.

Также важную роль метаданных подчеркивает инцидент информационной безопасности, информация о котором была получена от аналитика центра мониторинга и реагирования на инциденты MTC RED SOC. Антивирусное программное обеспечение центра зафиксировало подозрение на вредоносный файл (`fundapiext.dll`), однако открытые источники (VirusTotal, AlienVault) не содержали информации об этом файле и хэш-сумме. Несмотря на недостаток данных, сотрудники SOC провели собственное расследование и, используя метаданные файла, смогли выявить его связь с деятельностью хакерской группировки Lazarus, известной своими киберпреступлениями [10].

Использование метаданных позволило вовремя выявить угрозу и предотвратить возможное дальнейшее проникновение злоумышленников.

Проведенное исследование показало, что метаданные занимают важную роль в обеспечении информационной безопасности организаций. Метаданные являются важным источником информации, позволяющим выявлять нарушения, предотвращать утечки данных и расследовать инциденты. Важно обеспечить защиту всех компонентов инфраструктуры, включая метаданные устройств. И также стоит отметить, что использование метаданных позволяет эффективно выявлять угрозы и защищать организации от потенциальных рисков.

Таким образом, защита и правильное использование метаданных является необходимым условием для обеспечения информационной безопасности любой организации и для предотвращения возникновения потенциальных инцидентов информационной безопасности. Организации должны уделять особое внимание управлению метаданными, обеспечивая их защиту, сохранность и целостность.

Список источников

1. ГОСТ Р 57668-2017. Пространственные данные. Метаданные. Часть 1. Основные положения // База ГОСТ, ГОСТ Р – национальные стандарты РФ : сайт. URL: https://rososts.ru/file/gost/35/220/gost_r_57668-2017.pdf, свободный (дата обращения: 20.04.2025).
2. ГОСТ Р 7.0.95-2015. Национальный стандарт Российской Федерации. Система стандартов по информации, библиотечному и издательскому делу // Амурский государственный университет : сайт. URL: <https://amursu.ru/upload/files/podrazdeleniya/library/informatsiya-polzovatelyam/reglamentiruyushchaya-dokumentatsiya/gost-r-7.0.95-2015.pdf>, свободный (дата обращения: 20.04.2025).
3. ГОСТ Р ИСО 15489-1-2019. Система стандартов по информации, библиотечному и издательскому делу. Информация и документация. Управление документами. Часть 1. Понятия и принципы // Судебные и нормативные акты РФ: Крупнейшая в сети база судебных и нормативных актов : сайт. URL: <https://sudact.ru/law/gost-r-iso-15489-1-2019-natsionalnyi-standart-rossiiskoi/>, свободный (дата обращения: 20.04.2025).
4. ГОСТ Р ИСО/МЭК 11179-1-2010. Информационная технология (ИТ). Регистры метаданных (РМД). Часть 1. Основные положения // ГОСТ АС-СИСТЕНТ AI : сайт. URL: <https://gostassistant.ru/doc/ff88c358-712c-4009-80fb-6a81cb451386>, свободный (дата обращения: 20.04.2025).
5. Метаданные // Большая российская энциклопедия : сайт. URL: <https://bigenc.ru/c/metadannye-0b2c68>, свободный (дата обращения: 20.04.2025).
6. Venable's \$20-Million-Plus-Sanctions Trade Secrets Win for Government Contractor: What It Means For You // Venable LLP : сайт. URL: <https://www.venable.com/insights/publications/2015/10/venables-20millionplussanctions-trade-secrets-win>, свободный (дата обращения: 20.04.2025).

7. CURRENT REPORT AT&T INC // U.S. Securities and Exchange Commission : сайт. URL: <https://www.sec.gov/Archives/edgar/data/732717/000073271724000046/t-20240506.htm>, свободный (дата обращения: 20.04.2025).

8. Личные данные пользователей DeepSeek слили в сеть // 4PDA : сайт. URL: https://4pda.to/2025/01/30/438053/lichnye_dannye_polzovatelej_deepseek_slili_v_set/, свободный (дата обращения: 20.04.2025).

9. Io.net responds to GPU metadata attack // COINTELEGRAPH The future of money : сайт. URL: <https://cointelegraph.com/news/io-net-responds-to-gpu-metadata-attack>, свободный (дата обращения: 20.04.2025).

10. Доверяй, но проверяй: история расследования инцидента на основе OSINT // Хабр : сайт. URL: https://habr.com/ru/companies/ru_mts/articles/816795/, свободный (дата обращения: 20.04.2025).

11. Когаловский М. Р. Метаданные / М. Р. Когаловский, В. А. Серебряков // Общенациональный интерактивный энциклопедический портал «Знания». 2022. № 9.

Статья поступила в редакцию 20.04.2025; принята к публикации 10.05.2025

Информация об авторах

Морозова К.В. – студент кафедры «Системы информационной безопасности», направление подготовки 10.03.01 – Информационная безопасность ФГБОУ ВО «БГТУ».

Горелов П.Д. – студент кафедры «Системы информационной безопасности», направление подготовки 10.03.01 – Информационная безопасность ФГБОУ ВО «БГТУ».

Денисеня Д.И. – студент кафедры «Компьютерные технологии и системы», направление подготовки 09.03.02 – Информационные системы и технологии ФГБОУ ВО «БГТУ».

Лысов Д.А. – старший преподаватель кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Вклад авторов

Морозова К.В. – идея, сбор материала, обработка материала, написание статьи (25%).

Горелов П.Д. – идея, сбор материала, обработка материала, написание статьи (25%).

Денисеня Д.И. – идея, сбор материала, обработка материала, написание статьи (25%).

Лысов Д.А. – идея, научное редактирование текста (25%).

Конфликт интересов отсутствует.

Научная статья

УДК 004.056.5

Атака хакерами IronHusky государственных информационных систем России и Монголии

Артём Андреевич Родин^{1✉}, Федор Евгеньевич Березкин²

^{1, 2}Брянский государственный технический университет, Брянск, Россия

¹temuchrussian@gmail.com✉, <https://orcid.org/0009-0001-9206-4639>

²fedor.berezkin32@yandex.ru, <https://orcid.org/0009-0002-0105-7335>

Аннотация. В статье анализируется семейство троянов удалённого доступа MysterySnail, изучаются принципы из работы и заражения устройств, а также рассматривается деятельность связанной с данным RAT хакерской группировки IronHusky.

Ключевые слова: хакеры, троян удалённого доступа, программное обеспечение, злоумышленники, информационная безопасность, вредоносный код, фишинг.

Для цитирования: Родин А.А., Березкин Ф.Е. Атака хакерами IronHusky государственных информационных систем России и Монголии // Актуальные проблемы кибербезопасности. Противодействие экстремизму и терроризму в информационной молодежной среде: сборник докладов I межрегиональной научно-практической конференции. – Брянск: БГТУ, 2025. – С. 193 – 196.

В 2025 году группировки типа Advanced Persistent Threat (APT) продолжают представлять серьёзную угрозу для международной кибербезопасности, часто нацеливаясь на государственные организации. Хакерская группировка IronHusky, действующая как минимум с 2017 года, продемонстрировала интерес к государственным информационным системам (ГИС) в России и Монголии. Недавние расследования выявили возобновление активности этой группы, связанное с использованием обновлённых версий трояна удаленного доступа (RAT) MysteryMonoSnail, впервые идентифицированного в 2021 году [1]. Эта активность подчеркивает возможность повторного использования и развертывания старых семейств вредоносных программ.

Недавняя кампания атак, приписываемая IronHusky, была реализована с помощью многоступенчатого процесса заражения, начинающегося с запуска вредоносного скрипта Microsoft Management Console (MMC), замаскированного под документ Microsoft Word. Один из таких файлов был отправлен якобы от Национального агентства земельных ресурсов Монголии (ALAMGAC) (рис. 1).

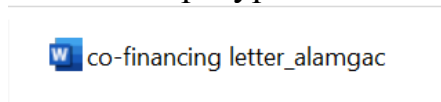


Рис. 1. Фишинговый файл MMC

Этот скрипт был разработан для совершения подгрузки на заражённый персональный компьютер с операционной системой семейства Windows ZIP-ар-

хива, содержащего полезную нагрузку и безвредный файл-обманку с расширением ".docx", из общедоступного сервиса обмена файлами. При его открытии архив распаковывался, а также запускался и добавлялся в автозапуск при загрузке ОС исполняемый файл "CiscoCollabHost.exe".

CiscoCollabHost.exe является легитимным исполняемым файлом, но он использовал изменённую злоумышленниками библиотеку "CiscoSparkLauncher.dll". Данная библиотека реализовывала бэкдор, предназначенный для связи с сервером управления и контроля (Command and Control, C2). Примечательно, что этот бэкдор использовал проект с открытым исходным кодом "ripping-server", взаимодействуя с сервером "https://ppng.io" для получения команд и передачи данных с заражённого устройства. Для противодействия обратному инжинирингу информация об используемых функциях Windows API, хранилась в зашифрованном виде во внешнем файле.

Созданный промежуточный бэкдор обеспечивал реализацию базового функционала, включая выполнение операций в командной строке, передача файлов (загрузка/выгрузка), получение списка каталогов, создание и завершение процессов (рис. 2).

Название команды	Описание команды
RCOMM	Запуск командных оболочек
FSEND	Загрузка файлов с командного сервера
FRECV	Выгрузка файлов на командный сервер
FSHOW	Перечисление содержимого каталога
FDELE	Удаление файлов
FEXEC	Создание нового процесса
REXIT	Завершение работы бэкдора
RSLEE	Переход в спящий режим
RESET	Сброс счетчика времени ожидания соединения с командным сервером

Рис. 2. Перечень доступных злоумышленникам операций

Затем хакеры из IronHusky развёртывали на заражённом устройстве основную полезную нагрузку – MysteryMonoSnail RAT, который был настроен на постоянную работу в виде службы на скомпрометированных операционных системах [2]. Компонент вредоносной DLL загружал финальную полезную нагрузку, хранящуюся во внешнем файле (attach.dat), зашифрованную с использованием криптографических алгоритмов RC4 и XOR. Эта полезная нагрузка запускалась с использованием техники DLL hollowing. Данная техника заключается в загрузке в оперативную память незаражённого исполняемого DLL-файла и подмене части его кода на вредоносный код. Ранее связь для MysterySnail RAT осуществлялась через контролируемые злоумышленниками HTTP-серверы "watch-smcsvc.com" и "leotolstoys.com".

Данный троян удалённого доступа в своих более ранних версиях обладал обширными возможностями, поддерживая около 40 команд для управления файловой системой, выполнения операций в командной строке, манипулирования

процессами и службами, а также подключения к сетевым ресурсам. Изначально весь этот функционал реализовывался одним подгружаемым компонентом. Затем произошёл переход к модульной архитектуре вредоносного программного кода, и недавно обнаруженная версия MysterySnail загружает уже пять дополнительных модулей DLL во время выполнения ("BasicMod.dll", "ExplorerMoudleDll.dll", "process.dll", "cmd.dll", "tcptran.dll") для выполнения определённых категорий команд (рис. 3).

Внутренний идентификатор модуля	Внутреннее имя модуля	Имя DLL-библиотеки модуля	Описание модуля
0	Basic	BasicMod.dll	Позволяет перечислять содержимое дисков, удалять файлы и делать цифровой отпечаток зараженной машины
1	EMode	ExplorerMoudleDll.dll (sic!)	Позволяет считывать файлы, управлять службами и создавать новые процессы
2	PMod	process.dll	Позволяет перечислять запущенные процессы и завершать их
3	CMod	cmd.dll	Позволяет создавать новые процессы и командные оболочки
4	TranMod	tcptran.dll	Позволяет подключаться к сетевым ресурсам

Рис. 3. Дополнительные программные модули и их функции

После обнаружения и нейтрализации первоначальных вторжений с использованием MysterySnail RAT, злоумышленники адаптировали своё программное обеспечение, создав более легковесный вариант, названный MysteryMonoSnail [3]. Эта версия отошла от модульной конструкции своего предшественника. Хотя она использует те же адреса серверов C2, что и ранее связанные с MysterySnail RAT, MysteryMonoSnail взаимодействует с ними с использованием протокола WebSocket вместо HTTP. Также возможности новой версии RAT значительно сокращены, ограничиваясь примерно 13 базовыми командами, в основном сосредоточенными на получении содержимого каталогов, записи файлов и запуске процессов.

Повторное появление и эволюция MysterySnail RAT, используемого группой IronHusky против ГИС в России и Монголии, показывает, что данная группа хакеров сохраняет нацеленность на эти конкретные геополитические регионы, адаптируя свой инструментарий с течением времени, о чём свидетельствует переход к модульности в основной версии MysterySnail, а также создание и использование облегчённого варианта MysteryMonoSnail.

Таким образом, использование актуальных техник по внедрению вредоносных DLL библиотек, шифрование конфигурационных файлов, хранящихся отдельно от самой вредоносной программы, и злоупотребление легитимными проектами с открытым исходным кодом для C2 отражает целенаправленность усилий IronHusky по уклонению от анализа и обнаружения. Приоритет атак на ГИС определённых стран подчеркивает геополитические мотивы, вероятно, ле-

жащие в основе целей этой группировки. Эта кампания служит мощным напоминанием о том, что семейства вредоносных программ, считающиеся спящими или устаревшими, могут быть обновлены и повторно развернуты спустя годы, часто с минимальными изменениями в их основной функциональности. Для противодействия деятельности подобных хакерских группировок требуется поддержание актуальных сигнатур обнаружения для исторических угроз и непрерывный мониторинг активности опознанных АРТ-групп, таких как IronHusky.

Список источников

1. Группа IronHusky обновила MysterySnail для атак на организации в России и Монголии. URL: <https://securelist.ru/mysterysnail-new-version/112317/> (дата обращения: 18.04.2025).
2. IronHusky APT Revives MysterySnail RAT to Target Government Organizations in Russia and Mongolia. URL: <https://www.technadu.com/ironhusky-apt-revives-mysterysnail-rat-to-target-government-organizations-in-russia-and-mongolia/587052/> (дата обращения: 18.04.2025).
3. Один клик — и улитка внутри: как MysterySnail берёт госсистемы под контроль. URL: <https://www.securitylab.ru/news/558466.php> (дата обращения: 18.04.2025).

Статья поступила в редакцию 20.04.2025; принята к публикации 10.05.2025

Информация об авторах

Родин А.А. — студент кафедры «Системы информационной безопасности», направление подготовки 10.05.03 — Информационная безопасность автоматизированных систем, профиль «Безопасность автоматизированных систем» ФГБОУ ВО «БГТУ».

Березкин Ф.Е. — студент кафедры «Системы информационной безопасности», направление подготовки 10.05.03 — Информационная безопасность автоматизированных систем, профиль «Безопасность автоматизированных систем» ФГБОУ ВО «БГТУ».

Вклад авторов

Родин А.А. — идея, сбор материала, обработка материала, написание статьи (50%).

Березкин Ф.Е. — идея, сбор материала, обработка материала, написание статьи (50%).

Научный руководитель

Шапенская А.М. — ассистент каф. «СИБ» ФГБОУ ВО «БГТУ».

Конфликт интересов отсутствует.

Научная статья
УДК 004.056.5

Атака хакерами SideWinder информационных систем стран Африки и Южной Азии

Артём Андреевич Родин^{1✉}, Федор Евгеньевич Березкин²

^{1, 2}Брянский государственный технический университет, Брянск, Россия

¹temuchrussian@gmail.com[✉], <https://orcid.org/0009-0001-9206-4639>

²fedor.berezkin32@yandex.ru, <https://orcid.org/0009-0002-0105-7335>

Аннотация. В статье анализируются техники, применяемые хакерами из группировки SideWinder при проведении атак на информационные системы стран Африки и Южной Азии.

Ключевые слова: программное обеспечение, хакеры, вредоносный код, злоумышленники, фишинг, информационная безопасность.

Для цитирования: Родин А.А., Березкин Ф.Е. Атака хакерами SideWinder информационных систем стран Африки и Южной Азии // Актуальные проблемы кибербезопасности. Противодействие экстремизму и терроризму в информационной молодежной среде: сборник докладов I межрегиональной научно-практической конференции. – Брянск: БГТУ, 2025. – С. 197 – 201.

Развитие информационных технологий и глобальная цифровизация сопровождаются ростом сложности и увеличением масштаба воздействия инцидентов информационной безопасности. Одними из основных субъектов, проводящих подобные атаки, являются хакерские группировки. Они реализуют сложные постоянные угрозы (Advanced Persistent Threats, АРТ). Эти группы обладают значительными ресурсами и высоким уровнем технической подготовки, позволяющим им проникать в защищённые сети и оставаться незамеченными на протяжении длительного времени. Их целями обычно становятся государственные информационные системы (ИС), военные структуры, критическая инфраструктура и крупные корпорации, обладающие ценной информацией или стратегическим значением. Одной из таких активных и постоянно развивающихся групп является SideWinder, чья деятельность представляет серьёзную угрозу для организаций по всему миру, особенно в Южной Азии, Африке и на Ближнем Востоке.

Группировка SideWinder активна предположительно с 2012 года и за время своего существования продемонстрировала способность адаптироваться к меняющимся условиям и совершенствовать свой инструментарий. Исторически её основной фокус был направлен на правительственные и военные организации в таких странах, как Китай, Пакистан, Шри-Ланка, Непал, а также в некоторых регионах Африки [1]. Однако результаты наблюдений, проводимых в течение 2024 и начале 2025 года, указывают на существенное расширение как географии атак, так и перечня подверженных им групп информационных систем.

Исследователи отмечают возросшую активность SideWinder в отношении целей в Джибути и Египте, что свидетельствует о стратегическом интересе к африканскому континенту. Более того, зафиксировано значительное увеличение числа атак на организации морского и логистического секторов, а также на объекты ядерной энергетики, особенно в Южной Азии [2]. Это расширение интересов не означает отказа от прежних целей. Атаки на военные, дипломатические и правительственные ИС продолжаются, но дополняются новыми векторами, что свидетельствует об эволюции набора тактик и техник, применяемых группой. Помимо указанных секторов, под воздействие SideWinder попали телекоммуникационные компании, консалтинговые фирмы, поставщики ИТ-услуг, агентства недвижимости и гостиничный бизнес, что указывает на стремление группы получить доступ к широкому спектру данных [3].

Несмотря на явную техническую изощренность и способность быстро адаптировать свои инструменты для обхода средств защиты, основной вектор атак SideWinder остаётся относительно неизменным и основывается на методах социальной инженерии. Атаки чаще всего начинаются с рассылки фишинговых писем определённым лицам. Эти письма тщательно подготавливаются и маскируются под легитимную корреспонденцию, зачастую с использованием тем, релевантных для конкретной цели [4]. Например, организациям ядерной отрасли могут направляться документы, якобы связанные с предстоящими заседаниями комитетов, в то время как морским и портовым структурам рассылаются поддельные кадровые документы, служебные записки о правительственных решениях или дипломатические сводки. К письмам прилагаются вредоносные документы, как правило, в формате DOCX.

Техническая реализация атаки через вложенные документы использует известную, но всё ещё эффективную методику. Вредоносный DOCX-файл содержит эксплойт для удаленного выполнения кода в Microsoft Office. Хотя данная уязвимость была обнаружена и исправлена производителем ещё в 2017 году, продолжение её использования группой SideWinder подчёркивает проблему несвоевременного обновления программного обеспечения в атакуемых организациях. Эксплуатация уязвимости достигается с помощью техники внедрения удаленного шаблона. При открытии документа он пытается загрузить и выполнить содержимое файла RTF, расположенного на удалённом сервере, контролируемом злоумышленниками. Этот RTF-файл содержит вредоносный код, который, в свою очередь, инициирует многоступенчатый процесс заражения системы.

После успешной эксплуатации данной уязвимости запускается сложная цепочка заражения, направленная на закрепление в системе и развёртывание основного инструментария. Вредоносный код инициирует выполнение кода на языке JavaScript, который, в свою очередь, злоупотребляет стандартной утилитой Windows "mshta.exe". Эта утилита используется для загрузки и выполнения вредоносного HTA-файла с удалённого сервера злоумышленников. Данный HTA-файл содержит обфусцированный (усложнённый для чтения и анализа) JavaScript-код, выполняющий роль загрузчика следующего уровня вредоносного ПО.

Этот JavaScript-загрузчик действует в несколько этапов. На первом этапе он загружает различные строки, изначально закодированные с использованием шифра подстановки и сохранённые в виде переменных. Затем он выполняет проверку объёма установленной оперативной памяти и прекращает свою работу, если объём ОЗУ составляет менее определённого уровня (например, 950 МБ), что является одним из методов противодействия анализу в виртуальных средах или песочницах. Если проверка пройдена, закодированные строки используются для загрузки и выполнения второго этапа. Второй этап представляет собой еще один JavaScript-файл, который перебирает каталоги в директории Windows%\Microsoft.NET\Framework\ для определения установленной версии .NET Framework и использует полученное значение для настройки переменной среды COMPLUS_Version. Наконец, второй этап загружает и запускает основной модуль загрузчика (Downloader Module).

Основной модуль загрузчика представляет собой библиотеку .NET, основной задачей которой является сбор информации об установленных средствах защиты (антивирусах) и загрузка следующего компонента – установщика модуля (Module Installer). Более поздние версии этого загрузчика демонстрируют усложненные функции для идентификации защитных решений, используя WMI-запросы для получения не только названия антивируса, но и связанного с ним состояния ("productState"). Кроме того, вредоносное ПО сравнивает имена всех запущенных процессов со встроенным словарём, содержащим уникальные имена процессов, ассоциированных с популярными продуктами безопасности. Этот WMI-запрос выполняется только в том случае, если в системе не обнаружено запущенных процессов Kaspersky, что указывает на целенаправленные усилия по обходу защитных решений, созданных данной компанией.

Завершающим этапом инфекционной цепочки является установка вредоносного ПО, которое исследователи называли "Backdoor Loader". Её основная функция – загрузка в память основного шпионского эксплойта "StealerBot". StealerBot – приватный пост-эксплуатационный инструментальный, используемый исключительно хакерской группой SideWinder. Хотя сам StealerBot оставался относительно неизменным в течение последних наблюдаемых кампаний, его загрузчик (Backdoor Loader) распространялся во множестве вариантов с различными именами файлов. Например, "propsys.dll", "vsstrace.dll", "JetCfg.dll", "policymanager.dll", "winmm.dll" и другие, что указывает на попытки атакующих сделать образцы вредоносного ПО непохожими друг на друга для усложнения их обнаружения. Новые варианты загрузчика также демонстрируют улучшенные методы противодействия анализу, включая более широкое применение техники Control Flow Flattening для запутывания логики выполнения кода. Control Flow Flattening – одна из распространённых техник обфускации исходного кода программы [5]. Данная техника подразумевает разбиение блоков кода (функций, циклов и условных конструкций) на фрагменты, и их организации в бесконечный цикл с оператором "switch", что сильно усложняет анализ алгоритма работы программы.

Способность SideWinder быстро реагировать на обнаружение своих инструментов является одной из ключевых характеристик, подчеркивающих высокий уровень подготовки группы. Наблюдения показывают, что после идентификации их вредоносного ПО средствами защиты, группа способна выпустить новую, модифицированную версию своих инструментов, часто в течение нескольких часов. Эта адаптивность распространяется не только на сами вредоносные файлы, но и на используемые техники. Если срабатывают поведенческие детекторы, хакеры из SideWinder пытаются изменить методы, используемые для закрепления в инфицированной операционной системе и загрузки компонентов. Они также меняют имена и пути своих вредоносных файлов. Использование хорошо поддерживаемого и эффективного вредоносного ПО, такого как StealerBot, в сочетании с быстрой разработкой и адаптацией инструментов, характеризует SideWinder как высокоразвитую и опасную группировку.

Таким образом, деятельность группы SideWinder представляет собой наглядный пример эволюции современных киберугроз. Начав с атак на такие традиционные для кибершпионажа цели, как военные и правительственные структуры в некоторых странах, группа значительно расширила свой географический охват и спектр интересующих отраслей, добавив в него морской, логистический и ядерный секторы, а также объекты критической информационной инфраструктуры. Применение целевого фишинга с использованием тщательно подготовленных документов-обманок, эксплуатация старой, но все еще актуальной уязвимости Microsoft Word, сложная многоступенчатая цепочка заражения и продвинутые методы уклонения от обнаружения, включая быструю адаптацию инструментария, свидетельствуют о высоком профессионализме данной хакерской группировки. Для успешного противодействия таким угрозам требуется ведение комплексного подхода, включающего не только обучение сотрудников методам противодействия фишингу и социальной инженерии, но и внедрение передовых решений для обнаружения инцидентов информационной безопасности и реагирования на них. Постоянный мониторинг активности подобных группировок и обновление защитных средств являются критически важными требованиями для обеспечения высокого уровня защищенности организаций в условиях постоянно меняющегося ландшафта киберугроз.

Список источников

1. Beyond the Surface: the evolution and expansion of the SideWinder APT group. URL: <https://securelist.com/sidewinder-apt/114089/#> (дата обращения: 18.04.2025).
2. APT-группа SideWinder обновила инструментарий и атакует морскую и ядерную отрасли. URL: <https://securelist.com/sidewinder-apt-updates-its-toolset-and-targets-nuclear-sector/115847/> (дата обращения: 18.04.2025).
3. SideWinder APT Targets Maritime, Nuclear, and IT Sectors Across Asia, Middle East, and Africa. URL: <https://undercodenews.com/sidewinder-apt-targets-maritime-nuclear-and-it-sectors-across-asia-middle-east-and-africa-3/> (дата обращения: 18.04.2025).

4. Sidewinder goes nuclear, charts course for maritime mayhem in tactics shift.
URL: https://www.theregister.com/2025/03/10/sidewinder_tactics_shift/ (дата обращения: 18.04.2025).

5. Control Flow Flattening URL: <https://github.com/obfuscator-llvm/obfuscator/wiki/Control-Flow-Flattening> (дата обращения: 18.04.2025).

Статья поступила в редакцию 20.04.2025; принята к публикации 10.05.2025

Информация об авторах

Родин А.А. – студент кафедры «Системы информационной безопасности», направление подготовки 10.05.03 – Информационная безопасность автоматизированных систем, профиль «Безопасность автоматизированных систем» ФГБОУ ВО «БГТУ».

Березкин Ф.Е. – студент кафедры «Системы информационной безопасности», направление подготовки 10.05.03 – Информационная безопасность автоматизированных систем, профиль «Безопасность автоматизированных систем» ФГБОУ ВО «БГТУ».

Вклад авторов

Родин А.А. – идея, сбор материала, обработка материала, написание статьи (50%).

Березкин Ф.Е. – идея, сбор материала, обработка материала, написание статьи (50%).

Научный руководитель

Шапенская А.М. – ассистент каф. «СИБ» ФГБОУ ВО «БГТУ».

Конфликт интересов отсутствует.

Научная статья
УДК 004.056

Использование Microsoft Trusted Signing злоумышленниками

Артём Андреевич Родин ^{1✉}, Алина Михайловна Шапенская ²

^{1, 2}Брянский государственный технический университет, Брянск, Россия

¹temuchrussian@gmail.com [✉], <https://orcid.org/0009-0001-9206-4639>

²alinashapenskaya@yandex.ru, <https://orcid.org/0009-0007-8434-5848>

Аннотация. В статье рассматривается компрометация системы сертификации программного обеспечения Microsoft Trusted Signing злоумышленниками.

Ключевые слова: сертификация, безопасность, программное обеспечение, злоумышленники, цифровая подпись, вредоносный код.

Для цитирования: Родин А.А., Шапенская А.М. Использование Microsoft Trusted Signing злоумышленниками // Актуальные проблемы кибербезопасности. Противодействие экстремизму и терроризму в информационной молодежной среде: сборник докладов I межрегиональной научно-практической конференции. – Брянск: БГТУ, 2025. – С. 202 – 204.

В современном мире в условиях регулярной разработки нового программного обеспечения проверка его подлинности и целостности является неотъемлемой частью любой системы информационной безопасности. Механизмы цифровой подписи исполняемых файлов играют ключевую роль в установлении доверия между разработчиками и пользователями, подтверждая, что ПО не было изменено с момента его проверки и подписания доверенным источником. Операционные системы, такие как Windows, часто полагаются на эти подписи для принятия решений о безопасности, особенно при загрузке драйверов уровня ядра. В ответ на потребность в упрощении и повышении безопасности процесса подписи кода корпорация Microsoft представила облачный сервис Trusted Signing, предназначенный для интеграции управления сертификатами в рабочие процессы разработчиков через платформу Azure [1]. Несмотря на заявленные преимущества в области безопасности, недавние инциденты продемонстрировали, что даже новые, усовершенствованные системы могут стать объектом злоупотреблений.

Сервис Microsoft Trusted Signing, запущенный в 2024 году, был разработан с целью предоставления разработчикам современного и безопасного метода подписи кода. Он позволяет управлять жизненным циклом сертификатов непосредственно в облачной среде, что должно было снизить риски, связанные с компрометацией закрытых ключей, хранимых локально [2]. Предполагалось, что интеграция с существующими программами Microsoft, такими как Microsoft Partner Network (MPN) и Windows Hardware Developer Program (WHDP), обеспечит необходимый уровень проверки разработчиков, запрашивающих сертификаты. Однако, заявления Microsoft об эффективности и безопасности их новой системы

сертификации программного обеспечения оказались не в полной мере достоверными.

Суть инцидента заключается не в техническом взломе самого сервиса Trusted Signing, а в эксплуатации его процессов регистрации и проверки личности. Киберпреступные группы, выдавая себя за легитимных разработчиков или партнеров Microsoft, успешно прошли необходимые этапы верификации и получили доступ к возможностям сервиса. Получив доверенные сертификаты, злоумышленники использовали их для подписи вредоносного программного обеспечения, в частности, драйверов уровня ядра операционной системы.

Подписанные таким образом вредоносные драйверы представляют особую опасность [3]. Наличие действительной цифровой подписи от доверенного центра сертификации позволяет им обходить стандартные механизмы защиты операционной системы Windows, которые требуют наличия действительной подписи для загрузки драйверов, особенно в 64-битных версиях. Это даёт вредоносному коду возможность выполняться с высокими привилегиями в системе, что может быть использовано для отключения защитных решений, кражи конфиденциальной информации, повышения привилегий или развёртывания дополнительных вредоносных модулей, включая программы-вымогатели.

Обнаружение данной активности стало возможным благодаря усилиям исследователей в области кибербезопасности, которые выявили подозрительные драйверы, подписанные с использованием сертификатов, выданных через Trusted Signing. После уведомления корпорация Microsoft провела расследование, подтвердила факт злоупотребления и приняла ответные меры. Эти меры включали отзыв скомпрометированных сертификатов, что сделало их недействительными для дальнейшего использования, а также блокировку учетных записей злоумышленников в соответствующих партнёрских программах. Важно отметить, что сама информационная система Trusted Signing не была скомпрометирована, уязвимым местом оказались процедуры проверки и идентификации разработчиков.

Данный случай подчеркивает главную задачу любой современной системы сертификации ПО: достижение баланса между удобством использования для разработчиков и надёжностью процессов верификации для предотвращения деятельности злоумышленников. Использование такого доверенного сервиса, как Microsoft Trusted Signing, для подписи вредоносного ПО подрывает общую модель доверия, на которой строится безопасность современных операционных систем. Пользователи и системы полагаются на цифровые подписи как на индикатор надёжности, и компрометация этого механизма, даже через эксплуатацию процессов регистрации разработчиков, служит напоминанием о том, что злоумышленники постоянно адаптируют свои тактики и ищут слабые звенья даже в современных и более защищённых системах.

Таким образом, необходимо непрерывное совершенствование процедур проверки личности, мониторинг активности и быстрая реакция на выявляемые угрозы для поддержания целостности и надёжности механизмов сертификации программного обеспечения.

Список источников

1. Microsoft Azure – Secure your Code with Trusted Signing: A Practical Guide. URL: <https://blog.sonnes.cloud/microsoft-azure-secure-your-code-with-trusted-signing-a-practical-guide/> (дата обращения: 10.04.2025).
2. What is Trusted Signing? URL: <https://learn.microsoft.com/en-us/azure/trusted-signing/overview> (дата обращения: 10.04.2025).
3. Trusted Signing: хакеры легализуют вирусы через официальный сервис Microsoft. URL: <https://www.securitylab.ru/news/557628.php> (дата обращения: 11.04.2025).

Статья поступила в редакцию 20.04.2025; принята к публикации 10.05.2025

Информация об авторах

Родин А.А. – студент кафедры «Системы информационной безопасности», направление подготовки 10.05.03 – Информационная безопасность автоматизированных систем, профиль «Безопасность автоматизированных систем» ФГБОУ ВО «БГТУ».

Шапенская А.М. – ассистент кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Вклад авторов

Родин А.А. – идея, сбор материала, обработка материала, написание статьи (50%).

Шапенская А.М. – научное редактирование текста, частичное написание статьи (50%).

Конфликт интересов отсутствует.

Научная статья

УДК 004.056

Анализ крупных утечек данных 2023–2024 годов: причины, последствия и уроки для организаций

Данила Алексеевич Сычев

Брянский государственный технический университет, Брянск, Россия

danila.sychev.13@gmail.com, <https://orcid.org/0009-0008-8816-3731>

Аннотация. В 2023–2024 годах наблюдался значительный рост числа утечек данных в России и мире, затронувших государственные учреждения, корпорации и граждан. В статье рассматриваются ключевые инциденты атак на российские компании. Особое внимание уделяется последствиям для бизнеса и мерам противодействия.

Ключевые слова: утечки данных, персональные данные, конфиденциальная информация.

Для цитирования: Сычев Д.А. Анализ крупных утечек данных 2023–2024 годов: причины, последствия и уроки для организаций // Актуальные проблемы кибербезопасности. Противодействие экстремизму и терроризму в информационной молодежной среде: сборник докладов I межрегиональной научно-практической конференции. – Брянск: БГТУ, 2025. – С. 205 – 208.

В эпоху цифровизации вопрос безопасности данных становится все более актуальным. Утечки данных представляют собой не только угрозу для конфиденциальности пользователей, но и могут привести к значительным финансовым потерям для организаций. В данной статье проанализируем крупнейшие утечки данных, произошедшие в 2023–2024 годах, их причины, последствия, а также уроки, которые организации могут извлечь для повышения своей безопасности.

Анализ утечек данных 2023–2024 годов

В 2024 году объем скомпрометированных персональных данных в России достиг 1,58 млрд записей, что на 30% больше, чем в 2023 году. Всего за год было зафиксировано 592 случая утечек персональных данных против 569 инцидентов годом ранее. Общее число утечек конфиденциальной информации составило 778, что немного ниже показателя 2023 года (786 случаев, снижение на 1%). Однако объем скомпрометированных данных вырос значительно сильнее. В 2024 году он составил 1,58 млрд записей, тогда как в 2023 году этот показатель был 1,2 млрд.

Наибольшее количество инцидентов зафиксировано в розничной торговле, включая онлайн и офлайн-сегменты. В 2024 году на нее пришлось 27,8% всех утечек и 35,1% случаев компрометации персональных данных. На втором месте — государственные учреждения (18% от всех утечек), однако их доля сократилась по сравнению с 2023 годом. Телекоммуникационные компании заняли третье место (9,8% против 8,7% в 2023 году).

Среди утечек можно выделить следующие случаи:

1. Бонусная программа Сбера подверглась хакерским атакам дважды за март 2023г. Суммарно утечки раскрыли почти 52 млн уникальных номеров телефона, 3,2 млн email-адресов, а также хешированные данные карт и даты рождения клиентов. В первом файле были записи с июля 2015 по июнь 2022 года, в следующем с июня 2022 по январь 2023.

2. Хакеры слили в сеть 13,9 млн записей с данными о зарегистрированных пользователях и заказах с онлайн-сервиса продажи билетов на городские события. Были раскрыты ФИО, даты рождения, города, пол, email, телефоны, хешированные пароли и другие данные об аккаунтах на kassu.ru с 2018 по 2023 годы. В разбитых по городам файлах с данными о заказах были ФИО, телефон, email, а также даты и идентификаторы заказов.

3. В феврале 2023 года произошла утечка данных о клиентах интернет-аптеки — 8,9 млн уникальных номеров и 3,4 млн email-адресов, а также информацию о датах и суммах покупок, адресах аптек и другие.

4. В сентябре 2024 года стало известно об утечке персональных данных почти 500 тысяч владельцев автомобилей KIA в России. В распространенных базах содержатся фамилии, имена, отчества, электронные адреса (172 тысячи уникальных записей), номера телефонов (448 тысяч уникальных), даты рождения, IP-адреса, хешированные пароли, а также тексты обращений клиентов и даты их отправки. Данный инцидент стал одной из крупнейших утечек данных в российском автомобильном секторе.

5. 10 июня 2024 года стало известно об утечке персональных данных, связанных с Департаментом информационных технологий (ДИТ) Москвы. В открытом доступе появился файл, содержащий 13,4 млн строк с различными персональными данными. Файл включает такие данные, как ФИО, паспортные данные, адреса регистрации и другие важные сведения.

Причины утечек данных

Утечки данных могут происходить по различным причинам. Вот несколько распространенных факторов, способствующих этому:

1. Недостаточная безопасность.

Использование устаревшего программного обеспечения или отсутствие обновлений безопасности может сделать систему уязвимой.

2. Фишинг и социальная инженерия.

Злоумышленники могут обманом заставить сотрудников раскрывать конфиденциальную информацию или вводить данные на поддельных сайтах.

3. Ошибка сотрудников.

Неправильные действия сотрудников, такие как случайное отправление файлов не тем людям или использование слабых паролей, могут привести к утечкам.

4. Вредоносное ПО.

Вирусы и другие типы вредоносного программного обеспечения могут получать доступ к конфиденциальной информации и передавать ее злоумышленникам.

5. Кража устройств.

Утеря или кража ноутбуков, смартфонов и других устройств с доступом к данным может привести к утечкам, если на них не установлена должная защита.

6. Неправильные настройки конфиденциальности.

Неправильные настройки баз данных и облачных сервисов могут привести к тому, что информация будет доступна широкой аудитории.

Последствия утечки данных

Результатами утечки данных являются финансовые проблемы (упущенная выгода, потеря денег со счетов и даже разорение), юридические последствия в виде штрафов и иных санкций, утрата репутации. Также компрометация засекреченных сведений сопряжена с ущербом бизнесу: потерей клиентов, отзывом контрактов с партнерами и подрядчиками, нарушениями бизнес-процессов и т.д.

Иногда последствия утечки данных бывают настолько глобальными, что компании приходится прекращать деятельность. Особенно часто это случается, если бизнес утратил много клиентов и не выдержал финансовых потерь.

Уроки для организаций

На основе анализа инцидентов 2023-2024 годов можно выделить ключевые рекомендации для организаций:

1. Регулярные обновления.

Обеспечение актуальности программного обеспечения и систем безопасности.

2. Обучение сотрудников.

Проведение регулярных тренингов по кибербезопасности для повышения осведомленности сотрудников.

3. Инвестиции в технологии.

Внедрение современных решений по защите данных, таких как шифрование и системы обнаружения вторжений.

4. Изучение и анализ инцидентов.

Регулярный анализ инцидентов утечек данных для улучшения системы безопасности.

Утечки данных остаются одной из главных угроз для организаций в цифровом мире. Анализируя причины и последствия крупнейших инцидентов 2023-2024 годов, мы можем выработать эффективные стратегии защиты информации, что позволит минимизировать риски и защитить как компании, так и их клиентов. Обеспечение кибербезопасности должно стать приоритетом для всех организаций в условиях постоянно меняющейся угрозы.

Список источников

1. Утечка данных // Anti-malware: официальный сайт. URL: <https://www.anti-malware.ru/news/2025-03-05-121598/45436> (дата обращения: 06.04.2025).

2. Самые громкие утечки данных // falcongaze: официальный сайт.
URL: <https://falcongaze.com/ru/pressroom/publications/incidenty-ib/samye-gromkie-utechki-dannyh-2024-goda.html> (дата обращения: 06.04.2025).

Статья поступила в редакцию 17.04.2025; принята к публикации 10.05.2025

Информация об авторе

Сычев Д.А. – студент кафедры «Системы информационной безопасности»,
направление подготовки 10.05.03 – Информационная безопасность автоматизи-
рованных систем ФГБОУ ВО «БГТУ».

Научная статья

УДК 004.056

Роль человеческого фактора в инцидентах информационной безопасности

Данила Алексеевич Сычев

Брянский государственный технический университет, Брянск, Россия

danila.sychev.13@gmail.com, <https://orcid.org/0009-0008-8816-3731>

Аннотация. В статье исследуется роль человеческого фактора в возникновении инцидентов информационной безопасности (ИБ). Предложены методы минимизации рисков, включая обучение, внедрение технологий контроля доступа и развитие корпоративной культуры безопасности. На основе проведенного исследования сформулированы рекомендации по интеграции технических и организационных мер для повышения уровня защиты.

Ключевые слова: человеческий фактор, информационная безопасность, инсайдерские угрозы, обучение сотрудников.

Для цитирования: Сычев Д.А. Роль человеческого фактора в инцидентах информационной безопасности // Актуальные проблемы кибербезопасности. Противодействие экстремизму и терроризму в информационной молодежной среде: сборник докладов I межрегиональной научно-практической конференции. – Брянск: БГТУ, 2025. – С. 209 – 211.

В современном мире безопасности информации, управление человеческим фактором становится ключевым элементом. Недостаточная осведомленность сотрудников и их возможная уязвимость перед социальной инженерией оставляют организации открытыми для атак. Это подчеркивает необходимость балансирования технических мер безопасности с обучением и образованием персонала. Осознание этой проблемы и принятие соответствующих мер позволят компаниям эффективно справиться с угрозами информационной безопасности в современном цифровом мире.

В данной статье мы глубже рассмотрим роль человеческого фактора в обеспечении информационной безопасности, выявим основные угрозы, связанные с ним, а также предложим стратегии и инновации, направленные на укрепление защиты от этих угроз. Осознание важности человеческого фактора и принятие соответствующих мер по его управлению помогут организациям сделать свои данные более защищенными в эпоху все возрастающих киберугроз [3].

Человеческий фактор как слабое звено

Человеческий фактор остается одной из ключевых причин инцидентов информационной безопасности. По данным исследования InfoWatch (2023), 75% утечек данных в России связаны с действиями сотрудников, включая ошибки, халатность и умышленные нарушения. Несмотря на развитие технологий защиты, такие угрозы, как фишинг и социальная инженерия, продолжают оставаться актуальными.

К основным проявлениям человеческого фактора в кибербезопасности можно отнести:

- **Фишинг и социальная инженерия.** Один из самых распространенных методов, используемых киберпреступниками, — фишинг. Злоумышленники рассылают электронные письма с целью обмана и получения конфиденциальной информации. Часто сотрудники, не подозревая об угрозе, открывают такие письма и переходят по вредоносным ссылкам, что позволяет хакерам получить доступ к внутренним системам компании.
- **Слабые пароли.** Несмотря на постоянные рекомендации использовать сложные пароли, многие сотрудники продолжают устанавливать простые и легко угадываемые комбинации. Это делает учетные записи уязвимыми для атак методом подбора пароля.
- **Недостаточное внимание к обновлениям ПО.** Часто пользователи игнорируют обновления программного обеспечения, которые включают важные патчи безопасности. Это создает лазейки для злоумышленников, которые могут использовать известные уязвимости.
- **Использование личных устройств для работы.** В эпоху удаленной работы все больше сотрудников используют свои личные устройства для выполнения рабочих задач. Эти устройства часто не имеют достаточного уровня защиты, что открывает дополнительные возможности для хакеров.
- **Несоблюдение политик безопасности.** Даже если в компании внедрены строгие политики безопасности, сотрудники могут их игнорировать или выполнять небрежно. Например, записывать пароли на стикерах или оставлять компьютеры без блокировки на рабочем месте.

Методы минимизации рисков

Несмотря на то, что полностью устранить человеческий фактор невозможно, есть ряд мер, которые помогут значительно снизить риски, связанные с ним. Рассмотрим основные шаги, которые компании могут предпринять для повышения уровня кибербезопасности.

1. Обучение и повышение осведомленности сотрудников

Проведение регулярных тренингов и семинаров по вопросам информационной безопасности, создание интерактивных программ по повышению осведомленности о рисках, связанных с безопасностью, могут значительно снизить вероятность ошибок со стороны сотрудников.

2. Политики и процедуры безопасности

Разработка четких политик и процедур в области безопасности, а также их регулярное обновление, поможет создать у сотрудников понимание того, какие действия допустимы, а какие — нет. Важно, чтобы эти документы были доступны и понятны каждому работнику.

3. Технические меры

Внедрение современных технологий защиты, таких как многофакторная аутентификация, системы обнаружения и предотвращения вторжений (IDS/IPS),

может служить дополнительным уровнем защиты данных и снижать последствия человеческих ошибок.

4. Культура безопасности

Создание культуры безопасности в организации, когда каждый сотрудник понимает свою роль в обеспечении безопасности, может значительно улучшить общий уровень защиты. Это включает в себя поощрение сотрудников за сообщения о возможных рисках и инцидентах.

5. Регулярные аудиты и тестирование

Проведение регулярных аудитов безопасности и тестирование на проникновение помогает выявить слабые места в защите, включая те, которые могут быть связаны с человеческим фактором.

Развитие стратегий безопасности должно быть постоянным процессом. Организации должны регулярно анализировать свои политики безопасности и внедрять обновления, учитывая новые методы атак и опыт предыдущих инцидентов. Это включает в себя как технические, так и организационные аспекты, такие как обучение сотрудников и улучшение процессов реагирования на инциденты.

Таким образом, человеческий фактор остается критическим звеном в цепи информационной безопасности. Только сочетание технических мер, регулярного обучения и формирования культуры ответственности позволит снизить риски. Даже небольшие инвестиции в осведомленность персонала способны предотвратить масштабные финансовые и репутационные потери.

Список источников

1. Человеческий фактор в информационной безопасности // Хабр: официальный сайт. URL: <https://habr.com/ru/articles/344542/> (дата обращения: 06.04.2025).
2. Действия сотрудников назвали главной причиной утечек информации // InfoWatch: официальный сайт. URL: <https://goo.su/OUfVB> (дата обращения: 06.04.2025).
3. Заозерский А. А. Роль человеческого фактора в информационной безопасности // Научный аспект. 2024. Т. 26, № 3. С. 3285-3290.

Статья поступила в редакцию 17.04.2025; принята к публикации 10.05.2025

Информация об авторе

Сычев Д.А. – студент кафедры «Системы информационной безопасности», направление подготовки 10.05.03 – Информационная безопасность автоматизированных систем ФГБОУ ВО «БГТУ».

Научная статья
УДК 004

Анализ актуальных угроз информационной безопасности

Дарья Алексеевна Терехова^{1✉}, Ольга Сергеевна Козлова^{2✉}

^{1, 2}Брянский государственный технический университет, Брянск, Россия

¹daraterehova5@gmail.com✉, <https://orcid.org/0009-0006-7482-0409>

²Bryansk-tu@yandex.ru✉

Аннотация. Статья посвящена актуальным угрозам информационной безопасности, таким как программы-шантажисты, социальная инженерия, утечки данных и атаки с использованием ИИ. Приведены примеры инцидентов, статистика и рекомендации по защите.

Ключевые слова: информационная безопасность (ИБ), информационные технологии (ИТ), злоумышленник, программное обеспечение (ПО), персональные данные (ПДн), искусственный интеллект (ИИ), информация.

Для цитирования: Терехова Д.А., Козлова О.С. Анализ актуальных угроз информационной безопасности // Актуальные проблемы кибербезопасности. Противодействие экстремизму и терроризму в информационной молодежной среде: сборник докладов I межрегиональной научно-практической конференции. – Брянск: БГТУ, 2025. – С. 212 – 214.

С каждым днем число информационных технологий растет со стремительной скоростью, как и число потребителей/пользователей, которых становится еще больше многократно, а поскольку ИТ плотно фигурируют в жизни почти каждого человека, то и число опасностей также продолжает расти.

На сегодняшний день актуальными проблемами в ИБ являются:

1. Программы-шантажисты.

Программы-шантажисты — разновидность вредоносных программ, с помощью которой злоумышленники крадут или шифруют данные, после вымогают деньги у жертв, угрожая блокировкой или удалением этих данных, их публикацией в социальных сетях или передачей третьим лицам. Распространяются через фишинговые сообщения, вредоносные сайты и пакеты эксплойта.

По данным британской компании Comparitech, которая предоставляет сравнение продуктов в сфере кибербезопасности, за первый квартал 2025 года было зафиксировано 2190 атак по всему миру с использованием данных программ, а это на 1000 атак больше, чем за тот же период 2024 года (1172). Средний размер выкупа составляет 2,14 миллиона долларов.

2. Социальная инженерия.

Социальная инженерия – это манипуляция человеком с целью получения каких-либо данных, используя разные способы и инструменты. Чаще всего: настраивание доверительных отношений. Мошенники научились имитировать звонки из банка настолько убедительно, что даже специалисты по кибербезопасности иногда попадаются на их уловки.

По результатам российской компании Positive Technologies за четвертый квартал 2024 года в качестве кибератак чаще всего использовалась социальная инженерия. Например, крупный ритейлер Hot Topic и связанные с ним бренды Vox Lunch и Torrid столкнулись с утечкой ПДн по меньшей мере 54 млн клиентов. Связано было с компьютером компании, который был заражен инфостилером. На устройстве сотрудника обнаружили учетные записи, связанные с корпоративными системами Hot Topic и Torrid в Snowflake и Looker (Google Cloud). Больше всего атакуют частные лица через шпионское ПО, которое успешно доставлялось за счет фишинговой кампании поддельных CAPTCHA и множественных атак типа SEO poisoning и malvertising (88% на частные лица, 50% - организации).

3. Утечки через третьих лиц.

Суть заключается в использовании облачных сервисов, платёжных системы, интегрируют CRM и других ИТ, предоставляемых скомпрометированными источниками/поставщиками. По сводной информации исследования компании Positive Technologies за 2023 и 2024 года скомпрометированных цепочек поставок или доверенных каналов связи (успешных) было 3% как по организации, так и по частным лицам.

4. Атаки с использованием искусственного интеллекта.

С помощью ИИ создаются фейковые аудио- и видеозвонки, имитация голоса, внешности, поведения человека; пишут части кода, создают план взлома, собирают информацию о жертве, искать уязвимости в системах и т.д. Это делает процесс быстрее и проще и влечет риск увеличения числа злоумышленников.

По данным компании Positive Technologies в феврале 2024 года группа исследователей из Иллинойского университета в Урбана-Шампейне подтвердила, что LLM-агенты могут искать и эксплуатировать уязвимости в веб-сайтах. Из 10 тестируемых языковых моделей стабильные результаты показала только GPT-4 на простых уязвимостях. В апреле 2024 года той же команде удалось улучшить результат: с помощью LLM-агентов оказалось возможным проэксплуатировать ряд уязвимостей нулевого дня. GPT-4 вновь справился с задачей, при том, что исследователи сообщали LLM описание уязвимости. А в 2023 году команда Kaspersky Digital Footprint Intelligence обнаружила в даркнете и теневого Telegram-каналах немало сообщений, рассказывающих о различных сценариях использования ИИ, в том числе о незаконных и деструктивных. Из чего следует, что в ближайшем будущем есть вероятность либо ограниченного использования ИИ, либо его полный запрет, так как уже сейчас трудно отличить правду от лжи и небезопасно выкладывать о себе даже крупицу информации.

Чтобы не оказаться жертвой следует выполнять ряд мер для обеспечения безопасности:

- не выкладывать и не передавать о себе важной информации на каких-либо площадках;
- ставить базовую защиту на устройствах – пароли;
- не переходить по ссылкам на подозрительные источники;
- перепроверять информацию через достоверные лица и источники;

- следить за своим кругом общения;
- делать резервные копии данных;
- проводить аудит и мониторинг, для выявления уязвимостей и предотвращения угроз.

Выполняя данные меры, можно минимизировать риски, количество уязвимостей и по возможности предотвращать действия злоумышленников.

Список источников

1. Актуальные проблемы информационной безопасности: сайт. – URL: <https://www.gartel.ru/articles/aktyalnost-informatsionnoy-bezopasnosti/> (дата обращения: 30.04.2025).
2. Что такое программы-шантажисты? – URL: <https://www.microsoft.com/ru-ru/security/business/security-101/what-is-ransomware> (дата обращения: 30.04.2025).
3. Comparitech: сайт. – URL: <https://www.comparitech.com/news/ransomware-roundup-q1-2025/> (дата обращения: 30.04.2025).
4. Positive Technologies: сайт. – URL: <https://www.ptsecurity.com/ru-ru/research/analytics/aktualnye-kiberugrozy-iv-kvartal-2024-goda-i-kvartal-2025-goda/#id21> (дата обращения: 30.04.2025).
5. Positive Technologies: сайт. – URL: <https://www.ptsecurity.com/ru-ru/research/analytics/iskusstvennyj-intellekt-v-kiberatakah/#id3> (дата обращения: 30.04.2025).
6. Keepersecurity: сайт. – URL: <https://www.keeper-security.com/blog/ru/2023/10/23/what-is-an-exploit-kit/> (дата обращения: 30.04.2025).
7. Securelist: сайт. – URL: <https://securelist.ru/story-of-the-year-2023-ai-impact-on-cybersecurity/108558/> (дата обращения: 30.04.2025).

Статья поступила в редакцию 25.04.2025; принята к публикации 10.05.2025

Информация об авторах

Терехова Д.А. - студент кафедры «Системы информационной безопасности», направление подготовки 10.03.01 – Информационная безопасность ФГБОУ ВО «БГТУ».

Козлова О.С. – студент кафедры «Системы информационной безопасности», направление подготовки 10.03.01 – Информационная безопасность ФГБОУ ВО «БГТУ».

Вклад авторов

Терехова Д.А. - сбор материала, обработка материала, написание статьи (70%).

Козлова О.С. - обработка материала, написание статьи (30%).

Конфликт интересов отсутствует.

Научная статья

УДК 004.056.5

OSINT как инструмент предотвращения мошенничества

Александр Максимович Урецкий¹ ✉, Оксана Михайловна Голембиовская²

^{1,2} Брянский государственный технический университет, Брянск, Россия

^{1,2} bryansk-tu@yandex.ru ✉

Аннотация. В материале рассматривается концепция разведки по открытым источникам (OSINT – Open Source Intelligence), её актуальное состояние. Описывается набор инструментов для проведения разведки по открытым источникам “OSINT Framework”, выделяются преимущества и недостатки методов OSINT. Автор уделяет внимание проблеме роста количества мошенничества в сфере финансов, бизнеса и торговли. Предлагаются меры по противодействию мошенническим действиям с помощью информации, полученной из открытых источников.

Ключевые слова: разведка, открытые источники, информация, OSINT, кибербезопасность, мошенничество, информационная безопасность.

Для цитирования: Урецкий А.М., Голембиовская О.М. OSINT как инструмент предотвращения мошенничества // Актуальные проблемы кибербезопасности. Противодействие экстремизму и терроризму в информационной молодежной среде: сборник докладов I межрегиональной научно-практической конференции. – Брянск: БГТУ, 2025. – С. 215 – 219.

В цифровую эру количество угроз компьютерной безопасности растет в геометрической прогрессии, о чем свидетельствует постоянно растущий набор инструментов и тактик злоумышленников. Это могут быть как простые схемы социальной инженерии, нацеленные на невнимательных и доверчивых людей, так и целевые атаки на критические инфраструктуры.

В этих условиях традиционные подходы обеспечения информационной безопасности становятся все более недостаточными. Для противодействия постоянно растущему списку угроз, специалистам по информационной безопасности необходимо строить многопрофильную защиту, выходящую за рамки классических средств.

В сфере кибербезопасности с момента появления сети Интернет все больше набирает популярность аналитическая интернет-разведка. Разведка по открытым источникам (англ. Open Source Intelligence, OSINT) – это информационная работа, направленная на поиск и обработку открытой или частично открытой информации.

Основным назначением OSINT является бизнес-разведка, аналитика, проверка состояния информационной безопасности организации. Кроме того, инструментарий разведки по открытым источникам активно используется для решения задач национальной безопасности. Разведывательные агентства используют OSINT для отслеживания людей, событий, вооружений других стран [1]. Сам феномен OSINT появился раньше Интернета, долгое время правительства использовали газеты, радио и обычные рассказы очевидцев для отслеживания

военных, политических и экономических действий потенциального противника. Однако, в современных реалиях Интернет стал практически единственным местом подобных разведывательных действий.

Согласно актуальной статистике [2], на момент 2024 года пользователями сети Интернет являются 5.5 млрд. человек, что составляет 67% населения Земли. Объем информации, генерируемой в сети Интернет, огромен. Все эти данные представляют ценность для правительств, разведывательных служб и коммерческих организаций, которые стремятся выделиться среди конкурентов. Для организации такого значительного объема данных используется OSINT Framework.

OSINT Framework представляет собой набор инструментов, которые используются для сбора разведанных из открытых источников. В этом простом веб-интерфейсе инструменты OSINT отсортированы по категориям, классификация производится на основе тем и целей поиска (Рисунок 1).

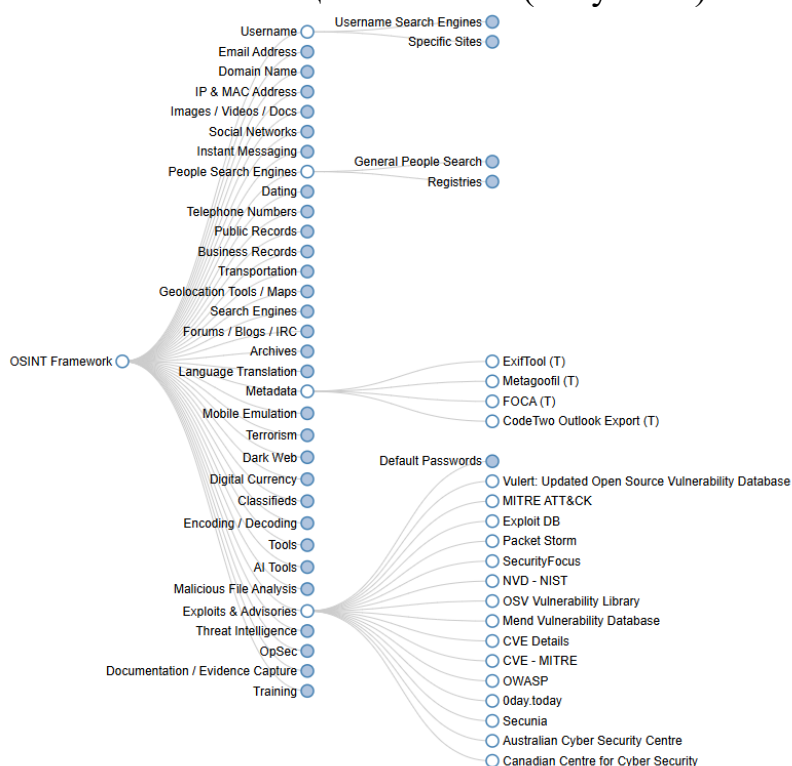


Рис. 1. Классификатор инструментов OSINT Framework

Использование OSINT обладает как преимуществами, так и недостатками. В качестве сильной стороны разведки по открытым источникам в первую очередь стоит выделить финансовый аспект, а именно – практически полное отсутствие затрат на проведение мероприятий, т.к. добываемая из открытых источников информация по своему определению является бесплатной. Кроме того, сам факт доступа к такой информации не является противозаконным. Другим преимуществом является актуальность информации и ее обновление в режиме реального времени. Также OSINT может быть эффективно использован в качестве инструмента “самопроверки” службы безопасности – полученные из открытых

источников данные позволяют обнаружить потенциальные или уже произошедшие утечки информации, которая является ценной и конфиденциальной для обладателя.

Тем не менее, использование открытых источников для получения разведанных сопряжено с определенными трудностями. Основной проблемой OSINT является объем получаемой в Сети информации, анализ и фильтрация которой без средств автоматизации зачастую представляют крайне трудоемкое мероприятие. Помимо этого, полученные данные необходимо проверять на достоверность, т.к. в сети Интернет часто распространяется заведомо ложная информация. Этическая сторона использования OSINT все еще является предметом обсуждения [3, 4], а сам инструментарий активно используется в том числе и для незаконной деятельности.

Одним из направлений актуального использования OSINT является противодействие мошенничеству. Согласно статистике Генпрокуратуры РФ [5], в 2023 году рост преступлений с использованием Интернета и мобильной связи вырос на 39,3%.

OSINT является отличным инструментом для организаций, позволяющим усилить противодействие мошенничеству.

Наиболее распространенным является мошенничество в финансовой сфере. Это постоянно растущая угроза, как на уровне мелкого мошенничества с банковскими картами, так и на уровне целых финансовых пирамид и мировых фондовых рынков. Рост количества преступлений показывает, что стандартные способы выявления финансовых мошенников не всегда эффективны.

Мошенники могут красть деньги у ничего не подозревающих жертв по всему миру, используя веб-сайты и фишинг. Стоит отметить, что злоумышленники часто используют информацию, доступную в социальных сетях. OSINT можно использовать и в обратную сторону - для получения разведанных о поведении, репутации и онлайн-активности подозрительных людей или организаций, а затем анализировать их на основе определенных индикаторов мошеннического поведения. Например, согласно иностранным исследованиям, 42% мошенников живут не по средствам [6]. OSINT позволяет выявлять несоответствие формального благосостояния реальным расходам.

Для обеспечения эффективной защиты от мошенников, финансовые учреждения должны продолжать корректировать свои методы оценки рисков, включая в них анализ информации из открытых источников.

Другим распространенным вариантом мошенничества является использование инсайдерской информации. Это могут быть коррупционные схемы, утечки данных, саботаж или мошенничество с бухгалтерской отчетностью. На уровне организаций это, как правило, подкуп или получение взяток за заключение договоров, а также замаскированное хищение средств. Случаи инсайдерского мошенничества часто раскрываются путем поиска связей между сотрудником и потенциальным преступником. Проверить наличие таких сотрудников и их связи с третьей стороной можно при помощи открытых источников информации и инструментария OSINT.

Борьба с подобным мошенничеством начинается с определения категорий информации, которая может или не может быть использована в мошеннических целях, а также людей, которые имеют к ней доступ. Стоит учитывать, что не все сотрудники осознанно идут на преступление, многие подвергаются воздействию психологического манипулирования со стороны злоумышленника. Это требует принятия мер по повышению осведомленности, проведения обучающих мероприятий. Со стороны организации потребуется усиленное разграничение доступа и использования информации. Используя инструментарий OSINT, можно проводить проверку мотивированности на совершение мошенничества. Например, биографических данных потенциальных сотрудников, подрядчиков и субподрядчиков для поиска скрытого уголовного прошлого, финансовых проблем, а также степень удовлетворенности работой в организации.

Подобная осмотрительность является эффективной превентивной мерой, позволяющей исключить потенциальные угрозы, связанные с инсайдерской информацией, даже на стадии принятия сотрудника на работу или заключения контракта с партнером.

С ростом внедрения Интернета в сферу продаж, появился целый рынок, переполненный поддельными и краденными товарами. Согласно оценкам Международной торговой палаты (МТП), контрафактная продукция и связанные с ней мошеннические операции в 2015 году привели к убыткам в размере 125 миллиардов долларов только в качестве неуплаченных налогов, а также к потере 2.5 миллионов рабочих мест. МТП также сообщает, что доля контрафактных товаров в этот момент уже достигала 1.7 триллиона долларов, что составляет 2% от общемирового экономического производства.

Нарушители, торгующие контрафактной продукцией в Интернете, часто используют ложную личную информацию или вовсе анонимны. OSINT может быть использован в качестве инструмента де-анонимизации таких лиц. В дополнение к полученной из Сети информации можно произвести тестовую покупку для получения электронной почты, платежных счетов и юридического адреса.

Вся эта информация проверяется при помощи OSINT Framework и запросов в определенных базах данных, зачастую позволяя идентифицировать субъекта, являющегося обладателем подставной учетной записи или организации. Регистрация компаний и их данные в значительной степени или полностью публичны, что позволяет производить поиск на основе имен, адресов, идентификаторов и т.п. Если расследование идентифицирует компанию как основное лицо, осуществляющее деятельность, нарушающую права, OSINT также может помочь в выявлении учредителей, определении того, является ли компания платежеспособной, а также выявить дополнительные зарегистрированные юридические лица и компании, контролируемые теми же людьми.

Таким образом, OSINT является своеобразным “швейцарским ножом”, полезным как для бизнес-аналитики и правоохранительных органов, так и для специалистов по информационной безопасности. Информация, полученная из открытых источников, представляет собой отличный фундамент для построения

альтернативного подхода к решению проблемы мошенничества в современном мире.

Список источников

1. Минченко В. Разведка на основе открытых источников (OSINT) и ее методология в современных реалиях / В. Минченко, Г. Ф. Вильдяйкин // Молодежь и наука: актуальные проблемы фундаментальных и прикладных исследований : Материалы III Всероссийской национальной научной конференции студентов, аспирантов и молодых ученых. В 3 ч. Комсомольск-на-Амуре, 06–10 апреля 2020 года / Редколлегия: Э.А. Дмитриев (отв. ред.) [и др.]. Часть 2. – Комсомольск-на-Амуре: Комсомольский-на-Амуре государственный университет, 2020. – С. 319-322.

2. Naveen, Kumar How Many Use The Internet in 2024 (New Data) / Kumar Naveen. — Текст : электронный // demandsage : [сайт]. URL: <https://www.demand-sage.com/internet-user-statistics/> (дата обращения: 24.10.2024).

3. Хайперосов Д. Этические дилеммы в OSINT: где проходит допустимая грань? // SecurityLab : [сайт]. URL: <https://www.securitylab.ru/blog/personal/xiaomite-journal/353686.php?ysclid=m2n8xdmrnx587833634> (дата обращения: 24.10.2024).

4. Климанова Е. А. Этические аспекты использования открытых данных, полученных с помощью технологии OSINT / Е. А. Климанова, О. В. Ярыгин // Аналитические технологии в социальной сфере: теория и практика : сборник студенческих работ. Москва, 18 мая 2023 г. – Москва: Изд-во НИЦ «Национальная безопасность», 2023. – С. 45-50.

5. В России число совершенных через мобильную связь и интернет преступлений выросло на 39% // ТАСС : [сайт]. URL: <https://tass.ru/obschestvo/18417795?ysclid=m2n5yrksn9232966540> (дата обращения: 24.10.2024).

6. Using Open Source Intelligence To Battle Fin Crime . URL: <https://www.netas.com/using-open-source-intelligence-to-battle-fin-crime/> (дата обращения: 24.10.2024).

Статья поступила в редакцию 17.04.2025; принята к публикации 10.05.2025

Информация об авторах

Урецкий А.М. - аспирант кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Голембиовская О.М. - к.т.н., доцент кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Вклад авторов

Урецкий А.М. - идея, сбор и обработка материала, написание статьи (50%).

Голембиовская О.М. - сбор материала, частичное написание статьи, научное редактирование текста (50%).

Конфликт интересов отсутствует.

Научная статья

УДК 004.056

Анализ актуальных угроз ситуационного центра регионального уровня

Арина Викторовна Фурсова^{1✉}, Алексей Вячеславович Яковлев²

^{1, 2}Тамбовский государственный технический университет, Тамбов, Россия

¹fursova_arina@inbox.ru ✉, <https://orcid.org/0009-0008-3540-3797>

²yava73@bk.ru, <https://orcid.org/0000-0003-2764-6461>

Аннотация. Для оперативного реагирования региональных органов на кризисные ситуации создаются ситуационные центры, представляющие собой системы принятия решений на основе сбора, обработки и агрегирования. Однако, несмотря на современное оснащение, ситуационные центры остаются уязвимы к кибератакам со стороны нарушителя со средним уровнем возможностей. Такие атаки могут привести к нарушению функционирования ситуационного центра, утечке информации и другим негативным последствиям. Для повышения устойчивости системы к кибератакам предлагается использовать комбинацию децентрализованной системы защиты и мультиагентного подхода, что позволит синхронизировать управление защитными механизмами и снизить риски.

Ключевые слова: ситуационный центр, угрозы информационной безопасности, уровень нарушителя.

Для цитирования: Фурсова А.В., Яковлев А.В. Анализ актуальных угроз ситуационного центра регионального уровня // Актуальные проблемы кибербезопасности. Противодействие экстремизму и терроризму в информационной молодежной среде: сборник докладов I межрегиональной научно-практической конференции. – Брянск: БГТУ, 2025. – С. 220 – 224.

В условиях угроз национальной безопасности необходимо принимать качественные и стратегические решения для урегулирования региональных кризисных ситуаций. Одним из инструментов, позволяющим оперативно реагировать на сложившуюся ситуацию, является ситуационный центр (СЦ). Ситуационный центр представляет собой инженерно-технический комплекс, включающий в себя системы для сбора, обработки и демонстрации информации об объектах мониторинга [1]. Типовая структура представлена на рис. 1.

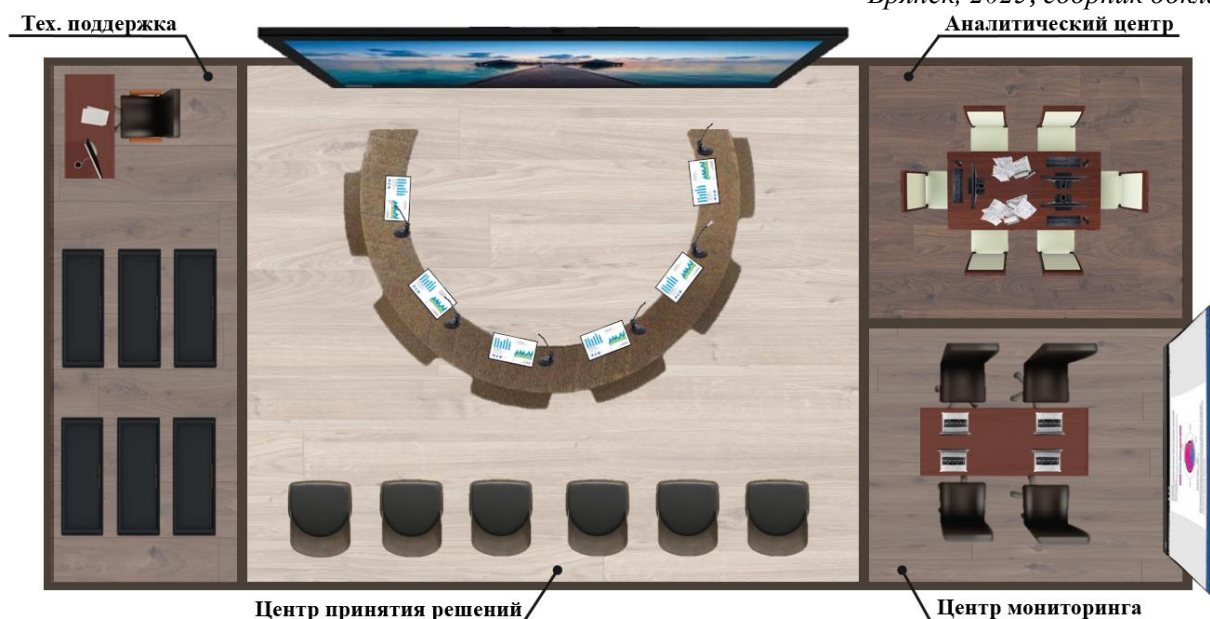


Рис. 1. Типовая структура ситуационного центра

Структура ситуационного центра основывается на принципе последовательной обработки информации, этапы которого отражены в основных задачах рассматриваемого объекта [2]:

- получение информации из различных источников;
- анализ информации в режиме реального времени для разбиения инцидентов по группам реагирования на чрезвычайные ситуации;
- передача сведений об инцидентах ответственным лицам;
- поддержка принятия решений (моделирование сценариев возникновения чрезвычайных ситуаций, анализ последствий, демонстрация возможных действий ответственным лицам и организация действий по реагированию);
- ретроспективный анализ инцидентов и соответствующие принятые меры.

Зона мониторинга предназначена для первичной обработки и классификации инцидентов согласно заданным критериям в режиме реального времени. Оснащенность данного помещения представлена всего лишь системами отображения информации, такими как видеостены и ЖК-дисплеи, со специализированным программным обеспечением, поскольку системные блоки, сервера баз данных, обработки данных и архивы вынесены в отдельное помещение.

Обработка данных, полученных от центра мониторинга, выявление закономерностей и подготовка отчетов – основные задачи аналитического центра. Их выполнение возможно благодаря оснащенностью аналитиков рабочими станциями и серверами со специальным программным обеспечением для анализа данных.

Центр принятия решений – ключевой элемент ситуационного центра, где на основании данных, полученных из зоны мониторинга и аналитического центра, разрабатываются варианты реагирования на произошедший инцидент. Само

помещение оснащено системой видеоконференцсвязи для оперативного взаимодействия с другими центрами или структурными подразделениями, а также несколькими дисплеями для отображения имеющихся сведений. Слаженная работа руководителей и специалистов на основании оценки текущей обстановки позволяет спрогнозировать и минимизировать возможные последствия инцидентов и обеспечить эффективную работу служб.

Зона технической поддержки необходима для обеспечения работоспособности технического и программного обеспечения, функционирующего в ситуационном центре. Бесперебойная работа системы возможна за счет резервирования всех компонентов системы, их легкой замены в случае критической ситуации и перехода с интегрированного управления на ручное. Функционирующие технические системы (например, видеостена и камеры видеонаблюдения) дублируются на мониторы сотрудников. Это дает возможность отслеживать и контролировать, происходящие в ситуационном центре, процессы.

Хотя ситуационные центры и оснащены современными техническими системами для мониторинга, анализа данных и защиты информации, они все равно остаются уязвимыми к действиям нарушителей. Ведь при успешной атаке на ситуационные центры возможными негативными последствиями могут быть: нарушение штатного функционирования, утечка информации ограниченного доступа, неспособность выполнения договорных обязательств, невозможность решения поставленных задач и т. д.

Согласно классификации ФСТЭК [3], выделяют следующие уровни возможностей нарушителей:

- нарушитель, обладающий базовыми возможностями;
- нарушитель, обладающий базовыми повышенными возможностями;
- нарушитель, обладающий средними возможностями;
- нарушитель, обладающий высокими возможностями.

Нарушитель, обладающий средними возможностями, представляет значительную угрозу информационной безопасности ситуационного центра. Данный вид нарушителей обладает достаточными знаниями, инструментами и ресурсами для осуществления атак и эксплуатации уязвимостей на следующие объекты воздействия ситуационного центра [3]: автоматизированные рабочие места, сервера, периферийное оборудование, активное сетевое оборудование, телефония, средства защиты информации, физические линии связи. Каждый объект представляет собой совокупность взаимосвязанных компонентов, на которые направлено деструктивное воздействие нарушителя с целью реализации угрозы информационной безопасности. Например [3], сервера включает в себя такие компоненты, как встроенная микропрограмма, операционная система, UEFI/BIOS, программная оболочка, драйвер, загрузчик операционной системы, системные и сетевые службы, сетевой интерфейс. В Таблице 1 рассмотрены возможные действия нарушителя со средним потенциалом по отношению к компонентам сервера, а также последствия воздействий.

Таблица 1

Перечень актуальных угроз безопасности информации ситуационного центра

Действие нарушителя	Компонент сервера	Код угрозы согласно ФСТЭК
Внедрение программных и аппаратных закладок	Встроенная микропрограмма, ОС, UEFI/BIOS	УБИ.1.2.5 УБИ.2.2.5 УБИ.3.2.5 УБИ.4.2.5 УБИ.6.2.5 УБИ.8.2.5
Модификация или подмена прошивки	Встроенная микропрограмма	УБИ.2.2.23 УБИ.3.2.23 УБИ.4.2.23 УБИ.6.2.23 УБИ.8.2.23
Нарушение изоляции процессов	ОС	УБИ.1.2.16 УБИ.2.2.16 УБИ.3.2.16 УБИ.4.2.16 УБИ.8.2.16
Применения скрытых каналов по времени	Системные и сетевые службы, сетевой интерфейс	УБИ.1.2.11

В общей сложности, действия нарушителя, обладающего средним потенциалом, могут привести к более чем 100 различным угрозам информационной безопасности ситуационного центра в соответствии с методикой ФСТЭК.

В таких условиях централизованная система защиты ситуационного центра уязвима не только из-за единой точки отказа, но и из-за несинхронизированных элементов системы защиты. В это время децентрализованная система защиты имеет более устойчивую архитектуру, поскольку функции защиты распределены между множеством узлов. Применяв мультиагентный подход к средствам защиты информации ситуационного центра и связав их, получаем синхронизированное управление средствами защиты, взаимный обмен данными и сигналами для достижения глобальной цели защиты ситуационного центра.

Список источников

1. ГОСТ Р 56875-2016. Информационные технологии. Системы безопасности комплексные и интегрированные. Типовые требования к архитектуре и технологиям интеллектуальных систем мониторинга для обеспечения безопасности предприятия и территорий : национальный стандарт Российской Федерации : дата введения 2017-010-01 / Федеральное агентство по техническому регулированию и метрологии. – Изд. официальное. – Москва : Стандартинформ, 2019. – 46 с.

2. Ситуационный центр как инструмент управления. - URL: <https://www.jetinfo.ru/situatsionnyj-tsentr-kak-instrument-upravleniya/> (дата обращения: 20.03.2025).

3. Методика оценки угроз безопасности информации : методический документ: утвержден ФСТЭК России 5 февраля 2021 года // Официальный сайт Федеральной службы по техническому и экспортному контролю. - URL: <https://fstec.ru/tekhnicheskaya-zashchitainformatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/2170-metodicheskij-dokumentutverzhdenn-fstek-rossii-5-fevralya-2021> (дата обращения: 20.03.2025).

Статья поступила в редакцию 12.04.2025; принята к публикации 10.05.2025

Информация об авторах

Фурсова А.В. - аспирант кафедры «Информационные системы и защита информации», направление подготовки 2.3.6 – Методы и системы защиты информации, информационная безопасность ФГБОУ ВО «ТГТУ».

Яковлев А.В. - к.т.н., доцент кафедры «Информационные системы и защита информации» ФГБОУ ВО «ТГТУ».

Вклад авторов

Фурсова А.В. - идея, сбор и обработка материала, написание статьи (75%).

Яковлев А.В. - научное редактирование текста (25%).

Конфликт интересов отсутствует.

СЕКЦИЯ 4. АУДИТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, УПРАВЛЕНИЕ РИСКАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Научная статья

УДК 004.056

Основные особенности оценки уровня остаточного риска информационной безопасности

Павел Вадимович Банный ^{1✉}, Никита Витальевич Петроченко ²,

Кирилл Андреевич Седаков ³

^{1,2,3}Брянский государственный технический университет, Брянск, Россия

¹kotenauka@gmail.com ✉, <https://orcid.org/0009-0005-3540-3015>

²nikitapetrochenko32@yandex.ru, <https://orcid.org/0009-0003-0213-2648>

³sekira98@mail.ru, <https://orcid.org/0009-0002-9284-4624>

Аннотация. В статье исследуются ключевые аспекты оценки остаточного риска информационной безопасности. Рассмотрены различия между первичным и остаточным риском, влияние динамичных угроз (включая AI и deepfake), неопределённости данных и человеческого фактора. Проанализированы технологические решения (SIEM-системы) и регуляторные требования. Особое внимание уделено необходимости междисциплинарного подхода и адаптивных методов оценки. Результаты подчёркивают важность комплексной стратегии для минимизации рисков при сохранении гибкости бизнес-процессов.

Ключевые слова: остаточный риск, информационная безопасность, управление рисками, киберугрозы, SIEM-системы, регуляторные требования.

Для цитирования: Банный П.В., Петроченко Н.В., Седаков К.А. Основные особенности оценки уровня остаточного риска информационной безопасности // Актуальные проблемы кибербезопасности. Противодействие экстремизму и терроризму в информационной молодежной среде: сборник докладов I межрегиональной научно-практической конференции. – Брянск: БГТУ, 2025. – С. 225 – 230.

Остаточный риск - это уровень угрозы, сохраняющийся после внедрения контрмер, направленных на минимизацию исходного (первичного) риска. Согласно ГОСТ Р ИСО/МЭК 27005-2010 [1], процесс управления рисками включает этапы идентификации, анализа, обработки и мониторинга, где остаточный риск становится ключевым показателем эффективности принятых мер. Первичный риск утечки персональных данных может быть снижен за счёт внедрения шифрования и систем контроля доступа. Однако остаточный риск сохраняется из-за возможности эксплуатации нулевых уязвимостей или ошибок сотрудников.

Для полного понимания темы следует разобрать разницу между первичным и остаточным риском. Первичный риск отражает угрозы до применения защитных мер, тогда как остаточный - после. Например, для банковской системы первичный риск DDoS-атаки оценивается как высокий (вероятность 80%, ущерб

- до 10 млн руб.). После внедрения системы фильтрации трафика остаточный риск снижается до среднего (вероятность 20%, ущерб — до 2 млн руб.).

Понимание остаточного риска и его взаимосвязи с классификацией угроз и уязвимостей является ключевым аспектом эффективного управления информационной безопасностью. Рассмотрим, как различные типы угроз, как внешние, так и внутренние, а также технические и организационные уязвимости, могут влиять на уровень остаточного риска и, соответственно, на общую безопасность информационных систем.

Внешние угрозы исходят от злоумышленников, не имеющих прямого доступа к информационным системам организации. В 2023 году 67% российских компаний подверглись целевым атакам [2], что подчеркивает их высокую актуальность.

Современные киберугрозы всё чаще принимают форму многоэтапных операций, где злоумышленники действуют скрытно и методично. Многоэтапные кибератаки ориентированы на получение долгосрочного доступа к инфраструктуре для хищения данных или саботажа. Такие операции отличаются высокой адаптивностью и могут оставаться необнаруженными месяцами, что усиливает их разрушительный потенциал. Например, в 2022 году группа APT29 провела серию атак на российские научные центры, целенаправленно похищая исследования в области биоинженерии [3]. Длительная скрытность таких кампаний, часто сопровождающаяся имитацией легитимной активности, делает их особенно опасными для критически важных секторов.

Массовая рассылка поддельных сообщений остаётся одним из самых распространённых методов кражи учётных данных. Согласно исследованию Group-IB, в 2023 году на фишинг пришлось 45% всех киберинцидентов в России [4]. Злоумышленники имитируют письма от банков, государственных служб или коллег, вынуждая жертв раскрывать конфиденциальную информацию.

Шифрование данных с последующим требованием выкупа продолжает наносить значительный ущерб. Например, атака группировки LockBit на «Роснефть» в 2021 году парализовала часть IT-систем компании на 72 часа, что привело к многомиллионным потерям [5].

Непреднамеренные действия персонала — частая причина утечек. 60% инцидентов в малом бизнесе РФ в 2022 году были связаны с некорректной настройкой прав доступа к облачным хранилищам AWS [6].

Эксплуатация неподдерживаемого ПО, например Windows 7, остаётся критической проблемой. По данным ФСТЭК, в 2023 году зафиксировано 120 успешных атак на организации, использующие такие системы [7].

Некорректные настройки инфраструктуры создают лазейки для злоумышленников. Открытые RDP и SSH порты становятся причиной 25% успешных атак на государственные учреждения [8]. Не менее опасны ошибки в правилах межсетевых экранов — например, разрешение всех соединений (правило ANY-ANY в Cisco ASA).

Теперь, когда мы рассмотрели, что такое остаточный и первичный риск, а также уделили внимание классификации угроз и уязвимостей, подробно рассмотрим особенности оценки остаточного риска.

Основными особенностями оценки остаточного риска являются: динамичность угроз, неопределённость данных, человеческий фактор, технологические аспекты, регуляторные требования, кросс-функциональный подход. Разберем каждую особенность отдельно.

Современные киберугрозы стремительно развиваются благодаря развитию технологий искусственного интеллекта и deepfake, что принципиально меняет подходы к оценке остаточных рисков. Генеративные ИИ-алгоритмы позволяют создавать персонализированные фишинговые атаки с высокой эффективностью, в то время как технологии синтетических медиа (deepfake) используются для сложных схем мошенничества, включая имитацию голосов руководителей при авторизации транзакций. Эти изменения требуют перехода от традиционных статических моделей оценки рисков к динамическим системам, способным анализировать не только известные угрозы, но и прогнозировать новые векторы атак с помощью предиктивной аналитики и непрерывного мониторинга киберпространства [9].

Особую сложность представляет адаптивный характер современных угроз - AI-аугментированные атаки способны самообучаться и оптимизироваться в процессе эксплуатации уязвимостей, что делает традиционные методы защиты менее эффективными. В этих условиях ключевое значение приобретает интеграция в системы управления рисками технологий машинного обучения, позволяющих выявлять формирующиеся угрозы по слабым сигналам и анализировать поведенческие паттерны. При этом необходимо учитывать, что новые типы атак часто требуют принципиально иных подходов к оценке рисков, учитывающих их способность к быстрой эволюции и адаптации под защитные механизмы.

Для эффективного управления остаточными рисками в условиях динамично меняющегося ландшафта угроз организациям необходимо развивать системы прогнозной аналитики, внедрять специализированные сценарии оценки AI-аугментированных угроз и обеспечивать непрерывный мониторинг новых векторов атак. Это требует пересмотра традиционных методологий риск-менеджмента в сторону большей гибкости и адаптивности, а также тесной интеграции технологий искусственного интеллекта в процессы оценки и мониторинга киберрисков.

Одной из ключевых проблем при оценке остаточных рисков является неопределённость данных, обусловленная их неполнотой, устареванием или ограниченной доступностью, что существенно затрудняет прогнозирование потенциальных угроз и их последствий. Организации, полагающиеся на устаревшие данные о прошлых атаках, рискуют недооценить вероятность и масштаб новых, более изощрённых угроз, таких как AI-аугментированные атаки или эксплуатация ранее неизвестных уязвимостей. Например, традиционные модели оценки, основанные на статистике прошлых лет, могут не учитывать стремительное развитие методов социальной инженерии или появление принципиально новых векторов

атак, связанных с развитием квантовых вычислений. В условиях такой неопределённости критически важными становятся постоянная актуализация данных, интеграция информации из разнообразных источников (включая Threat Intelligence-платформы и отраслевые базы уязвимостей), а также применение адаптивных методов анализа, способных работать с неполными или изменяющимися входными данными. Это позволяет минимизировать погрешности в оценке остаточных рисков и повысить эффективность принимаемых защитных мер [10].

Человеческий фактор остается одним из ключевых элементов при оценке остаточных рисков в сфере информационной безопасности, где субъективность восприятия угроз экспертами часто приводит к существенным ошибкам в определении уровня риска. Особую опасность представляют когнитивные искажения, такие как эффект "привыкания" к повторяющимся угрозам, когда регулярность инцидентов снижает их воспринимаемую значимость, или "избыточная уверенность" в эффективности существующих защитных механизмов, что особенно критично при оценке новых типов угроз вроде атак с использованием ИИ или сложных эксплуатационных цепочек. Многочисленные исследования подтверждают, что до 60% ошибок в оценке рисков связаны именно с психологическими факторами, проявляющимися в недооценке незнакомых угроз или переоценке защищенности систем, длительное время не подвергавшихся атакам. Для противодействия этим тенденциям современная практика информационной безопасности предполагает внедрение структурированных методик оценки, включающих стандартизированные шкалы и метрики, методы коллективной экспертной оценки, а также постоянное обучение специалистов, дополненное автоматизацией процессов сбора и анализа данных о рисках, что в комплексе позволяет минимизировать субъективное влияние и сформировать более объективное восприятие угроз безопасности.

Современные технологические решения, в частности системы управления событиями и инцидентами безопасности (SIEM), существенно трансформируют подходы к оценке остаточных рисков, обеспечивая комплексный сбор и анализ данных из разнородных источников, что значительно повышает точность выявления угроз. Однако внедрение таких систем сопряжено с существенными организационными и экономическими вызовами, особенно для малых и средних предприятий, которые сталкиваются не только с высокими затратами на развертывание и сопровождение SIEM-решений, но и с дефицитом квалифицированных специалистов, способных эффективно использовать эти технологии. При этом даже полнофункциональные SIEM-системы не обеспечивают абсолютного устранения остаточных рисков, поскольку их эффективность во многом зависит от качества настройки правил корреляции, актуальности используемых индикаторов компрометации (IoC) и способности адаптироваться к новым тактикам, техникам и процедурам (TTPs) злоумышленников, что требует постоянного обновления и тонкой настройки системы в условиях быстро меняющегося ландшафта угроз.

Современные организации сталкиваются со сложной задачей интеграции многочисленных законодательных и нормативных требований в процесс оценки

остаточных рисков, где соблюдение стандартов информационной безопасности, таких как ISO/IEC 27001[11], или специальных требований к защите персональных данных (например, GDPR или ФЗ-152) требует не только значительных ресурсов, но и глубокого понимания как технических, так и юридических аспектов. Несоблюдение этих требований может привести не только к финансовым штрафам и репутационным потерям, но и к существенному увеличению остаточного риска из-за формального подхода к реализации мер защиты, что делает критически важным системное включение регуляторных аспектов в методологию оценки рисков. При этом эффективное решение данной проблемы невозможно без реализации кросс-функционального подхода, предполагающего тесное взаимодействие между ИТ-подразделениями, юридическими службами, risk-менеджментом и бизнес-единицами, поскольку именно такое междисциплинарное сотрудничество позволяет учесть как технические уязвимости и угрозы, так и правовые последствия, операционные ограничения и бизнес-контекст, создавая тем самым целостную картину рисков и обеспечивая разработку сбалансированных мер защиты, соответствующих как регуляторным требованиям, так и практическим возможностям их реализации в конкретной организационной среде.

Оценка остаточного риска информационной безопасности требует комплексного подхода, учитывающего технологические, организационные и человеческие факторы. Ключевыми условиями эффективного управления рисками являются: адаптация к динамичным угрозам, преодоление когнитивных искажений при оценке, соблюдение регуляторных требований и межфункциональное взаимодействие. Реализация этих принципов позволяет организациям поддерживать оптимальный уровень безопасности, минимизируя остаточные риски при сохранении бизнес-гибкости.

Список источников

1. ГОСТ Р ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности: национальный стандарт Российской Федерации / утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 30 ноября 2010 г. № 632-ст. 2011. URL: <https://unicons.biz/upload/medialibrary/338/3389c91d011a3fa83b4600bcac6c188f.pdf>.
2. Global Scam-paign: Number of scam resources per brand soars by 162% in 2022 – Digital Risk Trends. Group-IB. 2023. URL: <https://www.group-ib.com/media-center/press-releases/digital-risk-trends-2023/>.
3. They See Me Roaming: Following APT29 by Taking a Deeper Look at Windows Credential Roaming. Google Cloud Blog. 2022. URL: <https://cloud.google.com/blog/topics/threat-intelligence/apt29-windows-credential-roaming/>.
4. Актуальные киберугрозы: IV квартал 2023 года // Positive Technologies. 2024. URL: <https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2023-q4/>.

5. Масштабная кибератака парализовала работу «Лукойла» и «Роснефти» // Оху.Аз. 2025. URL: <https://oxu.az/ru/ekonomika/masshtabnaya-kibertaka-paralizovala-rabotu-lukoila-i-rosnefti>.
6. Исследование уязвимостей в облачных хранилищах // Positive Technologies. 2022. URL: <https://www.ptsecurity.com/ru-ru/about/news/positive-technologies-pomogla-ustranit-uyazvimost-v-setevyh-hranilishchah-asustor/>. 2 с.
7. Методические рекомендации по оценке рисков / ФСТЭК. 2023. URL: <https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-5-fevralya-2021-g>.
8. Защита RDP-подключения к VDS/VPS в эпоху «заслуженного» киберпанка // Habr. 2020. URL: <https://habr.com/ru/companies/ruvds/articles/516814/>.
9. Gartner Unveils Top Eight Cybersecurity Predictions for 2023-2024. Gartner. 2023. URL: <https://www.gartner.com/en/newsroom/press-releases/2023-03-28-gartner-unveils-top-8-cybersecurity-predictions-for-2023-2024>. 3 с.
10. Выбор эффективных ИБ-решений в условиях неопределенности // Cisoclub. 2024. URL: <https://cisoclub.ru/vybor-jeffektivnyh-ib-reshenij-v-uslovijah-neopredelennosti/>.
11. ISO/IEC 27001:2022 Information technology - Security techniques - Information security management systems - Requirements. ISO. 2022. URL: <https://www.iso.org/standard/27001>.

Статья поступила в редакцию 16.04.2025; принята к публикации 10.05.2025

Информация об авторах

Банний П.В. - студент кафедры «Системы информационной безопасности», направление подготовки 10.03.01 - Информационная безопасность ФГБОУ ВО «БГТУ».

Петроченко Н.В. - студент кафедры «Системы информационной безопасности», направление подготовки 10.03.01 - Информационная безопасность ФГБОУ ВО «БГТУ».

Седаков К.А. - ассистент кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Вклад авторов

Банний П.В. - идея, сбор материала, обработка материала, частичное написание статьи (25%).

Петроченко Н.В. - идея, сбор материала, обработка материала, частичное написание статьи (25%).

Седаков К.А. - написание статьи, научное редактирование текста (50%).

Конфликт интересов отсутствует.

Научная статья

УДК 004.056

Алгоритм определения актуальных угроз согласно методическим рекомендациям ФСТЭК России

Вячеслав Владимирович Иваничкин^{1✉}, **Кирилл Евгеньевич Шинаков**^{2✉},
Владислав Ильич Волков^{3✉}

^{1,2,3}Брянский государственный технический университет, Брянск, Россия

¹ ivani4kin.slavik@yandex.ru ✉

² bryansk-tu@yandex.ru ✉

³ iamvolkov27@gmail.com ✉

Аннотация. В данной статье рассматривается порядок оценки актуальности угроз безопасности информации и построения документа модели угроз, который регулируется Методическим документом «Методика оценки угроз безопасности информации».

Ключевые слова: информационная безопасность, модель угроз, методические рекомендации ФТЭК.

Для цитирования: Иваничкин В.В., Шинаков К.Е., Волков В.И. Алгоритм определения актуальных угроз согласно методическим рекомендациям ФСТЭК России // Актуальные проблемы кибербезопасности. Противодействие экстремизму и терроризму в информационной молодежной среде: сборник докладов I межрегиональной научно-практической конференции. – Брянск: БГТУ, 2025. – С. 231 – 235.

В условиях постоянного роста числа киберугроз и усложнения методов атак, разработка эффективной модели угроз безопасности информации систем и сетей становится неотъемлемой частью стратегии по обеспечению информационной безопасности.

Знание о том, какие именно угрозы могут возникнуть, позволяет организациям более эффективно распределять ресурсы и разрабатывать соответствующие меры защиты. В том числе помогает определить приоритетные направления для инвестиций в программные решения, обучение сотрудников или укрепление физической безопасности.

Порядок оценки актуальности угроз безопасности информации и построения документа модели угроз регламентирует Методический документ «Методика оценки угроз безопасности информации» [1] и включает в себя следующие этапы:

1. Определение негативных последствий от реализации (возникновения) угроз безопасности информации.
2. Определение возможных объектов воздействия угроз безопасности информации.
3. Описание источников угроз безопасности информации.
4. Описание способов реализации (возникновения) угроз безопасности информации.

5. Формирование перечня актуальных угрозы безопасности информации.

Помимо данного документа, базисным ресурсом при построении модели угроз является новый раздел Банка данных угроз ФСТЭК [2].

Первый этап оценки актуальности УБИ – определение негативных последствий от реализации (возникновения) угроз, предполагает заполнение таблицы, в рамках которой для каждого объекта информатизации организации (ИС/АС) описывается его назначение, существующие виды риска и возможные негативные последствия.

Виды риска (ущерба) – это три категории возможных последствий:

- для физического лица;
- для юридического лица;
- для государства.

Соотнесенный с видами риска перечень возможных негативных последствий представлен в методических рекомендациях ФСТЭК [1] (Приложение 4 к Методике оценки угроз безопасности информации), а также в новом разделе БДУ ФСТЭК в справочнике «Негативные последствия» [2].

Определяемые в ходе оценки угроз безопасности информации негативные последствия должны быть конкретизированы применительно к областям и особенностям деятельности обладателя информации или оператора.

На втором этапе должны быть определены объекты и компоненты систем и сетей, несанкционированный доступ к которым или воздействие на которые в ходе реализации (возникновения) угроз безопасности информации может привести к негативным последствиям – объекты воздействия.

Объекты и компоненты воздействия выделяются на основе анализа исходных данных и результатов инвентаризации систем и сетей. Опорный перечень объектов и компонентов систем и сетей представлен в новом разделе БДУ ФСТЭК [2] в справочниках «Объекты» и «Компоненты». Справочники интегрированы и при нажатии на объект можно увидеть входящие в него компоненты. Из рассмотрения должны быть исключены отсутствующие по результатам инвентаризации объекты и компоненты.

Третий этап – определение источников угроз безопасности информации. В качестве источника угрозы рассматривается нарушитель информационной безопасности. На основе оценки возможных целей реализации нарушителями угроз безопасности информации определяются виды нарушителей, актуальных для систем и сетей.

Нарушители, согласно Методике ФСТЭК, подразделяются на две категории:

- внешние нарушители – нарушители, не имеющие прав доступа в контролируемую зону и полномочий по доступу к информационным ресурсам, требующим авторизации;
- внутренние нарушители – нарушители, имеющие права доступа в контролируемую зону и полномочия по автоматизированному доступу к информационным ресурсам и компонентам систем и сетей.

В зависимости от уровня возможностей нарушители подразделяются на нарушителей, обладающих:

- базовыми возможностями по реализации угроз безопасности информации (Н1);
- базовыми повышенными возможностями по реализации угроз безопасности информации (Н2);
- средними возможностями по реализации угроз безопасности информации (Н3);
- высокими возможностями по реализации угроз безопасности информации (Н4).

Полный перечень возможных видов нарушителей с указанием категории и возможных целей реализации угроз представлен в приложении 6 Методики ФСТЭК [1], уровни возможностей нарушителей по реализации угроз безопасности информации подробно описаны в приложении 8 Методики ФСТЭК [1].

Итогом данного этапа должна стать таблица, в рамках которой каждый из существующих видов нарушителя будет оценен на предмет заинтересованности реализации УБИ в отношении объекта.

Указанные в рамках Методики ФСТЭК возможные цели нарушителя оцениваются отдельно применительно к физическим лицам, юридическим лицам и в отношении государства. Также в рамках этапа следует для каждого из видов нарушителей указать способы реализации угроз, которые он может реализовать в соответствии со своими возможностями. Полный перечень способов реализации угроз представлен в новом разделе БДУ ФСТЭК в справочнике «Способы реализации» [2].

На четвертом этапе производится описание способов реализации (возникновения) угроз безопасности информации. Способы реализации угроз безопасности информации определяются применительно к объектам воздействия, определенным в рамках второго этапа. Способы являются актуальными, когда возможности нарушителя позволяют их использовать для реализации угроз безопасности и имеются или созданы условия, при которых такая возможность может быть реализована в отношении объектов воздействия. Одна угроза безопасности информации может быть реализована несколькими способами.

Результатом данного этапа должна стать таблица, в рамках которой для каждого из актуальных способов реализации рассматриваются возможные объекты воздействия, точки входа (компоненты), и нарушители, способные его реализовать.

Способ реализации угрозы считается актуальным если хотя бы один из заинтересованных нарушителей имеет возможности, чтобы его реализовать.

В ходе последнего этапа, оценки угроз безопасности информации, должны быть определены возможные угрозы безопасности информации и оценена их актуальность для систем и сетей.

Угроза безопасности информации возможна, если имеются нарушитель или иной источник угрозы, объект, на который осуществляются воздействия,

способы реализации угрозы безопасности информации, а реализация угрозы может привести к негативным последствиям.

Актуальность возможных угроз безопасности информации определяется наличием сценариев их реализации. При наличии хотя бы одного сценария угрозы безопасности информации угроза признается актуальной для системы и сети.

Сценарий составляется как последовательность тактик и техник, применение которых возможно актуальным нарушителем с соответствующим уровнем возможностей в том числе с учетом доступности интерфейсов для использования соответствующих способов реализации угроз безопасности информации.

Перечень основных тактик и соответствующих им типовых техник, используемых для построения сценариев реализации угроз безопасности информации, приведен в приложении 11 к Методике ФСТЭК [1], а перечень способов реализации угроз, возможных к применению на объекте за счет наличия актуальных нарушителей с соответствующим уровнем возможностей, систематизируется на четвертом этапе.

Результатом данного этапа должна стать таблица 1, в рамках которой для каждой из 11 УБИ, представленных в рамках нового раздела БДУ ФСТЭК [2] будут описаны возможные способы реализации угроз (из числа возможных к применению на объекте), а также наиболее вероятные сценарии ее реализации.

Таблица 1

Актуальные угрозы безопасности информации

УБИ (11 угроз из БДУ ФСТЭК)	Способы реализации угроз (Актуальные на основе этапа 4 и под- ходят к УБИ)	Наиболее вероятный сценарий реализации УБИ (последовательность тактик и техник на основе таблицы 11.1 методики ФСТЭК, исходя из СП)	Вывод об актуальности угрозы (если есть хотя бы один сценарий реализации угрозы – угроза актуальна)
УБИ.1 Угроза утечки информации	СП.1 Эксплуатация уязвимостей СП.2 Использование недостатков конфигурации	T1(T1.2, T1.4) ->T2(T2.3, T2.8) ->...	Актуальна
...	...	...	...

Сформированный перечень угроз является результатом построения модели угроз безопасности информации. На его основе составляется список требуемых программных решений, обучений сотрудников и мер укрепления физической безопасности объекта.

Список источников

1. Методический документ «Методика оценки угроз безопасности информации» (утв. Федеральной службой по техническому и экспортному контролю 5 февраля 2021 г.).
2. Банк данных угроз безопасности информации / Федеральная служба по техническому и экспортному контролю. URL: <https://bdu.fstec.ru/threat-section> (дата обращения: 14.04.2025).

Статья поступила в редакцию 15.04.2025; принята к публикации 10.05.2025

Информация об авторах

Иваничкин В.В. – студент кафедры «Системы информационной безопасности», направление подготовки 10.00.00 – Информационная безопасность ФГБОУ ВО «БГТУ».

Шинаков К.Е. – к.т.н., доцент кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Волков В.И. – студент кафедры «Высокотехнологичное транспортное машиностроение», направление подготовки 13.03.03 – Энергетическое машиностроение ФГБОУ ВО «БГТУ».

Вклад авторов

Иваничкин В.В. – идея, сбор материала, частичное написание статьи (33%).

Шинаков К.Е. – обработка материала, частичное написание статьи, научное редактирование текста (34%).

Волков В.И. – сбор материала, частичное написание статьи (33%).

Конфликт интересов отсутствует.

Научная статья

УДК 004.056

Особенности построения политики защищенной обработки персональных данных

Ольга Сергеевна Козлова ^{1✉}, Егор Павлович Горбачев ^{2✉},

Екатерина Владимировна Кондрашова ^{3✉}

^{1,3} Брянский государственный технический университет, Брянск, Россия

³ Финансовый университет при Правительстве Российской Федерации, Москва, Россия

^{1,2} bryansk-tu@yandex.ru ✉

³ kondrashova_katerina@bk.ru ✉

Аннотация. В статье обсуждается, как усиливающиеся законодательные меры и нормативные акты, а также увеличения штрафов за нарушения в области безопасности способствуют созданию более защищенной среды. А также представлена предлагаемая последовательность построения политики защищенной обработки ПДн.

Ключевые слова: информационная безопасность, персональные данные, политика защищенности.

Для цитирования: Козлова О.С., Горбачев И.В., Кондрашова Е.В. Особенности построения политики защищенной обработки персональных данных // Актуальные проблемы кибербезопасности. Противодействие экстремизму и терроризму в информационной молодежной среде: сборник докладов I межрегиональной научно-практической конференции. – Брянск: БГТУ, 2025. – С. 236 – 239.

Значимость обеспечения информационной безопасности в целом и защиты персональных данных в частности растет стремительными темпами, в том числе это связано с тем, что на данный вопрос обращено пристальное внимание со стороны государства. Разрабатываются и дополняются нормативно правовые акты, систематизируются и увеличиваются штрафы за различные нарушения, увеличивается количество проверок со стороны регуляторов. Однако статистика все равно не утешительна – всего в 2024 году в РФ зарегистрировано 765,4 тысячи киберпреступлений, что составляет 40% от общего числа преступлений, наибольшее количество атак (15%) пришлось на государственные организации, сфера IT заняла второе место с 20% от общего числа атак и 14% высококритичных инцидентов [1].

Во многом это связано с тем, что наращивание требований и штрафов влияет укрепление системы ИБ косвенно, гораздо важнее системная структурная работа, производящаяся на уровне предприятия.

Начинаться системный подход должен в первую очередь с внутреннего аудита объекта и проработки комплексной политики защищенной обработки данных на основе ключевых нормативно-правовых документов. Для объектов, обрабатывающих персональные данные могут быть выделены следующие ключевые НПА:

- Федеральный закон №152 «О персональных данных» [2]:

- Постановление Правительства РФ № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» [3];
- Приказ ФСТЭК России № 21 «Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» [4];
- Постановление Правительства РФ № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» (действует до 2030 года) [5].

Требования, описанные в рамках нормативно правовой базы, должны быть реализованы на объекте в виде внедрения программных и технических средств защиты, а также посредством закрепления во внутренней политике защищенной обработки данных.

При фиксации требований в рамках ОРД рекомендуется возле каждого из пунктов внутреннего документа прописывать наименование и пункт нормативно-правового акта, закрепляющего необходимость соблюдения данного требования. Это существенно упростит в дальнейшем процедуру аудита информационной безопасности и ускорит, сделав более прозрачным процесс проведения проверок со стороны регулятора.

Специфику формирования политики защищенной обработки персональных данных можно отразить в следующей последовательности действий, которые целесообразно выполнить оператору при ее построении и поддержании в актуальном состоянии:

1. Определение целей обработки ПДн.

Оператору следует определить, для каких целей осуществляется сбор и обработка ПДн, действительно ли это необходимо и нет ли избыточного сбора информации.

2. Изучение действующего законодательства о защите ПДн.

Оператору следует детально изучить требования нормативно-правовых актов, регламентирующих обработку персональных данных, помимо указанных выше законодательных актов, рассмотрению подлежат НПА, выпущенные органами местного самоуправления, а также положения КоАП и УК РФ.

3. Определение технических, программных и организационных мер, необходимых для защиты ПДн.

Здесь следует уделить внимание не только тому, что является обязательным со стороны законодательства, но и тому, что необходимо в условиях конкретного объекта, чтоб обеспечить защищенную обработку ПДн.

4. Оценка рисков и возможного ущерба.

На данном этапе необходимо произвести комплексный анализ возможных для объекта рисков и их последствий. В первую очередь с точки зрения возможных затрат на выплату штрафов, компенсаций пострадавшим субъектам и восстановление поврежденных активов. Здесь же можно рассмотреть финансовые

риски, связанные с простым организационным и снижением доверия со стороны клиентской базы. Данный этап позволит оценить экономическую целесообразность внедрения мер и средств, которые необходимы к внедрению по результатам прошлого этапа.

5. Внедрение технических и программных мер защиты, разработка внутренней организационно-распорядительной документации.

Непосредственно практический этап, на котором следует структурировать все процессы объекта и механизмы защиты ПДн в совокупности с требованиями законодательства в единую внутреннюю нормативную базу.

6. Обучение сотрудников.

Этап, который часто упускается из виду, но является самым важным. Без обучения персонала и внедрения подходов политики во внутренние процессы работы объекта, это будет просто очередной документ, не несущий в себе эффективности по защите от угроз безопасности информации. Руководству совместно со специалистами по обеспечению ИБ следует продумать план обучающих мероприятий и инструктажей, позволяющих донести до сотрудников суть прописанных требований и важность их соблюдения.

7. Мониторинг, аудит и обновление.

Чтобы закрепить эффективность произведенных инструктажей и сделать документальную базу эффективной в перспективе принимаемых решений и реструктуризаций, необходимо также разработать систему мониторинга за соблюдением политики и регулярного аудита. Она позволит отмечать и устранять выявленные пробелы в системе технической и программной защиты, в действиях сотрудников, а также в соответствии возможностей инфраструктуры предъявляемым требованиям.

Таким образом, предлагаемая последовательность построения политики защищенной обработки ПДн учитывает все нюансы процесса, чтобы сделать его результат наиболее эффективным и оказывающим влияние как на обеспечение информационной безопасности отдельных объектов, так и на улучшение обстановки в данной сфере в масштабах государства.

Список источников

1. Подборка статистических данных по информационной безопасности в России за 2024 год. – URL: <https://it-pole.com/about/events/podborka-statisticheskikh-dannykh-po-informatsionnoy-bezopasnosti-v-rossii-za-2024-god/> (дата обращения: 11.03.2025).

2. Федеральный закон «О персональных данных» от 27.07.2006 N 152-ФЗ (последняя редакция) // КонсультантПлюс. URL: https://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения: 14.04.2025).

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» // КонсультантПлюс. URL:

https://www.consultant.ru/document/cons_doc_LAW_137356/8c86cf6357879e861790a8a7ca8bea4227d56c72/ (дата обращения: 14.04.2025).

4. Приказ ФСТЭК России от 18.02.2013 N 21 (ред. от 14.05.2020) «Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (зарегистрировано в Минюсте России 14.05.2013 N 28375) // КонсультантПлюс. URL: https://www.consultant.ru/document/cons_doc_LAW_146520/ (дата обращения: 14.04.2025).

5. Постановление Правительства РФ от 15.09.2008 N 687 (ред. от 18.01.2025) «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» // КонсультантПлюс. URL: https://www.consultant.ru/document/cons_doc_LAW_80028/ee799eb6aa3e266dc1fcb9454b0c5e57fda5da68/ (дата обращения: 14.04.2025).

Статья поступила в редакцию 12.04.2025; принята к публикации 10.05.2025

Информация об авторах

Козлова О.С. – студент кафедры «Системы информационной безопасности», направление подготовки 10.00.00 – Информационная безопасность ФГБОУ ВО «БГТУ».

Горбачев Е.П. – аспирант кафедры «Корпоративные финансы» ФГБОУ ВО «Финансовый университет при Правительстве Российской Федерации».

Кондрашова Е.В. – ассистент кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Вклад авторов

Козлова О.С. – идея, сбор материала, частичное написание статьи (33%).

Горбачев И.В. – обработка материала, частичное написание статьи, научное редактирование текста (33%).

Кондрашова Е.В. – сбор материала, частичное написание статьи, научное редактирование текста (34%).

Конфликт интересов отсутствует.

Научная статья

УДК 004.056

Особенности построения модели угроз по методическим рекомендациям ФСБ России

Ольга Сергеевна Козлова ^{1✉}, Станислав Владимирович Сафоненко ^{2✉},

Оксана Михайловна Голембиовская ^{3✉}

^{1,2,3}Брянский государственный технический университет, Брянск, Россия

^{1,2,3}bryansk-tu@yandex.ru✉

Аннотация. В статье представлена методология разработки документа, регламентирующего обеспечение безопасности данных в информационных системах (ИСПДн) организации. Особое внимание уделено обоснованию необходимости и порядку применения средств криптографической защиты информации (СКЗИ) в соответствии с требованиями законодательства РФ и рекомендациями ФСБ.

Ключевые слова: информационная безопасность, модель угроз, методические рекомендации ФСБ.

Для цитирования: Козлова О.С., Сафоненко С.В., Голембиовская О.М. Особенности построения модели угроз по методическим рекомендациям ФСБ России // Актуальные проблемы кибербезопасности. Противодействие экстремизму и терроризму в информационной молодежной среде: сборник докладов I межрегиональной научно-практической конференции. – Брянск: БГТУ, 2025. – С. 240 – 246.

Построение модели угроз является важным элементом в сфере обеспечения информационной безопасности как для государственных учреждений, так и для коммерческих организаций. В России, помимо методических рекомендаций ФСТЭК разработаны методические рекомендации Федеральной службы безопасности (ФСБ) [1], которые помогают организациям формировать комплексный подход к идентификации и анализу потенциальных угроз, возникающих при обработке персональных данных в информационных системах персональных данных (ИСПДн), в которых в том числе для обеспечения защиты данных используются средства криптографической защиты информации (СКЗИ).

Документ имеет последовательную структуру и включает в себя 3 основных раздела:

1. Общее описание информационных систем персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности.
2. Определение актуальности использования СКЗИ для обеспечения безопасности персональных данных.
3. Определение актуальных угроз.

В рамках первого раздела описываются ИСПДн рассматриваемого объекта. Методические рекомендации ФСБ [1] различают однотипные и разноплановые информационные системы, однотипными считаются схожие системы, имеющие одинаковую структуру и обрабатывающие одинаковые категории ПДн

(например, ИСПДн центрального офиса и ИСПДн филиалов в субъектах), разноплановыми считаются системы различных структур, обрабатывающие разные категории ПДн. Однотипные системы могут быть сформированы в общую группу, для которой будет описана наиболее полная общая информация о среде их функционирования, разноплановые системы описываются отдельно.

Основные данные, которые следует отразить:

- наименование и назначение ИСПДн / группы однотипных ИСПДн;
- тип ИСПДн (единая для всех ПДн или совокупность изолированных или взаимосвязанных информационных подсистем);
- объем и содержание персональных данных, обрабатываемых в ИСПДн (если ИСПДн не единая - отдельно для каждой подсистемы);
- объекты, в которых размещены ресурсы ИС и физические меры защиты объектов, в которых размещены ресурсы ИС;
- наличие или отсутствие информационного взаимодействия с другими ИС и подсистемами ИС + отметка о факте передачи ПДн;
- используемые в ИС и подсистемах каналы связи, включая кабельные системы;
- применяемые меры по ограничению несанкционированного доступа (НСД) к защищаемой информации, передаваемой по каналам связи + отметка тех каналов, НСД к которым невозможен;
- носители защищаемой информации, используемые в каждой подсистеме ИС или в ИС в целом (за исключением каналов связи).

Данную информацию можно описать текстом или в формате таблицы.

Во втором разделе в первую очередь необходимо обосновать актуальность использования СКЗИ, согласно методическим рекомендациям ФСБ [1] использование СКЗИ для обеспечения безопасности персональных данных необходимо в следующих случаях:

- если персональные данные подлежат криптографической защите в соответствии с законодательством Российской Федерации;
- если в информационной системе существуют угрозы, которые могут быть нейтрализованы только с помощью СКЗИ. Случаи, когда угрозы могут быть нейтрализованы только с помощью СКЗИ также описаны в методике.

Далее следует привести описание ресурсов ИСПДн объекта, в которых размещены СКЗИ в формате текста или таблицы, где отразить:

- наименование и назначение ИСПДн / группы однотипных ИСПДн;
- помещения, в которых расположены ресурсы ИС имеющие отношение к СКЗИ;
- меры по разграничению доступа в помещения;
- информационные технологии, базы данных, технические средства, ПО используемые в ИС для обработки ПДн и относящиеся к СКЗИ;
- отчуждаемые носители защищаемой информации, используемые в ИС, для которых НСД не может быть исключен без СКЗИ;
- область и цели применения СКЗИ в ИС.

К областям применения СКЗИ могут относиться:

- взаимодействие с автоматизированными банковскими системами и государственными информационными системами;
- хранение корпоративных данных и обмен ими с филиалами и партнерами;
- взаимодействие информационных систем медицинских и иных организаций с Единой государственной информационной системой здравоохранения (ЕГИСЗ);
- предоставление цифровых или электронных услуг.

Цели применения СКЗИ в информационных системах могут формулироваться следующим образом:

- уберечь информацию во время её изменения, использования и отправки;
- обеспечить целостность и подлинность данных при хранении, обработке и распространении;
- создавать информацию, которая будет применяться для аутентификации и идентификации субъектов, людей и устройств;
- выработать данные, используемые для сохранности аутентифицирующих средств при их хранении, создании, изменении и передаче.

В этом же разделе необходимо составить матрицу доступа к СКЗИ, пример которой представлен в табл. 1.

Таблица 2

Пример матрицы доступа к СКЗИ

Должность	СКЗИ	Среда функционирования СКЗИ	Информация, относящаяся к криптографической защите ПДн, включая ключевую, парольную и аутентифицирующую информацию СКЗИ
Главный бухгалтер	Имеет доступ к КriptoПро CSP, ЭЦП	Используется при передаче отчетности и прочей информации в СФР, ФНС	ПДн работников и данные бухгалтерского и кадрового учета
Руководитель отдела маркетинга	Не имеет доступа к СКЗИ		
Руководитель отдела продаж	Не имеет доступа к СКЗИ		

Последний раздел является ключевым, в нем определяются ключевые объекты защиты (применяемые в ИСПДн СКЗИ, используемые каналы связи, помещения с СКЗИ и руководящая документация, связанная с функционированием СКЗИ), описываются потенциальные источники атак (пример описания представлен в табл. 2), на основании исходных данных об информационных системах, объектах защиты и источниках атак заполняется таблица об обобщенных возможностях источников атак (шаблон представлен в табл. 1 методических рекомендаций ФСБ [1]), и таблица обоснования актуальности существующих

угроз. Общий пример данной таблицы представлен в табл. 2 методических рекомендаций ФСБ [1], пример более детализированного описания для конкретной организации представлен в табл. 3.

Таблица 3

Пример описания источников атак

Источники атак	Возможности доступа
Главный бухгалтер	<i>Осуществляет формирование и отправку отчетности по защищенному каналу в контролирующие ведомства.</i> Имеет доступ в контролируемую зону по пропуску на КПП, помещения, в которых находятся ресурсы ИСПДн ООО «Организация», имеющие отношение к криптографической защите ПДн, к документации на СКЗИ, к техническим и программным средствам СКЗИ и СФ.
Руководитель отдела маркетинга Руководитель отдела продаж Руководитель отдела кадров	<i>Осуществляют выполнение должностных обязанностей, не связанных с функционированием и использованием СКЗИ, имеют доступ в кабинет главного бухгалтера в связи с тем, что утверждают сметы и проходящие платежи.</i> Имеет доступ в контролируемую зону по пропуску на КПП, помещения, в которых находятся ресурсы ИСПДн ООО «Организация», имеющие отношение к криптографической защите ПДн. Не имеют доступа к документации на СКЗИ, к техническим и программным средствам СКЗИ и СФ.
Сотрудники бухгалтерии, и прочих отделов	<i>Осуществляют выполнение должностных обязанностей, не связанных с функционированием и использованием СКЗИ.</i> Имеют доступ в контролируемую зону по пропуску на КПП, не имеют доступа к техническим и программным средствам СКЗИ и СФ, документации на СКЗИ и помещениям, в которых находятся ресурсы ИСПДн ООО «Организация», имеющие отношение к криптографической защите ПДн.
Партнеры организации	<i>Проводят переговоры с руководством организации по вопросам сотрудничества.</i> Имеют доступ в контролируемую зону по заранее выписанному пропуску на КПП, не имеют доступа к техническим и программным средствам СКЗИ и СФ, документации на СКЗИ и помещениям, в которых находятся ресурсы ИСПДн ООО «Организация», имеющие отношение к криптографической защите ПДн.
Администратор ИБ (привилегированный пользователь)	<i>Осуществляет техническое обслуживание технических и программных средств СКЗИ и СФ, включая их настройку, конфигурирование и распределение ключевой документации между непривилегированными пользователями.</i> Имеет доступ в контролируемую зону по пропуску на КПП, помещения, в которых находятся ресурсы ИСПДн ООО «Организация», имеющие отношение к криптографической защите ПДн, к документации на СКЗИ, к техническим и программным средствам СКЗИ и СФ.
Внешние источники (клиенты, конкуриру-	Не имеют возможности доступа в контролируемую зону, обслуживание клиентов производится в выездном порядке без личного посещения объекта, доступ лиц на объект строго ограничен, сотрудники проходят через КПП

Источники атак	Возможности доступа
щие организации, ха- керы и прочие заинтере- сованные лица)	

Таблица 4

Детализированный пример заполнения таблицы обоснования актуальности су-
ществующих угроз

№	Уточненные воз- можности нару- шителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построе- ния и реализа- ции атак	Обоснование отсутствия
1.1	проведение атаки при нахождении в пределах контро- лируемой зоны	не актуально	1.Проводятся работы по подбору персо- нала – в организации утвержден регламент подбора персонала, в котором утверждены требования к кандидатам на должность (к примеру отсутствие судимости), утвер- ждены формы входных анкет по зна- ниям/умениям/навыкам относительно ра- боты с информационными ресурсами ком- пании, что дает возможность уже на первом этапе спрогнозировать потенциал наруши- теля и более внимательно относиться к его работе, а также разъяснена ответственность за противоправные деяния относительно информационных ресурсов компании (Ре- гламент утвержден приказом №13 от 23.04.2025 г.). 2. Доступ в контролируемую зону, где располагается СКЗИ, обеспечивается в соответствии с контрольно-пропускным режимом – на объекте Приказом № 15 от 23.04.2024 г. введен Пропускной режим. В рамках данного приказа утверждено Поло- жение о пропускном режиме, которым ре- гламентирована выдача ключей, хранение ключей, действия в результате внештатных ситуаций. 3. Представители технических, обслужи- вающих и других вспомогательных служб при работе в помещениях (стой- ках), где расположены СКЗИ, и сотруд- ники, не являющиеся пользователями СКЗИ, находятся в этих помещениях только в присутствии сотрудников по эксплуатации – на объекте Приказом №67

№	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
			от 23.04.2023 утверждено Положение о порядке обеспечения безопасности при работе с СКЗИ, в рамках которого прописано, что представители технических, обслуживающих и других вспомогательных служб при работе в помещениях, где расположены СКЗИ, и сотрудники, не являющиеся пользователями СКЗИ, находятся в этих помещениях только в присутствии сотрудников по эксплуатации. 4. Сотрудники, являющиеся пользователями ИСПДн, но не являющиеся пользователями СКЗИ, проинформированы о правилах работы в ИСПДн и ответственности за несоблюдение правил обеспечения безопасности информации — при приеме на работу производится подробный инструктаж о правилах работы в ИСПДн, после которого сотрудники подписывают лист ознакомления, помимо этого обязанность по обеспечению безопасности информации в ходе выполнения должностных обязанностей прописана в должностной инструкции. 5. Пользователи СКЗИ проинформированы о правилах работы в ИСПДн, правилах работы с СКЗИ и ответственности за несоблюдение правил обеспечения безопасности информации – при приеме на работу производится подробный инструктаж о правилах работы в ИСПДн и с СКЗИ, сотрудники подписывают лист ознакомления, помимо этого обязанность по обеспечению безопасности информации в ходе выполнения должностных обязанностей прописана в должностной инструкции.

Данная таблица является итогом построения модели угроз в соответствии с требованиями ФСБ.

Таким образом, построение модели угроз по методическим рекомендациям ФСБ – это сложный, но важный процесс, который требует внимательного и системного подхода. Порядок построения имеет свои особенности и сконцентрирован на оценке, связанной с применением криптографических средств защиты

информации. Разработка данного документа совместно с другими ОРД позволяет комплексно оценить потенциальные угрозы и уязвимости, связанные с защищенным хранением и передачей данных.

Список источников

1. Методические рекомендации / Федеральная служба безопасности Российской Федерации. URL: http://www.fsb.ru/files/PDF/Metodicheskie_recomendacii.pdf (дата обращения: 14.04.2025).

Статья поступила в редакцию 16.04.2025; принята к публикации 10.05.2025

Информация об авторах

Козлова О.С. – студент кафедры «Системы информационной безопасности», направление подготовки 10.00.00 – Информационная безопасность ФГБОУ ВО «БГТУ».

Сафоненко С.В. – аспирант кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Голембиовская О.М. – к.т.н., доцент кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Вклад авторов

Козлова О.С. – идея, сбор материала, частичное написание статьи (33%).

Сафоненко С.В. – обработка материала, частичное написание статьи, научное редактирование текста (33%).

Голембиовская О.М. – сбор материала, частичное написание статьи, научное редактирование текста (34%).

Конфликт интересов отсутствует.

Научная статья

УДК 004.056.5

Анализ основных видов уязвимостей информационной безопасности учреждений сферы здравоохранения

Галина Дмитриевна Матюхина^{1✉}, Кирилл Андреевич Седаков²

^{1, 2}Брянский государственный технический университет, Брянск, Россия

¹ galinochka2303@gmail.com✉, <https://orcid.org/0009-0001-1295-2944>

² sekira98@mail.ru, <https://orcid.org/0009-0002-9284-4624>

Аннотация. В данной статье изучены уязвимости медицинских организаций и меры обеспечения безопасности.

Ключевые слова: сфера здравоохранения, DLP, «подделка личности», персональные данные пациентов, уязвимости, врачебная тайна.

Для цитирования: Матюхина Г.Д., Седаков К.А. Анализ основных видов уязвимостей информационной безопасности учреждений сферы здравоохранения //Актуальные проблемы кибербезопасности. Противодействие экстремизму и терроризму в информационной молодежной среде: сборник докладов I межрегиональной научно-практической конференции. – Брянск: БГТУ, 2025. – С. 247 – 250.

Медицинские учреждения России хранят и обрабатывают обширную базу конфиденциальных данных, требующую надежной защиты от потенциальных угроз и уязвимостей. Для повышения эффективности медицинской помощи актуальна интеграция современных информационных технологий в практику работы медицинских учреждений. В первом квартале 2024 года зафиксировано более сорока случаев утечек персональных данных пациентов [1].

В медицинских учреждениях обрабатываются два типа персональных данных: базовые и специальные. К базовым относятся: место рождения, физические параметры пациента, имя, дата рождения, а диагнозы и детали лечения к специальным. Эти сведения объединяются под термином «врачебная тайна» (п. 1 ст. 13 Федеральный закон №323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации») [2].

Информация медицинского характера, как правило, становится объектом кибератак, что приводит к утечкам конфиденциальных данных из медицинских учреждений. Среди всех существующих угроз информационной безопасности для организаций здравоохранения наиболее распространены следующие: «подделка» личности сотрудником организации, внедрение зловредного или разрушительного ПО, исчерпание системных ресурсов и т.д. [3].

Интеграция учетных записей, принадлежащих другим сотрудникам организации, с целью извлечения выгоды, может рассматриваться как «подделка» чужой личности [4]. Такое действие равносильно «подделке» другого лица и влечет за собой нарушение конфиденциальности медицинской информации.

Использование поставщиками продукции и услуг полученных данных относящихся к «врачебной тайне» является серьезной угрозой. Такое поведение, именуемое «подделка другого лица», представляет собой нарушение правил безопасного использования внешних ресурсов за счёт внедрения вредоносного ПО. В результате подобных действий может произойти утечка конфиденциальной информации о состоянии здоровья пациентов.

Представление собой другого лица третьими сторонами влечет за собой несанкционированный доступ к информации или ресурсам системы под видом уполномоченного пользователя. Такое проникновение может осуществляться путем обмана, позволяющего стать уполномоченным пользователем [4]. Данный вид проникновения может осуществляться такими лицами как: журналисты, частные детективы и «хак-активисты» (хакеры, действующие от имени или в поддержку политических групп).

Данные угрозы могут быть следствием уязвимостей. Уязвимости ПО — «дыры» в программном обеспечении, которыми пользуются преступники, чтобы взломать систему ИБ.

Эта уязвимость может привести к блокированию доступа к данным или даже к несанкционированной передаче конфиденциальных медицинских данных третьим лицам.

Атаки злоумышленников осуществляются на работников, которые работают в системе в целом. Низкий уровень осведомлённости в сфере информационной безопасности сотрудников — уязвимость. Атаки осуществляются через электронную почту, звонки на стационарные телефоны или другие коммуникационные каналы. Цель этих действий — доступ к информации данных учреждений.

Мошенники могут использовать эти данные в целях:

1. Собственного обогащения.
2. Создание фейковой личности.
3. Использование медицинских данных для получения медицинской помощи или лекарственных препаратов от имени другого лица.
4. Получение материальной выгоды с помощью шантажа.

Исходя из этого, для обеспечения защиты конфиденциальности и безопасности информации о пациентах, а также для поддержки целостности и доступности критически важных систем и инфраструктуры нужно применять организационные и технические меры для минимизации данных угроз и уязвимостей. На данный момент мерами защиты от вышерассмотренных уязвимостей являются:

1. Создание в медицинском учреждении чёткого регламента по работе с медицинскими данными, который выделяет основную критически важную информацию, обозначает её в отдельную категорию и создаёт правила её обработки и хранения. Контроль исполнения этого регламента на практике.
2. Жёсткий учёт носителей информации и введение ограниченного круга лиц, имеющих разрешенный доступ к этим данным.

3. Письменное уведомление сотрудников об ответственности за разглашение конфиденциальной информации, либо заключение соответствующих юридических договоров.

4. Внедрение соответствующих инструментов контроля и мониторинга информации в организации. Такие как, система предотвращения потери данных (DLP). **Принцип работы DLP-систем:** анализ всей информации: исходящей, входящей и циркулирующей внутри компании. Система отслеживает ввод данных, передачу файлов, печать документов, активность на сайтах и многое другое. Если обнаруживаются подозрительные действия, ПО принимает меры блокировки или оповещения [5].

5. Внедрение систем, которые помогут зафиксировать все происходящие события в коммуникациях и действиях пользователей, угрожающие безопасности, а также, обнаружить сотрудников, инициировавших наступление этих событий. Кроме того, рекомендуется стек технологий защиты медицинских данных дополнять различными техническими и программно-аппаратными решениями. С их помощью возможно охватить всю информационную структуру учреждения, своевременно выявлять инциденты безопасности [6].

Таким образом, данные угрозы способны вызвать несанкционированный доступ к информации, нарушить конфиденциальность персональных данных граждан и быть использованы злоумышленниками в противоправных целях. Данное обстоятельство противоречит законодательству Российской Федерации и ведёт к определенным мерам ответственности, поэтому защита медицинских данных – это прямая обязанность учреждений данной сферы деятельности, вступающих в отношения с пациентами, ведущими обработку ПДн и врачебной тайны. Для того чтобы минимизировать данные уязвимости должно быть реализованы регулярные автоматизированные мониторинги движения и использования конфиденциальной информации и исходя из этого, минимизировать риски, связанных с информацией, которая обрабатывается в учреждениях сферы здравоохранения.

Список источников

1. Утечки конфиденциальной информации в сфере здравоохранения | аналитический отчет за девять месяцев. - URL: <https://www.infowatch.ru/analytics/analitika/utechki-konfidentsialnoy-informatsii-v-sfere-zdravookhraneniya-otchet-za-devyat-mesyatsev?ysclid=lw6kkihodw226914815> (дата обращения: 12.03.2025).

2. Федеральный закон «Об основах охраны здоровья граждан в Российской Федерации» от 21.11.2011 N 323-ФЗ (последняя редакция) // КонсультантПлюс. - URL: https://www.consultant.ru/document/cons_doc_LAW_121895 (дата обращения: 12.03.2025).

3. Приложение А (справочное). Угрозы защиты медицинской информации | ГАРАНТ. - URL:

<https://base.garant.ru/71742172/53f89421bbdaf741eb2d1ecc4ddb4c33> (дата обращения: 01.04.2025).

4. ГОСТ Р ИСО 27799-2015. Информатизация здоровья. Менеджмент защиты информации в здравоохранении по ИСО/МЭК 27002. - URL: <https://ohranatruda.ru/upload/iblock/11f/4293755562.pdf?ysclid=luedtjcfz5510433452> (дата обращения: 12.03.2025).

5. DLP-системы для бизнеса: что это и как работает, виды, как выбрать. - URL: <https://lwcom.ru/blog/dlp-sistemy-dlya-biznesa-cto-eto-i-kak-rabotaet-vidy-kak-vybrat/> (дата обращения: 12.04.2025).

6. Защита медицинских данных: как защитить ПДн пациентов от разглашения? - URL: https://rt-solar.ru/products/solar_dozor/blog/3205/ (дата обращения: 12.04.2025).

Статья поступила в редакцию 20.04.2025; принята к публикации 10.05.2025

Информация об авторах

Матюхина Г.Д. - студент кафедры «Системы информационной безопасности», направление подготовки 10.05.03 – Информационная безопасность автоматизированных систем ФГБОУ ВО «БГТУ».

Седаков К.А. - ассистент кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Вклад авторов

Матюхина Г.Д. - идея, сбор материала, обработка материала, частичное написание статьи (50%).

Седаков К.А. - написание статьи, научное редактирование текста (50%).

Конфликт интересов отсутствует.

Научная статья

УДК 004.8

Основные показатели защищенности при проведении оценки эффективности системы защиты персональных данных в медицинских учреждениях

Кирилл Андреевич Седаков ^{1✉}, Михаил Юрьевич Рытов ²

^{1, 2}Брянский государственный технический университет, Брянск, Россия

¹sekira98@mail.ru ✉, <https://orcid.org/0009-0002-9284-4624>

²ozikts@yandex.ru, <https://orcid.org/0234-0023-2435-5763>

Аннотация. Рассмотрены основные критерии в проведении оценки эффективности принятых мер и средств в обеспечении защиты персональных данных в медицинских учреждениях.

Ключевые слова: оценка эффективности защиты персональных данных, алгоритм проведения аудита информационной безопасности.

Для цитирования: Седаков К.А., Рытов М.Ю. Основные показатели защищенности при проведении оценки эффективности системы защиты персональных данных в медицинских учреждениях // Актуальные проблемы кибербезопасности. Противодействие экстремизму и терроризму в информационной молодежной среде: сборник докладов I межрегиональной научно-практической конференции. – Брянск: БГТУ, 2025. – С. 251 – 254.

В наше время информационная безопасность становится все более актуальной темой, особенно в организациях сферы здравоохранения, где хранится большое количество чувствительных данных о пациентах. Информационная безопасность в здравоохранении имеет огромное значение, поскольку личные медицинские данные пациентов являются конфиденциальной информацией, требующей особой защиты.

Стоит также отметить, что медицинские учреждения относятся к критической информационной инфраструктуре (КИИ), потому что она связана с наиболее критичной информацией — данными о состоянии здоровья пациентов. Согласно Федеральному закону №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», учреждения сферы здравоохранения относятся к субъектам КИИ, а имеющиеся у них информационные системы, автоматизированные системы и информационно-телекоммуникационные сети, в случае участия их в критических процессах, являются объектами КИИ. Основная цель заключается в создании эффективного способа оценки эффективности средств и методов защиты персональных данных [1].

Таким образом, можно сделать вывод о том, что перед медицинскими учреждениями в современных реалиях стоят следующие основные задачи в области обеспечения защиты персональных данных:

- минимизировать различные угрозы безопасности информации и снизить ущерб от реализации данных угроз, которые могут привести к различным экономическим и репутационным последствиям;

- защитить данные, составляющие тайну (коммерческую, врачебную, персональные данные и т. д.);
- повысить защищённость медицинских учреждений от внешних угроз и атак.

Таким образом, можно сделать вывод о том, что для определения показателей защищенности нужно определить актуальность угроз конфиденциальной информации в медицинских учреждениях, необходимо определиться с тем, что такое ПДн в контексте здравоохранения. Их определение сформулировано в Федеральном законе № 149 от 27.07.2006 «Об информации, информационных технологиях и о защите информации», где они представлены как «информация ограниченного доступа». В ФЗ уточнено, что конфиденциальность персональных данных – это обязательное условие работы с ними, и поэтому государство устанавливает обязательные нормы и правила их обработки. Согласно федеральному закону от 27.07.2006 №152-ФЗ «О персональных данных» и памятке для медицинских учреждений по актуальным проблемам обработки персональных данных, сформированной федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор), персональными данными является любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (ФИО, дата рождения, место проживания, биологические параметры, сведения о состоянии здоровья, результаты анализов, сведения о факте обращения гражданина за оказанием медицинской помощи, состоянии его здоровья и диагнозе, иные сведения, полученные при его медицинском обследовании и лечении и т.д.). Эти же данные, на основании ФЗ от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации» составляют врачебную тайну и попадают под действие настоящего закона. Доступ к данной информации злоумышленниками может быть использован, например, для шантажа, мошенничества, подделке документов и так далее. А это, в свою очередь, может нанести большой ущерб как владельцу, так и организации, которой было дано согласие на обработку этих данных [5].

Одной из ключевых проблем при выявлении текущих угроз безопасности ПДн в здравоохранении является постоянно меняющийся характер киберугроз. Хакеры постоянно разрабатывают новые методы и инструменты для использования уязвимостей в системах здравоохранения и получения доступа к конфиденциальной информации. Отсюда возникает необходимость организациям здравоохранения проявлять повышенную бдительность при мониторинге своих систем и сетей на предмет любых признаков подозрительной активности – от атак программ-вымогателей до фишинговых атак.

Кроме того, отдел ИБ должен обеспечить защиту данных, которые хранятся в медицинской информационной системе на всех уровнях работы клиники: информация о медицинских учреждениях (общие данные, отчётность), сведения о медперсонале, в том числе конфиденциальные сведения, сведения о пациентах, важные сведения о системе здравоохранения в целом.

Для определения оценки риска сформированный алгоритм оценки ущерба от нарушения свойств защищенности должен базироваться на экспертно-статистической оценке, особенностью которой является использование метода прогнозного графа [2].

Следующий показатель, который нужно определить, это анализ актуальных угроз и выявление вероятности реализации угрозы. Помимо этого, в рамках определения данного показателя должны быть сформированы группы угроз, чтобы определить степень вариативности реализации угроз. При анализе угроз из состава Банка данных угроз (БДУ) ФСТЭК необходимо производить систематизацию перечисленных угроз [4]. Кроме нормативно-правовых актов (НПА) регулятора, Министерство здравоохранения выпустило внутренние НПА, в которых содержатся требования к государственным информационным системам в сфере здравоохранения (все ИСПДн медицинского назначения являются таковыми) и методические рекомендации по защите медицинских информационных систем (МИС).

Согласно этим рекомендациям оценочные мероприятия при определении актуальных угроз безопасности предлагается производить экспертным методом, что не всегда возможно и приемлемо для ИСПДн медицинского назначения. Сотрудники, привлекаемые в качестве экспертов, могут не обладать необходимой квалификацией при оценке угроз, также оценка может иметь субъективный характер. Согласно статистическим данным в сфере здравоохранения только в 29% случаев ИС их защитой занимаются профильные специалисты, а выделенные отделы информационной безопасности существуют только в 10% медицинских учреждений. Особенно эти проблемы актуальны при создании ИСПДн медицинского назначения для отдельных медицинских учреждений. Для его определения можно использовать данные, полученные ранее, а именно коэффициент важности и общее количество угроз, выявленных для данного медицинского учреждения [3].

Далее должна оцениваться степень критичности групп угроз. Этот показатель можно рассчитать с помощью значений коэффициента риска, последствия от реализации угрозы (ценность актива), количество определенных угроз.

Исходя из полученных данных, можно провести оценку уровня риска информационной безопасности. Показатель уровня риска информационной безопасности определяет, будет ли реализована угроза с учетом вероятности реализации угрозы и уровня коэффициента риска информационной безопасности. Уровень риска можно будет определить с помощью таких данных как возможность реализации угрозы и коэффициент риска. После расчета будут получены количественные оценки. Чтобы лучше понять их значения, можно будет перенести данный результат в качественные с помощью шкалы оценок.

В завершении всей работы, зная все ранее изученные показатели, можно определить итоговую оценку эффективности защиты персональных данных в медицинских учреждениях. Оценка эффективности формируется благодаря сравнительному анализу, который был получен в результате расчета таких показателей, как уровень риска и вероятности реализации угроз.

Таким образом, предложенные показатели в защищенности при проведении оценки эффективности системы защиты персональных данных можно использовать для оценки эффективности систем защиты в медицинских учреждениях. Разработка алгоритма оценки эффективности на основе данных показателей позволит значительно сократить финансовые и технические затраты на определение уровня защищенности учреждений, которые относятся к сфере здравоохранения.

Список источников

1. Дорошенко И.Е. Вопросы описания возможных сценариев угроз при разработке моделей угроз безопасности информации / И.Е. Дорошенко, М.О. Максудов, В.В. Селифанов // Интерэкспо Гео-Сибирь. 2021. Т. 7. № 1. С. 16-21.
2. Жук Р.В. Определение актуальности угроз информационной безопасности в информационных системах обработки персональных данных с использованием математического аппарата нейронных сетей / Р.В. Жук, П.И. Дзьобан, А.В. Власенко // Прикаспийский журнал: управление и высокие технологии. 2020. № 1(49). С. 169-178.
3. Кучкарова Н. В. Применение моделей интеллектуального анализа текстов при оценке угроз информационной безопасности // Современные проблемы цивилизации и устойчивого развития в информационном обществе: сборник материалов VI международной научно-практической конференции, Москва, 30 декабря 2021 года. - Москва: Институт развития образования и консалтинга, 2021. - С. 178-184.
4. Аверченков В. И. Аудит информационной безопасности: учебное пособие для вузов. - Брянск: Брянский государственный технический университет, 2012. - 268 с. - ISBN 978-89838-487-6. - URL: <http://www.iprbookshop.ru/6991.html>.

Статья поступила в редакцию 19.04.2025; принята к публикации 10.05.2025

Информация об авторах

Седаков К.А. - ассистент кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Рытов М.Ю. - д.т.н., зав. кафедрой «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Вклад авторов

Седаков К.А. - идея, сбор материала, обработка материала, написание статьи (50%).

Рытов М.Ю. - научное редактирование текста (50%).

Конфликт интересов отсутствует.

Научная статья

УДК 004.056

Сканирование сетей в информационной безопасности

Екатерина Николаевна Янченко

Брянский государственный технический университет, Брянск, Россия

kataancenko5@gmail.com, <https://orcid.org/0009-0001-3176-4404>

Аннотация. В статье рассматриваются методы и инструменты сканирования сетевой инфраструктуры, применяемые для выявления уязвимостей в информационных системах. Описаны подходы к активному и пассивному сканированию, а также возможности популярных программных решений, включая Nmap, Masscan, Nessus и Wireshark. Также затрагиваются вопросы правового регулирования проведения сканирования в Российской Федерации.

Ключевые слова: информационная безопасность, сканирование, пентест, уязвимости, проникновение.

Для цитирования: Янченко Е.Н. Сканирование сетей в информационной безопасности // Актуальные проблемы кибербезопасности. Противодействие экстремизму и терроризму в информационной молодежной среде: сборник докладов I межрегиональной научно-практической конференции. – Брянск: БГТУ, 2025. – С. 255 – 258.

Организации всё чаще оказываются под угрозой несанкционированного доступа к своим внутренним ресурсам, что связано с ростом числа технически простых, но эффективных атак. По данным исследования, проведённого Positive Technologies в 2023 году, в 96% компаний удалось смоделировать успешное проникновение во внутреннюю сеть, а в 63% случаев контроль над инфраструктурой мог получить даже малоквалифицированный нарушитель [1]. Одним из основных этапов таких проверок выступает сканирование сетевой инфраструктуры — процедура, позволяющая обнаружить потенциальные точки входа и оценить уязвимость систем до наступления реальных угроз.

Сканирование сети представляет собой процесс сбора сведений о её структуре, устройствах, открытых портах, активных сервисах, а также потенциальных уязвимостях. Такой анализ используется как в рамках легитимных действий (например, при проведении пентестов или внутреннего аудита безопасности), так и при подготовке к несанкционированным атакам. Несмотря на разницу в целях, сам процесс сканирования с технической точки зрения остаётся идентичным и базируется на использовании специальных программных средств и сетевых протоколов.

Среди основных подходов к сканированию выделяют активный и пассивный методы. Активное сканирование предполагает непосредственное взаимодействие с целевыми хостами: отправляются пакеты, анализируются отклики, строится карта сетевого окружения. Это позволяет получить достоверную информацию о конфигурации инфраструктуры, но сопровождается рисками — та-

кие действия могут быть замечены средствами мониторинга или нарушить работу системы. Пассивное сканирование, напротив, осуществляется за счёт анализа уже имеющегося сетевого трафика и логов, без отправки запросов. Оно менее заметно, но и менее информативно, поскольку зависит от объёма и характера доступных данных.

Технический инструментарий сетевого сканирования обширен. Так, одним из базовых методов является ping-сканирование, с помощью которого можно определить, какие хосты в сети являются активными. Ping-сканирование — это метод, основанный на отправке ICMP Echo-запросов (ping) и анализе ответов, чтобы определить, какие хосты активны и доступны для связи. Однако эффективность такого подхода ограничена, поскольку во многих корпоративных и защищённых сетях пакеты ICMP блокируются. На следующем этапе обычно производится сканирование портов, которое позволяет определить, какие службы и протоколы активны на целевых устройствах. Наиболее популярными техниками здесь являются TCP SYN и TCP CONNECT. Первый метод позволяет выявить открытые порты, не устанавливая полноценного соединения, что снижает вероятность обнаружения. Второй метод, наоборот, использует стандартную схему установления соединения и поэтому легче фиксируется средствами защиты. UDP-сканирование также используется, однако в связи со спецификой протокола требует дополнительной обработки и повторов.

В некоторых случаях применяются более изощрённые методы, такие как ACK-сканирование (позволяющее выявить правила фильтрации фаерволов), а также NULL, FIN и Xmas-сканирование, основанные на отправке нестандартных TCP-пакетов. Особое место занимает так называемое зомби-сканирование, при котором злоумышленник использует сторонний хост (зомби), чтобы скрыть истинный источник запроса.

У специалиста по информационной безопасности присутствует целый ряд программных решений, предназначенных для выполнения сканирования. Наиболее известным и универсальным инструментом считается Nmap. Он позволяет производить широкомасштабное сканирование портов, определять версии сервисов, типы операционных систем, а также запускать скрипты для автоматизированного поиска уязвимостей через модуль NSE (Nmap Scripting Engine). Альтернативой Nmap в части высокоскоростного сканирования является Masscan, способный обрабатывать миллионы IP-адресов в короткий промежуток времени, хотя его функциональность ограничивается только идентификацией открытых портов.

Более глубокий анализ уязвимостей осуществляется с помощью инструментов, таких как Nessus и OpenVAS. Nessus — это коммерческий сканер, предоставляющий подробные отчёты о найденных уязвимостях и рекомендации по их устранению. OpenVAS является его бесплатным аналогом с открытым исходным кодом, однако уступает по скорости и объёму базы данных.

Для анализа сетевого трафика и диагностики сетевых инцидентов применяется инструмент Wireshark. С его помощью можно перехватывать и анализировать пакеты, что особенно полезно при расследовании атак или выявлении

аномалий в сети. Для тестирования веб-приложений и серверов используются специализированные утилиты, такие как Nikto, OWASP ZAP и другие, способные обнаруживать ошибки конфигурации, SQL-инъекции и иные типы уязвимостей.

Современные тенденции в сфере сканирования направлены на интеграцию с более комплексными системами информационной безопасности. Так, внедрение искусственного интеллекта и алгоритмов машинного обучения позволяет предсказывать потенциальные векторы атак, анализируя поведение систем на основе исторических данных. Примером может служить решение Darktrace, которое сочетает в себе возможности анализа сетевого трафика, машинного обучения и интеграции с инструментами сканирования, такими как Nmap и Nessus. Благодаря этому становится возможным автоматическое выявление сложных многокомпонентных атак на ранних стадиях.

Кроме того, всё большую популярность приобретают облачные решения, позволяющие выполнять сканирование распределённых сетей без необходимости развёртывания локальной инфраструктуры. Они обеспечивают централизованное управление, автоматические обновления баз уязвимостей и масштабируемость, что делает их особенно удобными для организаций с гибридной или удалённой архитектурой.

Важно подчеркнуть, что проведение сканирования сетевой инфраструктуры, особенно в рамках внешнего анализа, должно соответствовать действующему законодательству. В России несанкционированное вмешательство в работу информационных систем квалифицируется в соответствии со статьями 272 [2], 273 [3] и 274 [4] Уголовного кодекса. Поэтому легитимное сканирование возможно только при наличии письменного разрешения от владельца системы, либо в рамках заключённого договора с внешним исполнителем. Нарушение этих требований может повлечь за собой ответственность.

Вывод

Таким образом, сканирование сетевой инфраструктуры представляет собой неотъемлемую часть работы по обеспечению информационной безопасности. Этот процесс позволяет не только выявить и устранить уязвимости, но и сформировать стратегию проактивной защиты корпоративных ресурсов. В сочетании с современными технологиями анализа и при соблюдении правовых норм сканирование становится мощным инструментом в борьбе с киберугрозами.

Список источников

1. Результаты пентестов за 2023 год: основные уязвимости и методы атак // Хакер: сайт. URL: <https://hacker.ru/2024/07/03/pt-pentests-results/> (дата обращения: 03.04.2025).
2. УК РФ. Статья 272. Неправомерный доступ к компьютерной информации.
3. УК РФ. Статья 273. Создание, использование и распространение вредоносных компьютерных программ.

4. УК РФ. Статья 274. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.

Статья поступила в редакцию 19.04.2025; принята к публикации 10.05.2025

Информация об авторе

Янченко Е.Н. - студент кафедры «Системы информационной безопасности», направление подготовки 10.05.03 - Информационная безопасность автоматизированных систем ФГБОУ ВО «БГТУ».

СЕКЦИЯ 5. ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ

Научная статья

УДК 003:26

Шифрование изображений: особенности и рекомендации

Алексей Григорьевич Белоусов

Брянский государственный технический университет, Брянск, Россия

belousov-ag@yandex.ru, <http://orcid.org/0009-0001-2873-4239>

Аннотация. Обсуждается специфика шифрования изображений по сравнению с другими форматами данных. Рассматриваются методы оценки качества алгоритмов шифрования изображений. Затрагиваются вопросы применения гаммирования для шифрования изображений, а также распараллеливания алгоритмов шифрования изображений.

Ключевые слова: шифрование изображений, гаммирование, псевдослучайный генератор, метод «хи-квадрат», параллельные вычисления.

Для цитирования: Белоусов А.Г. Шифрование изображений: особенности и рекомендации // Актуальные проблемы кибербезопасности. Противодействие экстремизму и терроризму в информационной молодежной среде: сборник докладов I межрегиональной научно-практической конференции. – Брянск: БГТУ, 2025. – С. 259 – 265.

Актуальность. Значительная часть данных, которыми оперируют в информационных системах, хранится и передается в виде изображений. Часто изображения содержат и персональные данные – например, речь идет о фотографиях человека или его документов. Размах приобрела практика шантажа разглашением фотографий, особенно «очень личного» характера. Чтобы персональные данные человека и подробности жизни не попали в руки посторонним, требуется уделять внимание защите данных, в том числе криптографической. К сожалению, даже на уровне компаний, а не рядовых граждан, вопросы защиты персональных и иных важных данных проработаны крайне плохо: по данным компании InfoWatch за 2023 г. из российских компаний утекло примерно 1,2 млрд. записей персональных данных, за 2024 г. – почти 1,6 млрд [5]. О каждом из нас в среднем 8-10 раз за год утекают персональные данные.

Вопрос шифрования изображений шире, чем кажется: видео можно рассматривать как серию изображений, поэтому, кроме обмена файлами изображений, речь может идти о защите данных в видеоконференцсвязи [2].

Специфика шифрования изображений. Изображения, как правило, характеризуются большим объемом: можно встретить камеры в 45, 60 или даже 100 Мп. Хорошая идея – предварительное сжатие [3], но 1) возможности алгоритмов сжатия ограниченные; 2) в некоторых сферах, например, телемедицине, нужна точность изображений [2], что отсекает сжатие с потерями. Некоторые ученые предлагают для изображений даже специальные методы шифрования [3]. Однако, на наш взгляд, есть смысл прорабатывать и вопросы, как адаптировать

шифры общего назначения: если в системе с разными форматами данных на каждый формат предлагать свой шифр, такая система тяжело конфигурируется и модифицируется.

Изображения могут иметь большие однородные или почти однородные области. В наибольшей степени это отмечают теоретики стеганографии, поскольку однородные области снижают надежность внедрения данных в изображение, но и в криптографии это важная особенность. Из нее следует, что блочные шифры в режиме электронной кодовой книги (ЕСВ) дадут ту же проблему, что и классические шифры простой замены или биграммные шифры на текстах: не маскируются в должной мере статистические свойства данных. AES, Blowfish и т.д. в ЕСВ – те же шифры простой замены, но в роли алфавита – множество значений в группе байт, а не для отдельных байт или символов. При хранении не в формате BMP, проблема останется – одинаковые фрагменты будут кодироваться одинаково.

По статистическим свойствам, лучше блочные шифры в режиме сцепления блоков (СВС). Но обратим внимание на формулу режима: если IV – вектор инициализации, P_i – i -й блок данных, C_i – i -й блок шифровки, E_k – шифрование базовым алгоритмом (AES, Blowfish и т.д.) с ключом k , то

$$C_i = \begin{cases} IV, i = 0 \\ E_k(P_i \text{ XOR } C_{i-1}), i = 1, 2, 3, \dots \end{cases}$$

СВС снизит скорость по сравнению с ЕСВ (операций больше), а также не даст такого же простого пути к распараллеливанию, как ЕСВ.

Гаммирование изображений. Разумно утверждать, что шифрование изображений – отличная сфера приложения для гаммирования. Здесь мы имеем следующие преимущества: 1) можно балансировать между скоростью и защищенностью, учитывая, что нам важнее, поскольку мы можем выбирать генератор псевдослучайных чисел (ГПСЧ); 2) большее удобство для передачи в реальном времени, нежели через блочные шифры – чтобы зашифровать передаваемые данные в блочном шифре, нужно ждать готовность целого блока к передаче; 3) возможность сгенерировать гамму заранее в ОЗУ; 4) модифицируемость – например, если использовать объектно-ориентированное программирование и механизм наследования, на верхних уровнях абстракции криптосистема вообще не изменится при смене ГПСЧ, достаточно лишь добавить новый класс ГПСЧ; 5) отсутствие распространения ошибки при замене отдельного байта шифровки (в случае AES, к примеру, в этом случае неправильно расшифруются 16 байт). Можно заметить, что блочный шифр в режиме обратной связи по выходу (OFB) – также гаммирование, но со специфическим способом выработки гаммы. По сути, это уже поточный шифр, но блочные шифры часто требуют много операций на фоне большинства ГПСЧ, по скорости OFB не выглядит обещающим подходом. Если же говорить о выборе традиционного ГПСЧ, требуется высокий период и хорошие статистические свойства – на изображении плохие свойства ГПСЧ проявятся гораздо лучше, чем на тексте: статистические закономерности тем заметнее, чем больше данных.

Заметим, что гаммирование имеет и существенную проблему – высокие требования к знанию математики разработчиком. При малейших неправильных рассуждениях о выборе ГПСЧ, можно существенно ослабить криптосистему. При этом, хорошие ГПСЧ, наподобие BBS, или грамотно настроенного генератора Фибоначчи, также требуют хороших оптимизаторских навыков, иначе их реализация будет работать медленно.

Оценка качества шифрования изображений. Шифровка изображения не несет никакой информации для криптоаналитика, если она близка к хаотичному набору пикселей, т.е. алгоритм преобразования хорошо имитирует случайную генерацию. Рассмотрим пример «от обратного»: что такое плохой шифр. Для демонстрации возьмем гаммирование и заведомо слабый ГПСЧ: генератор фон Неймана, рассматривая пиксель в RGB как 24-битное число. Будем возводить каждый член ряда в квадрат и брать 24 средних бита – так получаем новый член. Если обозначить i -й член как X_i ($i=0$ – опорное значение), то $X_{i+1} = \left[X_i^2 / 2^{12} \right] \bmod 2^{24}$ (скобки – целая часть). Если член ряда 0, 1 или совпадает с предыдущим, снова переходим к опорному значению. При опорном значении 10021 получим период 1322. На рис. 1 показано, что будет при гаммировании с помощью такого ГПСЧ, на конкретном примере (рис. 1А заимствован из сети Интернет). В качестве гаммируемой последовательности байт – пиксели в формате RGB слева направо сверху вниз (по 3 байта на пиксель). На рис. 1Б можно заметить, что шифровка совершенно не похожа на случайную – видно много наклонных полос. На рис. 1В обведено место, где устойчивая структура шифровки разрушается. И это там, где часть лица и волос девушки. Опытный криптоаналитик быстро поймет, что на фото есть большие однородные области, и что есть какой-то объект, не вполне однородный по цветам. Можно возразить: все еще неясно, что зашифровано фото девушки, и тем более – какой конкретно. Однако проблема в том, что это все равно дополнительная информация. По крайней мере, если мы в курсе, что девушка пересылала по сети официальное фото и 4 неформальных, оценка вероятности того, что на рис. 1Б шифровка именно официального фото, уже выше 1/5, ввиду как раз однородного фона.

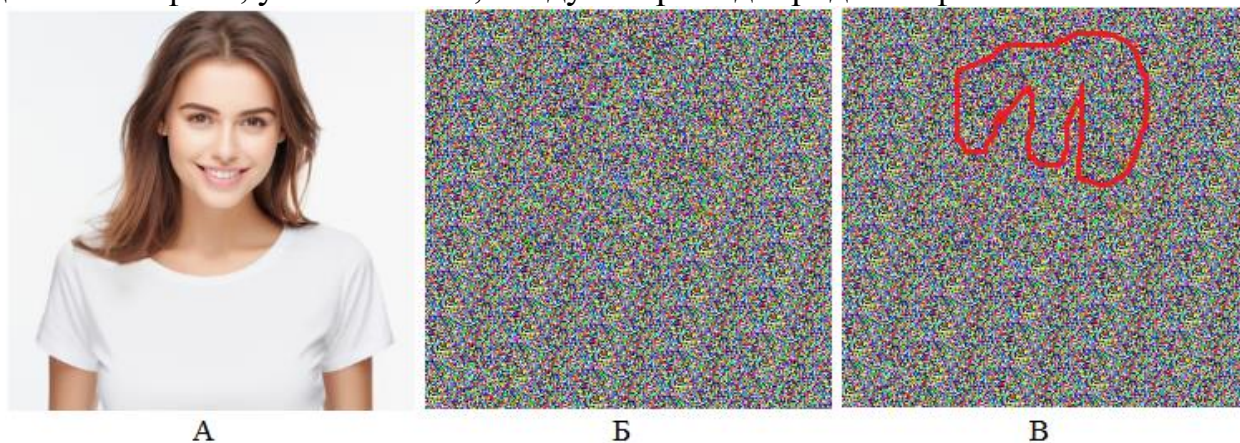


Рис. 1. Пример некачественного шифрования изображения. Результат

На рис. 2А – результат при взятии другого ГПСЧ: генератора Фибоначчи с лагами 17 и 5, опорные значения порождаются линейным генератором как $X_0 = 2$, $X_{i+1} = (5X_i + 3) \bmod 2^{24}$.

Рис. 2Б: сверху – график частот шифровки по красной составляющей для шифровки по фон Нейману, снизу – по Фибоначчи. 2В – аналогично для зеленой составляющей. Новый ГПСЧ также не вполне надежный, но видно, что его свойства лучше – на графиках нет такого резкого разброса значений.

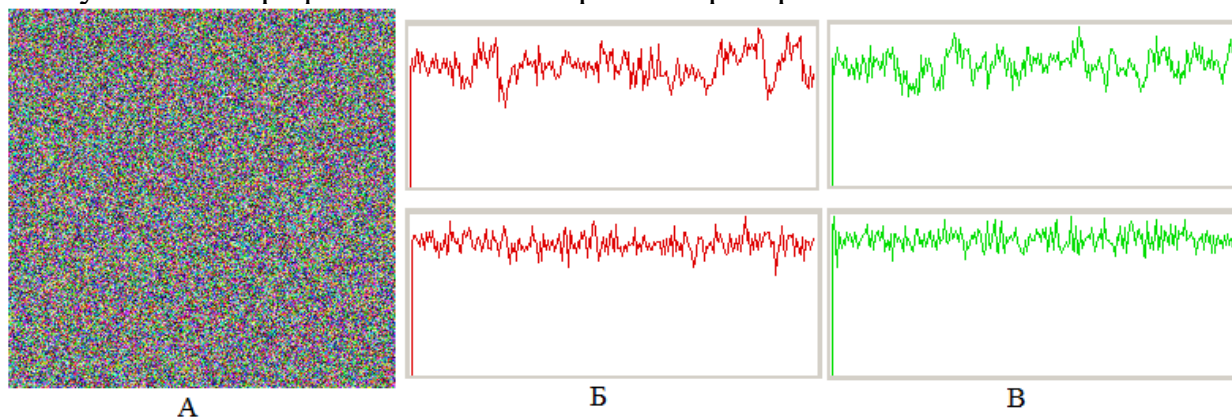


Рис. 2. Шифрование с другим ГПСЧ. Сравнение качества

Важно заметить, что 1) не всегда отсутствие визуальных признаков плохой шифровки означает, что алгоритм удачный, скорее, визуальный анализ – способ исключить откровенно слабые криптосистемы; 2) ЭВМ не анализируют «на глаз». Поэтому нужно использовать различные статистические тесты для ГПСЧ, начиная от частотного теста «хи-квадрат» на равномерность распределения дискретной величины и заканчивая более строгими тестами [1]. Требуется и задействовать тесты с учетом совместного расположения пикселей, т.е. строить уже таблицы сопряженности: возможны ситуации, когда значения R, G, B распределены более-менее равномерно в смысле частот (простейший «хи-квадрат» пройден), но по одному или нескольким окружающим пикселям можно с высокими шансами предположить, какой цвет имеет заданный пиксель. Статистические тесты помогают найти неочевидные слабости метода шифрования изображений и хорошо автоматизируются. Разработчики систем шифрования изображений должны «прогонять» алгоритмы на статистические свойства шифровок. Мы выше привели пример, зачем нужна математическая статистика при анализе качества шифрования: гаммирование с ГПСЧ на рис. 2А не дало серию полос или еще каких-то структур, однако лаги 17 и 5 – не для криптографических применений генератора Фибоначчи (они малы), и метод для начальных значений – линейный генератор – статистически плох. Заметим, что статистические тесты нужно проходить для любых шифров, не только гаммирования.

Распараллеливание шифрования изображений. В наше время ПК и ноутбуки с 4, 6, 8, 12, 16 ядрами процессора – норма, и вопрос о распараллеливании естественный при шифровании больших файлов. Изображение должно представляться в виде некой структуры, которую можно обработать независимо по ча-

стям [3]. Рассмотрим вариант, как можно распараллелить гаммирование растровых изображений, представленных в ОЗУ матрицей пикселей. Цветовая матрица – общая область памяти для всех потоков, само наложение гаммы распараллеливать рискованно. Однако можно распараллелить генерацию, сохраняя часть гаммы, сгенерированную потоком для полосы изображения, в зубчатой матрице – рис. 3 (зубчатой – поскольку не всегда можно распределить работу равномерно).

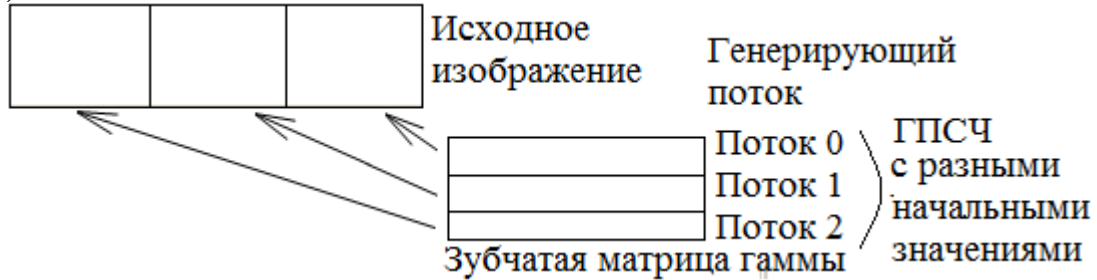


Рис. 3. Принцип многопоточной генерации гаммы

Как правило, ГПСЧ основаны на рекуррентных соотношениях, но если брать ГПСЧ наподобие BBS, где нужно лишь одно начальное значение, а остальные параметры обычно устойчивы, можно запускать разные потоки с разными начальными значениями, формула которых зависит от номера потока, например, как $X_0 + sk$, где s – дополнительный параметр, k – номер потока и полосы, в случае BBS. При таком подходе расшифровщик должен выбрать то же число потоков, что при шифровании. Мы также повысили уровень защиты – увеличилась мощность множества ключей за счет формулы начального значения по номеру потока. Если злоумышленник поймет, как восстановить одну из полос, не гарантия, что он восстановит и остальные. В случае хорошего ГПСЧ и подходящей формулы, статистические свойства гаммы не ухудшатся по сравнению с последовательной генерацией. При затруднении с оценкой влияния формул наподобие выше указанной, на статистику гаммы, при фиксированном числе потоков можно просто задать свое начальное значение в каждом потоке как отдельный ключ, хотя это усложнит администрирование криптосистемы.

Пример хорошей стратегии шифрования изображений. Рассмотрим, как можно реализовать шифрование изображений, эффективное в смысле соотношения скорости и надежности. Наша стратегия не вполне подходит для многопоточности, но быстрая сама по себе. При правильной настройке, генератор Фибоначчи является рациональным при гаммировании, за счет следующих факторов. 1. Высокая скорость за счет того, что нет умножения больших чисел. Умножение больших чисел – дорогостоящая операция: для случая двух чисел с N разрядами лучшие алгоритмы требуют $O(N \log N)$ времени, а сложение – только $O(N)$. 2. Большой период – в случае работы с n -битными числами и правильно выбранных лагов a, b ($a > b$), формула периода $2^n(2^a - 1)$. Для сопоставления: линейный генератор имеет период до 2^n . 3. Хорошие статистические свойства генератора. Единственная проблема – некоторое их ухудшение, когда оказывается, что k -й

член последовательности близок к (k-a)-му или (k-b)-му. Проблему можно решить, если выбрать в роли лагов не (55, 24), которые обычно предлагают в литературе, а гораздо выше. Вполне надежный вариант – (607, 273) [4].

При этом, генератор Фибоначчи вполне можно применить и для любого числа бит, кратного 8, а не только для 24, то есть одно число гаммы может приходиться на любое число байт.

Требуется решить две проблемы – выбор стартового ГПСЧ (для получения a первых значений) и рациональная реализация рекуррентного соотношения. Если стартовая серия имеет плохие статистические свойства, то генератор Фибоначчи теряет смысл, поэтому в первой ступени есть смысл взять BBS. Хотя это медленный ГПСЧ ввиду умножения больших чисел, для гаммирования больших файлов первая ступень имеет малый удельный вес.

Время получения очередного члена с помощью генератора Фибоначчи не будет зависеть от a , если использовать линейный связный список, запоминая указатели на голову, хвост и узел, соответствующий значению $a-b$ шагов назад. Новый член вставляется в один конец списка, самый старый из имевшихся удаляется из другого конца, и обновляются все три указателя.

Классический путь использования генератора Фибоначчи: получить целые псевдослучайные стартовые числа, преобразовать их в вещественные на промежутке $[0; 1)$, обычно делением на модуль M стартового генератора, далее применить формулу:

$$X_k = \begin{cases} X_{k-a} - X_{k-b}, & X_{k-a} \geq X_{k-b} \\ X_{k-a} - X_{k-b} + 1, & X_{k-a} < X_{k-b} \end{cases}.$$

Далее результат снова умножается на M . Но можно сделать иначе, и без ухудшения качества – минуем деления и умножения, напрямую используя генератор для целых чисел, введя формулу для случая модуля M :

$$X_k = \begin{cases} X_{k-a} - X_{k-b}, & X_{k-a} \geq X_{k-b} \\ X_{k-a} - X_{k-b} + M, & X_{k-a} < X_{k-b} \end{cases}.$$

Модуль генератора BBS в идеале должен быть тем же, что модуль генератора Фибоначчи, иначе немного усложнится реализация формирования списка стартовых значений.

Можно почти неограниченно наращивать надежность полученного генератора без ущерба скорости – например, увеличивать лаги или вместо записи всех BBS-значений в список стартовых, пропускать некоторые по определенным правилам (например, из каждых 15 значений пропускать 10-е и 15-е, т.е. записывать только 13 чисел в список). Битовая маска, определяющая порядок пропуска, – также дополнительный ключ.

Выводы. Для шифрования изображений, по сравнению с шифрованием текстов, гораздо более важны как скорость, так и статистические свойства. Некоторые традиционные шифры, особенно блочные, плохо адаптируются к изображениям, но хорошим вариантом являются поточные шифры, особенно гаммирование. При правильном выборе ГПСЧ, можно гаммировать изображения

быстро и без ущерба криптостойкости. При выборе ГПСЧ важно экспериментально исследовать статистические свойства ГПСЧ, а также уделять внимание оптимизации исходного кода. Возможен широкий спектр приемов оптимизации шифрования изображений – заблаговременная генерация многократно используемых данных в ОЗУ (как вариант, гаммы), правильный выбор структур данных, распараллеливание шифрования, минимизация умножения больших чисел и других дорогостоящих операций. При этом, необходимо правильное мышление программиста – оптимизация алгоритмов шифрования выполняется далеко не так же, как улучшение классических алгоритмов сортировки, конвертации и поиска данных.

Список источников

1. Белоусов А.Г., Мысютин А.П. Псевдослучайные величины и генераторы: иллюзия случайности // Фундаментальные и прикладные научные исследования: актуальные вопросы, достижения и инновации: сборник статей XI международной научно-практической конференции. В 3 ч. Ч. 1. – Пенза: МЦНС «Наука и просвещение», 2018. С. 21-25.
2. Подходы к квантовому шифрованию изображений. 2021. URL: <https://habr.com/ru/articles/594955/>.
3. Сидоренко А.В., Шишко М.С. Шифрование изображений на основе хаотических отображений с использованием параллельных вычислений // Информатика. 2017. № 4. С. 78-88.
4. Слеповичев И.И. Генераторы псевдослучайных чисел. – Саратов: СГУ, 2017. – 118 с.
5. Утечки информации в России: отчет за прошедший год. 2025. URL: <https://www.infowatch.ru/company/presscenter/news/kolichestvo-slitykh-personalnykh-dannykh-v-dve-tysyachi-dvadtsat-chetvertom-godu-vyroslo-na-tret>.

Статья поступила в редакцию 19.04.2025; принята к публикации 10.05.2025

Информация об авторе

Белоусов А.Г. – к.т.н., доцент кафедры «Высшая математика» ФГБОУ ВО «БГТУ».

Научная статья

УДК 004.056.55

Особенности IP-камер и перспективы их развития

Максим Дмитриевич Грива¹✉, Михаил Юрьевич Рытов²

^{1,2}Брянский государственный технический университет, Брянск, Россия

¹ maks.griva.04@mail.ru ✉

² ozikts@yandex.ru

Аннотация. IP-камеры состоят из объектива, ИК-фильтра, матрицы, процессора обработки изображения и центрального процессора, соединённых сетевым интерфейсом. Они отличаются от аналоговых способностью самостоятельной обработки видеопотоков и поддержкой технологии POE. Дополнительные модули, такие как микрофоны и динамики, расширяют функциональность. Современные тенденции включают развитие машинного зрения, AR-технологий и искусственного интеллекта, что повышает эффективность и точность видеонаблюдения.

Ключевые слова: ip- камера, видеонаблюдение, искусственный интеллект.

Для цитирования: Грива М.Д., Рытов М.Ю. Особенности IP-камер и перспективы их развития // Актуальные проблемы кибербезопасности. Противодействие экстремизму и терроризму в информационной молодежной среде: сборник докладов I межрегиональной научно-практической конференции. – Брянск: БГТУ, 2025. – С. 266 – 268.

Своим строением ip- камера достаточно проста. Она представляет из себя несколько элементов благодаря которым выполняются функции видеонаблюдения, обработки и отправки видеоданных. Следует выделить следующие конструктивные элементы, такие как: объектив — оптическая система, фокусирующая световые лучи на светочувствительной матрице. Объективы могут иметь фиксированное или переменное фокусное расстояние (вариофокальные), что позволяет настраивать угол обзора и масштабирование сцены. ИК-фильтр — располагается между объективом и матрицей и служит для отсеечения инфракрасного излучения, которое может искажать цвета изображения днем. Ночью этот фильтр может автоматически отключаться, чтобы улучшить чувствительность камеры в условиях низкой освещенности. Светочувствительная матрица — основной элемент, преобразующий свет в электрический сигнал. Матрицы бывают различных типов, включая CMOS и CCD. Процессор обработки изображения (ISP) — специализированный чип, отвечающий за обработку сигнала, поступающего с матрицы. ISP управляет параметрами изображения, такими как яркость, контрастность, насыщенность цветов, шумоподавление и другие характеристики. Современные процессоры также поддерживают функции видеоаналитики, такие как распознавание лиц, отслеживание объектов и обнаружение движения. Центральный процессор (CPU) — основное вычислительное ядро камеры, выполняющее широкий спектр функций. Помимо обработки изображений, CPU может отвечать за работу встроенного веб-сервера, поддержку протокола RTSP для передачи видеопотока, управление механическими функциями

камеры (панорамирование, наклон, зум) и выполнение других интеллектуальных задач. Сетевой интерфейс — модуль, обеспечивающий подключение камеры к сети. Обычно это порт Ethernet (RJ45), поддерживающий протоколы TCP/IP и стандарт PoE (Power over Ethernet), позволяющий подавать питание через тот же кабель, что и данные.

Следуя строению ip- камеры можно говорить, о её принципиальном отличии от аналоговых камер, где данные видеопотока только получаются камерой, а обрабатываются на другом устройстве. Ключевым преимуществом ip- камер становится возможность обработки информации непосредственно в камере, без необходимости использовать большие мощности на едином сервере с камерами. Также, преимуществом ip- камер является частое использование технологии POE. Технология POE (Power of Ethernet) – это технология позволяющая передавать электрический ток и напряжение, для питания устройства, в сетевом кабеле. Нередкостью является использование дополнительных модулей для взаимодействия камеры с окружающей средой, например: микрофон, с возможностью записи аудиопотока вокруг камеры; динамик, для взаимодействия между лицом управляющим камерой и окружающими устройством объектами; модуль подсветки.

Исследуя современные тенденции развития электронных устройств, можно утверждать о следующих векторах развития технологий ip- камер:

Машинное зрение- внедрение современных AR- технологий позволит пересмотреть стандартный взгляд на системы видеонаблюдения. Возможность снимать и сразу моделировать 3D- объект позволит развить применение камер в системах защиты для улучшения процесса идентификации объектов – городские системы видеонаблюдения смогут эффективней распознавать злоумышленников, а камеры на производствах распознавать авторизованных пользователей.

Развитие технологий процессоров, матриц и сетевых интерфейсов позволит улучшить качество видеопотоковой информации, увеличить скорость обработки и передачи данных пользователю. Крайне перспективным является создание видеокамер с использованием технологий топологических процессоров, хотя на данный момент они являются сверхдорогими, но в ближайшие 10-20 лет все устройства начнут использовать их.

Повсеместное использование искусственного интеллекта также отражается и в системах видеонаблюдения. Уже можно говорить об его использовании для улучшения качества видеозаписи, отслеживания объектов и их идентификации.

В заключении следует сказать, что технология ip- камер является достаточно простой, в общих чертах, но является крайне перспективной для развития, о чём говорит факт её использования во всех сферах жизни – от бытовой до производственной.

Список источников

1. Михайлов Ю.М. Конструктивное исполнение и принципы работы цифровых видеокамер / Ю.М. Михайлов // Радиопромышленность. 2022. № 3. С. 15–22.
2. Быков Л.Е. Архитектурные особенности и эволюция сетевого оборудования для видеонаблюдения // Информационная безопасность. 2023. № 1. С. 38–45.
3. Семёнов К.Р. Современные тенденции развития сетей видеонаблюдения и обработки видеоинформации // Телекоммуникации и информационные технологии. 2022. № 2. С. 56–63.
4. Иванов С.Л. Эволюция систем видеонаблюдения: история, настоящее и будущее. — Москва : Техносфера, 2021. — 256 с.
5. Соколов А.Б. Использование IP-камер и развитие стандартов передачи видеоданных // Журнал сетевых решений LAN. 2023. № 4. С. 28–35.

Статья поступила в редакцию 23.04.2025; принята к публикации 10.05.2025

Информация об авторах

Грива М.Д. - студент кафедры «Системы информационной безопасности», направление подготовки 10.03.01 – Организация защиты информации ФГБОУ ВО «БГТУ».

Рытов М.Ю. – д.т.н., профессор кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Вклад авторов

Грива М.Д. - идея, сбор материала, обработка материала, частичное написание статьи (50%).

Рытов М.Ю. - написание статьи, научное редактирование текста (50%).

Конфликт интересов отсутствует.

Научная статья
УДК 004.056.55

Принцип слежения, используемый IP-камерами

Максим Дмитриевич Грива¹✉, Михаил Юрьевич Рытов²

^{1,2}Брянский государственный технический университет, Брянск, Россия

¹maks.griva.04@mail.ru ✉

²ozikts@yandex.ru

Аннотация. Статья посвящена принципу работы систем слежения, используемых современными IP-камерами. Рассматриваются основы технологии, начиная с этапа детекции движения и заканчивая процессом автоматического сопровождения объектов. Описаны ключевые компоненты, необходимые для успешной реализации данной функции, такие как высокочувствительные сенсоры, оптические модули и мощные микропроцессорные ресурсы. Особое внимание уделено практическим аспектам применения, включающим защиту жилых помещений, общественных пространств и промышленных объектов. Статья акцентирует внимание на преимуществах автоматизации процесса видеонаблюдения, подчеркивая повышение надежности, скорости реагирования и снижение нагрузки на персонал служб безопасности. Приведены технические характеристики, влияющие на производительность систем слежения, а также описаны возможные сферы применения IP-камер с такими функциями.

Ключевые слова: IP- камера, видеонаблюдение, системы слежения.

Для цитирования: Грива М.Д., Рытов М.Ю. Принцип слежения, используемый IP-камерами // Актуальные проблемы кибербезопасности. Противодействие экстремизму и терроризму в информационной молодежной среде: сборник докладов I межрегиональной научно-практической конференции. – Брянск: БГТУ, 2025. – С. 269 – 272.

IP-камеры представляют собой современное решение для организации эффективных систем видеонаблюдения, отличающееся высоким качеством изображения и широким спектром функциональных возможностей. Среди множества технологий, применяемых в IP-камерах, одной из наиболее востребованных является система автоматического слежения за объектами наблюдения. Давайте рассмотрим подробно этот принцип и механизмы его реализации.

Система слежения - это механизм автоматической фиксации и сопровождения объектов, находящихся в зоне видимости видеокамеры. Благодаря таким технологиям, камера способна самостоятельно следить за движением предметов или людей, поддерживая их в центре кадра независимо от направления перемещения. Данная функция существенно улучшает эффективность охранных мероприятий и упрощает работу операторов, минимизируя необходимость постоянного вмешательства человека.

Для понимания принципов функционирования слежения важно рассмотреть ключевые элементы технологии:

1. Детекция движения

Первый этап процесса слежения начинается с выявления активности в кадре. Камера оснащена специальными алгоритмами, способными обнаруживать изменение положения объектов относительно фона. Такой метод основан на сравнении кадров видеосигнала и анализе возникающих различий, связанных с перемещением предметов. Алгоритм способен выделять области, в которых зафиксировано движение, отделяя их от статичных элементов сцены.

2. Распознавание и идентификация объектов

Следующий важный шаг — определение типа объекта, зафиксированного камерой. Современные решения используют интеллектуальные методы компьютерного зрения, такие как распознавание лиц, номеров автомобилей или характерных признаков телосложения человека. Эта информация необходима для принятия решений о дальнейшем сопровождении конкретного объекта.

3. Автоматическое сопровождение

Когда цель определена, включается механизм автоматического сопровождения. Для этого используются электромеханические приводы (например, серводвигатели), позволяющие оперативно менять положение объектива камеры, следуя за направлением движения объекта. Таким образом, IP-камера постоянно поддерживает заданный предмет в центральной части кадра, обеспечивая наилучшую видимость и детализацию изображения.

4. Предсказательная аналитика

Дополнительные улучшения обеспечивают продвинутые алгоритмы машинного обучения, способные анализировать поведение объекта и прогнозировать его дальнейшие шаги. Так, на основании ранее полученных данных о движении, камера заранее готовится к изменению своего положения, оптимально выстраивая кадр для последующей съемки.

Ключевые особенности и преимущества системы слежения

Использование технологии слежения имеет ряд значимых преимуществ перед традиционными методами охраны и видеонаблюдения:

Повышенная надежность и оперативность реагирования: автоматическое отслеживание потенциально опасных ситуаций увеличивает вероятность своевременного предотвращения преступлений или нарушений порядка.

Максимальная детализация происходящего: постоянная фиксация объекта гарантирует получение высококачественного материала, пригодного для последующего изучения и идентификации нарушителей.

Минимизация затрат труда персонала: автоматическая работа камер снижает нагрузку на сотрудников службы безопасности, позволяя сосредоточить внимание на важных аспектах работы.

Эффективность в больших зонах покрытия: наличие механизмов автоматического слежения делает камеру идеальным решением для охраны обширных площадей, включая крупные предприятия, общественные места и транспортные узлы.

Реализация механизма слежения требует наличия ряда технических компонентов и характеристик:

- Высококачественная матрица: чувствительная фотоматрица высокой разрешающей способности позволяет точно определять мелкие детали и реагировать на малейшее перемещение объектов.

- Оптика с быстрым механизмом регулировки: современные линзы оснащаются системой автофокусировки и быстрыми приводами поворотных устройств, что обеспечивает высокую скорость реакции на движение цели.

- Процессор с мощными вычислительными ресурсами: обработка большого объема визуальной информации требует значительных аппаратных ресурсов, именно поэтому IP-камеры оснащаются производительными чипсетами.

- Облачные сервисы и сетевые инфраструктуры: некоторые модели поддерживают удаленное управление и обработку данных на облачных платформах, предоставляя операторам доступ к управлению камерами через веб-интерфейсы и мобильные приложения.

Применение IP-камер с функцией слежения весьма разнообразно:

- Охрана государственных учреждений и офисов: обеспечение безопасности административных зданий и коммерческих организаций.

- Контроль торговых центров и супермаркетов: предотвращение краж и выявление подозрительного поведения посетителей.

- Наблюдение за транспортными узлами: эффективное наблюдение за вокзалами, аэропортами и автобусными станциями.

- Защита частной собственности: использование для защиты загородных участков, гаражей и подъездов многоквартирных домов.

- Отслеживание транспортных потоков: помощь органам правопорядка в мониторинге дорожного движения и предупреждении аварийных ситуаций.

Технология слежения, применяемая в IP-камерах, открывает широкие перспективы для совершенствования систем видеонаблюдения и оптимизации процессов охраны. Возможность автоматического отслеживания объектов в режиме реального времени существенно повышает уровень защищенности и комфорта пользователей, делая систему эффективной как в быту, так и в масштабных промышленных проектах.

Список источников

1. Петров А.В., Сидоров Б.Н. Основы видеонаблюдения // Безопасность бизнеса. 2022. № 5. С. 34–41.
2. Шаров Г.Д. Организация систем видеонаблюдения с использованием IP-технологий : учебник. – М. : Инфра-М, 2023. - 256 с.
3. Бурмистров М.И. Проблемы и пути развития видеонаблюдения на предприятиях малого и среднего бизнеса // Вестник Академии МВД России. 2021. № 3. С. 67–74.
4. Маслов Н.А. Интеллектуальное видеонаблюдение: тенденции и перспективы развития // Инновационные технологии в промышленности и экономике. 2022. № 4. С. 112–120.

5. Лукьянец Е.П. Особенности проектирования IP-камер с функцией слежения // Вопросы техники радиосвязи. 2020. № 1. С. 15–23.
6. Николаев Д.С. Выбор оборудования для построения систем видеонаблюдения // Техника и средства связи. 2021. № 2. С. 32–39.
7. Сергеев П.Г. Современное состояние рынка IP-камер в России // Экономика информационных технологий. 2023. № 1. С. 45–53.

Статья поступила в редакцию 23.04.2025; принята к публикации 10.05.2025

Информация об авторах

Грива М.Д. - студент кафедры «Системы информационной безопасности», направление подготовки 10.03.01 – Организация защиты информации ФГБОУ ВО «БГТУ».

Рытов М.Ю. – д.т.н., профессор кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Вклад авторов

Грива М.Д. - идея, сбор материала, обработка материала, частичное написание статьи (50%).

Рытов М.Ю. - написание статьи, научное редактирование текста (50%).

Конфликт интересов отсутствует.

Научная статья
УДК 004.056.55

Перспективы развития систем видеонаблюдения

Максим Дмитриевич Грива¹✉, Алина Михайловна Шапенская²

^{1,2}Брянский государственный технический университет, Брянск, Россия

¹maks.griva.04@mail.ru ✉

²alinashapenskaya@yandex.ru

Аннотация. В статье рассматриваются актуальные направления и перспективы развития систем видеонаблюдения. Освещаются достижения в повышении качества изображения, расширении функционала, внедрении искусственного интеллекта и аналитических инструментов, распространении беспроводных технологий и взаимодействии с Интернетом вещей (IoT), совершенствовании биометрии и увеличении значимости облачных сервисов. Подчеркивается важность вопросов энергетической эффективности и экологической устойчивости систем видеонаблюдения. Представлены выводы о неизбежности перехода к новым стандартам качества и уровню безопасности, формирующим цифровую среду будущего.

Ключевые слова: ip- камера, видеонаблюдение, перспективы развития.

Для цитирования: Грива М.Д., Шапенская А.М. Перспективы развития систем видеонаблюдения // Актуальные проблемы кибербезопасности. Противодействие экстремизму и терроризму в информационной молодежной среде: сборник докладов I межрегиональной научно-практической конференции. – Брянск: БГТУ, 2025. – С. 273 – 276.

Современные системы видеонаблюдения играют ключевую роль в обеспечении общественной безопасности, защите имущества и контроле производственных процессов. Постоянное развитие технологий открывает новые горизонты для дальнейшего усовершенствования систем видеонаблюдения, делая их более умными, надежными и удобными в эксплуатации.

Одним из главных направлений развития систем видеонаблюдения станет улучшение качества изображения. Прогресс в развитии технологий формирования изображения обеспечит увеличение разрешения камер вплоть до Ultra HD (4K и выше). Высокое разрешение позволит детально рассматривать объекты и события, облегчая идентификацию преступников, учет товаров и контроль технологических процессов.

Кроме того, ожидается дальнейшее развитие технологий стабилизации изображения и компенсации условий освещения, что сделает системы видеонаблюдения полезными даже в сложных погодных условиях или при недостаточной освещённости.

Интеграция новых форматов сжатия данных, таких как H.265+ и HEVC, повысит эффективность хранения записей и передачу видеопотоков по сетям с ограниченной пропускной способностью.

Важнейшим направлением эволюции систем видеонаблюдения является интеграция искусственного интеллекта (ИИ). Сегодня многие производители внедряют различные формы ИИ-анализа в камеры и программное обеспечение

для видеонаблюдения, что позволяет повысить точность и оперативность реагирования на происшествия.

Возможности искусственного интеллекта открывают огромные перспективы:

- Автоматизированное распознавание лиц и автомобильных номеров.
- Отслеживание маршрутов передвижения объектов.
- Быстрое обнаружение аномалий и нестандартных событий.
- Анализ эмоционального состояния и настроений людей.

Всё это способствует повышению точности мониторинга и снижению количества ложных срабатываний сигнализаций.

Искусственный интеллект будет играть важную роль в интеграции систем видеонаблюдения с системами управления предприятиями, учреждениями и городскими инфраструктурами, создавая комплексные решения для повышения общей безопасности и удобства жителей городов.

Системы видеонаблюдения активно интегрируются в экосистему Интернета вещей (IoT). Многие устройства становятся частью единой интеллектуальной среды, взаимодействуя друг с другом и централизованными платформами управления.

Сегодня всё чаще используется Wi-Fi и LTE/5G для подключения камер, что облегчает монтаж и эксплуатацию оборудования. Тем не менее, широкое распространение беспроводных технологий связано с необходимостью обеспечить высокий уровень безопасности и отказоустойчивость сетей.

Кроме того, существует потребность в разработке энергоэффективных протоколов обмена данными, поскольку рост числа подключенных устройств приведет к увеличению потребления энергии.

Биометрия занимает важное место среди будущих направлений развития систем видеонаблюдения. Сейчас наблюдается активное внедрение методов идентификации личности на основе уникальных физиологических характеристик (лица, отпечатков пальцев, голоса).

В будущем подобные системы станут незаменимыми элементами комплексной безопасности:

- Более высокая степень достоверности идентификации, снижающая риск мошенничества.
- Упрощенный доступ к охраняемым зонам и объектам.
- Индивидуализированные права доступа, повышающие общую управляемость безопасностью объектов.

Однако важным вопросом остается защита персональных данных, ведь неправильное хранение и утечка такой информации могут привести к серьезным последствиям.

Рынок видеонаблюдения стремительно движется в сторону облачных технологий. Хранение видеоданных и обработка сигналов на стороне облачной платформы освобождает локальную инфраструктуру от высоких нагрузок и обеспечивает гибкое масштабирование системы.

Будущие разработки позволят сделать облако основным элементом всей архитектуры видеонаблюдения, предлагая пользователям услуги по подписке («videонаблюдение как сервис»). Пользователи получают возможность получать доступ к данным практически из любой точки мира и пользоваться инструментами аналитики без приобретения дорогостоящего оборудования.

Но вместе с развитием облаков возникают риски нарушения конфиденциальности данных, и потому необходимо уделять особое внимание вопросам информационной безопасности и шифрования данных.

Рост популярности систем видеонаблюдения сопровождается повышенным вниманием к экологии и энергосбережению. Производители стремятся минимизировать энергопотребление камер и сопутствующего оборудования путем внедрения инновационных схем питания и режимов сна.

Перспективным направлением является разработка автономных систем видеонаблюдения, работающих на возобновляемых источниках энергии (солнечная энергия, ветряные установки). Такие системы идеально подойдут для труднодоступных районов и отдалённых объектов, где традиционные линии электропередачи отсутствуют или нестабильны.

Также важными аспектами являются выбор материалов для корпусов камер и правильная утилизация устаревшего оборудования, что снизит негативное воздействие на окружающую среду.

Современные системы видеонаблюдения находятся на пороге кардинальных изменений, обусловленных стремительным прогрессом в области компьютерных технологий, искусственного интеллекта и телекоммуникационных сетей. Будущее систем видеонаблюдения тесно связано с повышением их функциональности, надёжности и доступности.

Эти инновации приведут к созданию глобального цифрового окружения, где каждая камера станет активным участником большой распределённой сети, объединённой искусственным интеллектом и технологиями IoT. Важнейшие факторы успеха в данном процессе — развитие технологий, доступность, простота использования и максимальная забота о приватности и безопасности данных пользователей.

Список источников

1. Абрамян А.В. Тенденции развития систем видеонаблюдения // Научно-технический вестник ИТМО. 2022. № 1. С. 45–53.
2. Александров И.К. Искусственный интеллект в системах видеонаблюдения: проблемы и перспективы / И.К. Александров, В.А. Чиркин // Труды международной конференции «Информационно-коммуникационные технологии». — СПб.: Политех-Пресс, 2021. — С. 145–152.
3. Васильев А.Н. Биометрические технологии в системах видеонаблюдения: анализ тенденций и проблем // Вопросы кибербезопасности. 2022. № 3. С. 38–46.

4. Голубев Я.С. Экологичность и энергоэффективность систем видеонаблюдения: критический обзор // Известия вузов. Электроника. 2023. № 2. С. 112–120.

5. Жданова Е.Ю. Применение облачных технологий в системах видеонаблюдения: современный опыт и прогнозы / Е.Ю. Жданова, Д.О. Семенов // Вестник университета имени О.Е. Кутафина. 2022. № 4. С. 154–162.

6. Иванов С.В. Развитие беспроводных технологий и интернета вещей в системах видеонаблюдения // Новые технологии в науке и технике. 2021. № 2. С. 87–95.

Статья поступила в редакцию 23.04.2025; принята к публикации 10.05.2025

Информация об авторах

Грива М.Д. - студент кафедры «Системы информационной безопасности», направление подготовки 10.03.01 – Организация защиты информации ФГБОУ ВО «БГТУ».

Шапенская А.М. – ассистент кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Вклад авторов

Грива М.Д. - идея, сбор материала, обработка материала, частичное написание статьи (50%).

Шапенская А.М. - написание статьи, научное редактирование текста (50%).

Конфликт интересов отсутствует.

Научная статья
УДК 378:004

Разработка систем защиты персональных данных

Максим Викторович Колесников

Брянский государственный технический университет, Брянск, Россия
mkolesnikov@angel-it.ru, <http://orcid.org/0009-0001-8633-0021>

Аннотация. Растущий объём собираемых и обрабатываемых персональных данных влечет за собой увеличение числа инцидентов, связанных с их утечкой, и усложняют обеспечение соответствия информационных систем постоянно меняющимся требованиям законодательства. Для решения этой проблемы разработано программное обеспечение (ПО), автоматизирующее мониторинг и оценку соответствия информационных систем нормам защиты персональных данных. Решение, имеющее клиент-серверную архитектуру, обеспечивает комплексный подход, охватывающий мониторинг безопасности, проверку средств защиты, контроль доступа к веб-ресурсам и анализ работоспособности межсетевых экранов. Уникальной особенностью является возможность расчёта процента защищённости системы с учётом требований законодательства и влияния человеческого фактора, что позволяет организациям оперативно выявлять и устранять уязвимости, повышая доверие граждан и снижая риски утечки информации.

Ключевые слова: персональные данные, эффективность защиты, автоматизация, утечки, защита информации.

Для цитирования: Колесников М.В. Разработка систем защиты персональных данных // Актуальные проблемы кибербезопасности и их решения. Противодействие экстремизму и терроризму в информационной молодежной среде: сборник докладов I межрегиональной научно-практической конференции. – Брянск: БГТУ, 2025. – С. 277 – 282.

В современном мире персональные данные стали ценным активом, требующим особого внимания и защиты. Недостаточная защита персональных данных может привести к серьезным последствиям как для отдельных лиц, так и для организаций, что делает вопрос их безопасности крайне актуальным.

Вопрос защиты персональных данных становится всё более актуальным, поскольку объёмы собираемой и обрабатываемой информации быстро растут. Параллельно с этим наблюдается рост числа инцидентов, связанных с утечками и хищениями персональных данных. Так, по данным Роскомнадзора, за 2024 год было зафиксировано 135 случаев утечки баз данных, в которых содержалось более 710 млн записей о россиянах [1]. Такая динамика подчеркивает необходимость постоянного совершенствования мер безопасности и повышения осведомленности пользователей о рисках, связанных с обработкой и хранением персональных данных.

Настоящее исследование направлено на выявление ключевых факторов, влияющих на эффективность защиты персональных данных в современных условиях. Целью является разработка рекомендаций по повышению уровня защиты

персональных данных с учётом текущих угроз и изменений в нормативно правовых документах. Для достижения поставленной цели были сформулированы следующие задачи:

- провести анализ действующего законодательства в области защиты персональных данных, включая Федеральный закон № 152-ФЗ «О персональных данных» [2] и связанные с ним подзаконные акты;
- проанализировать эффективность существующих методов и технологий защиты персональных данных, использующих организационные, технические и правовые аспекты. Были использованы методы анализа и синтеза для обобщения данных из различных источников, включая нормативные акты, научные публикации и статистические отчёты.

Сравнительный анализ позволил оценить преимущества и недостатки различных методов защиты. В качестве эмпирического материала использованы данные о зарегистрированных утечках персональных данных за последние пять лет, полученные из открытых источников и отчётов регуляторов (Роскомнадзор, ФСТЭК). Анализ данных проводился с использованием статистических методов, а также качественного контент-анализа для выявления тенденций и закономерностей в области утечек и нарушений защиты персональных данных. Ограничениями данного исследования являются:

- доступность данных об утечках, которая может быть ограничена нежеланием компаний раскрывать информацию;
- субъективность оценки эффективности методов защиты, основанная на анализе открытых данных.

Проведено теоретическое и практическое исследование. Источниками теоретического исследования являются нормативные правовые акты Российской Федерации, регулирующие защиту персональных данных, в том числе ФЗ № 152, приказы ФСТЭК России № 17 [3] и № 21 [4], а также работы российских и зарубежных исследователей в области информационной безопасности и права. Эмпирическую базу составили статистические данные об утечках, персональных данных за 2019 – 2024 годы, полученные из отчетов Роскомнадзора [5], аналитических обзоров компаний и публикаций в средствах массовой информации, включая новостные сайты, специализированные издания по информационной безопасности и деловые издания. Сбор и анализ данных проводились с использованием систематизации нормативно правовых актов, анализа научных публикаций, мониторинга открытых источников и статистической обработки данных.

Анализ нормативно правовых документов и динамики утечек персональных данных выявил сложность обеспечения соответствия информационных систем постоянно меняющимся требованиям законодательства в области защиты информации. В связи с этим в рамках данного исследования было разработано ПО, предназначенное для автоматизированного отслеживания соответствия информационных систем нормам законодательства о защите персональных данных, что позволит организациям оперативно реагировать на изменения и снижать риски возникновения инцидентов.

Исследование проводилось на базе ИСПДн «Бухгалтерия и кадры» ООО «АйТиАнгел». Анализ поведения персонала выявил ряд рисков, связанных с человеческим фактором: посещение небезопасных веб-ресурсов, несоблюдение правил безопасности при работе с рабочими станциями и использование ненадежных паролей. Для дальнейшей оценки влияния человеческого фактора на безопасность данных были выбраны следующие критерии: наличие профильного ИТ-образования и возраст сотрудников как потенциальные факторы, влияющие на осведомленность и соблюдение мер безопасности.

Разработанное ПО имеет клиент-серверную архитектуру и состоит из множества клиентов и серверов. Клиентский компонент имеет графический интерфейс и предназначен для мониторинга безопасности рабочей станции, что включает в себя: проверку установленных сертифицированных средств защиты информации; проверку актуальности баз данных антивирусных программ; проверку доступа к запрещенным веб-ресурсам; проверку работоспособности межсетевого экрана и средств предотвращения вторжений; проверку разграничения доступа.

Серверная часть состоит из 2 серверов: сервер синхронизации и сервер проверки. Сервер синхронизации предназначен для: проверки действия лицензии на программный продукт; актуализации дат выпуска баз данных для антивирусного ПО; синхронизации информации. Сервер проверки предназначен для проверки работоспособности межсетевого экрана и средства предотвращения вторжения клиента. При осуществлении проверки эти серверы взаимодействуют.

На рис. 1 изображен обмен информацией 2 видов: информация для синхронизации и запросы для проверки.



Рис. 1. Схема взаимодействия компонентов ПО

Разработанное ПО способно рассчитать процент защищенности информационных систем, учитывая требования законодательства (рис. 2) и человеческий фактор (рис. 3). Дерево принятия решений представлено на рис. 2.

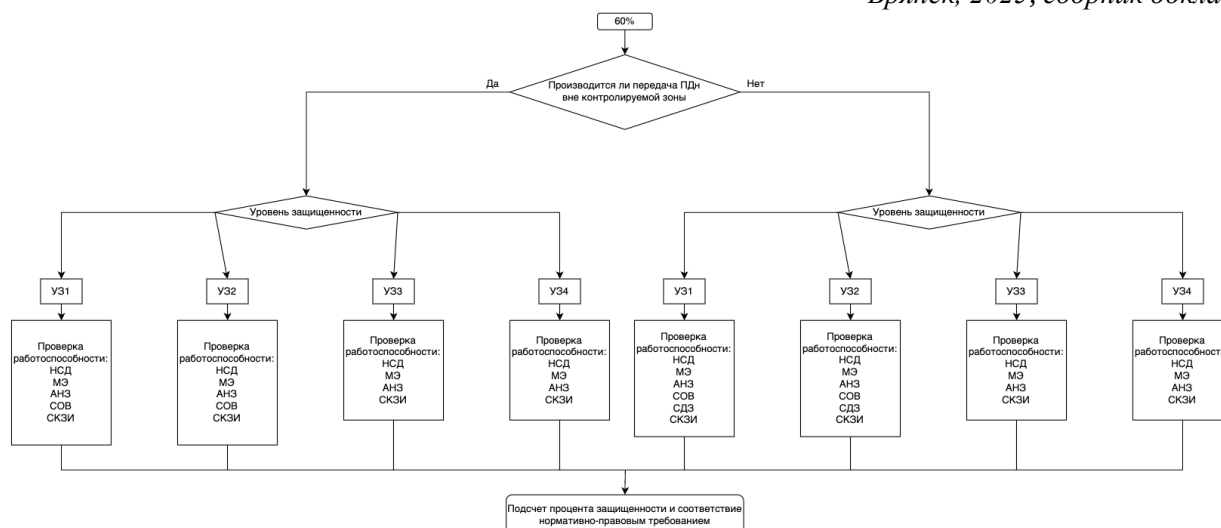


Рис. 2. Дерево принятия решений с учетом требования законодательства

Как видно из рис. 2, для работы ПО необходимо в качестве входного параметра задать уровень защищенности. После этого ПО проверяет наличие средств защиты информации и их работоспособность. В случае если будет отсутствовать критически важное средство защиты информации или оно будет не исправно, то ПО сообщит об этом пользователю.

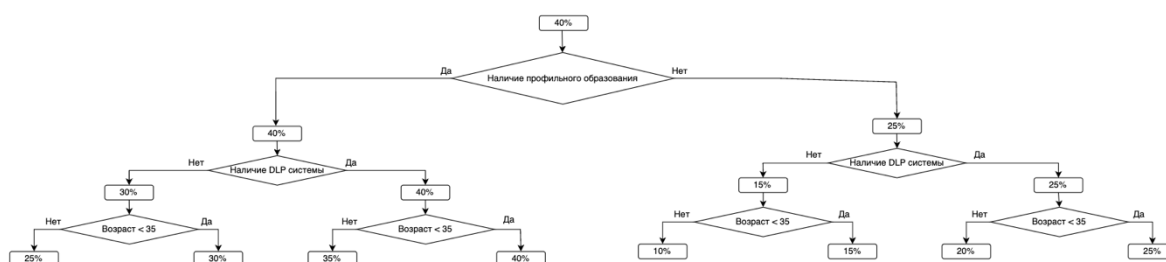


Рис. 3. Дерево принятия решений с учетом человеческого фактора

Для работы модуля, отвечающего за человеческий фактор, в качестве входных параметров необходимо указать наличие образования пользователя и его возраст. После этого основываясь на данных, высчитанных модулем ранее (рис. 2), будет возможно определить на сколько сильно человеческий фактор влияет на работоспособность информационной системы. На рис. 4-5 представлен результат работы ПО.

Установленные СЗИ Проверка АВЗ Запрещенные ресурсы Настройки Оценка

Автоматическая оценка СЗИ: 60
Посещение подозрительных ресурсов: обнаружено

Имя сотрудника: Иванов И.И.

Возраст сотрудника: ☒ 18-29 ☐ 30-50 ☐ больше 50

☐ Используются IDS или IPS системы

Посчитать итоговое значение

Рис. 4. Раздел ПО «Оценка»

Расчет человеческого фактора

Имя сотрудника: Иванов И.И.

Возраст сотрудника: 47

☐ Профильное образование

☐ Наличие DLP-системы

Результат: 10%

Расчет

Рис. 5. Раздел ПО «Расчет человеческого фактора»

Как видно из примера автоматизированное рабочее место сотрудника Иванова И. И. ИСПДн «Бухгалтерия и кадры» ООО «АйТиАнгел» имеет процент защищенности информационных систем равный 60. Это указывает на то, что все средства защиты информации установлены и работают в штатном режиме. Однако сотрудник заходил на подозрительные ресурсы. Основываясь на информации, собранной при помощи ПО, администратор информационной безопасности может понять какие ошибки допускают сотрудники и предотвратить их, используя средства защиты информации или организационные меры.

Вышеописанные действия необходимы, поскольку не всегда возможно уследить за всеми аспектами защиты информации. Автоматизация данного процесса позволит сократить количество инцидентов информационной безопасности, тем самым снижая вероятность хищения персональных данных.

Данное исследование подтверждает исключительную важность эффективной защиты персональных данных в условиях современной цифровой среды. Анализ нормативно правовой базы и статистики утечек выявил существенные пробелы и трудности в обеспечении соответствия информационных систем требованиям законодательства. Для решения этой проблемы в рамках исследования

было разработано специализированное ПО, предназначенное для автоматизированного мониторинга и оценки соответствия информационных систем нормам защиты персональных данных.

Тестирование ПО на базе ИСПДн «Бухгалтерия и кадры» ООО «АйТиАнгел» показало хорошие результаты и помогло выявить недочеты в работе сотрудников, тем самым подняв их осведомленность в информационной безопасности.

Данный продукт может стать важным элементом комплексной стратегии защиты персональных данных, способствуя повышению доверия граждан к организациям, обрабатывающим их данные, и снижению негативных последствий утечек информации.

Список источников

1. Роскомнадзор зафиксировал за 2024 год 135 случаев утечек данных, в которых содержалось более 710 млн записей о россиянах // Хабр: [сайт]. URL: <https://habr.com/ru/news/874016/> (дата обращения: 12.04.2025).
2. О персональных данных: Федеральный закон от 27 июля 2006 г. № 152-ФЗ: принят Гос. Думой 8 июля 2006 г.: одобр. Советом Федерации 14 июля 2006 г. // Собрание законодательства Российской Федерации. 2006. № 31 (ч. 1). Ст. 3451.
3. Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах: приказ ФСТЭК России от 11 февраля 2013 г. № 17: зарегистрирован в Минюсте России 31 мая 2013 г. № 2878 // Российская газета. 2013. № 124.
4. Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности при использовании атомной энергии в 2013 году № 21: зарегистрирован в Минюсте России 15 мая 2013 года № 2834 // Российская газета. 2013. № 118.
5. Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций: [сайт]. URL: <https://54.rkn.gov.ru/news/news332968.htm> (дата обращения: 12.04.2025).

Статья поступила в редакцию 21.04.2025; принята к публикации 10.05.2025

Информация об авторе

Колесников М.В. – студент кафедры «Системы информационной безопасности», направление подготовки 10.04.01 – Информационная безопасность, профиль «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Научный руководитель

Шапенская А.М. – ассистент каф. «СИБ» ФГБОУ ВО «БГТУ».

Научная статья

УДК 004.6

Сравнительный анализ технологий двухфакторной аутентификации для физических лиц

Галина Дмитриевна Матюхина^{1✉}, Владимир Александрович Воронин²

^{1, 2}Брянский государственный технический университет, Брянск, Россия

¹galinochka2303@gmail.com✉, <https://orcid.org/0009-0001-1295-2944>

²voroni.vladimir.oz@gmail.com, <https://orcid.org/0009-0009-5380-2465>

Аннотация. Проанализированы технологии двухфакторной аутентификации (как защита персональных данных) для физических лиц сравним их преимущества и недостатки.

Ключевые слова: двухфакторная аутентификация (2FA), SMS-коды, push-уведомления, Adversary-in-the-Middle (AiTM), SIM-swap, SIM-jacking, фишинг, MFA Hammering.

Для цитирования: Матюхина Г.Д., Воронин В.А. Сравнительный анализ технологий двухфакторной аутентификации для физических лиц // Актуальные проблемы кибербезопасности. Противодействие экстремизму и терроризму в информационной молодежной среде: сборник докладов I межрегиональной научно-практической конференции. – Брянск: БГТУ, 2025. – С. 283 – 286.

Двухфакторная аутентификация (2FA) давно стала неотъемлемой частью современных систем безопасности, она обеспечивает дополнительный уровень защиты для пользователей. В данной статье рассмотрим три популярные технологии 2FA: SMS-коды, Push-уведомления и электронную почту. Проведем их сравнительный анализ и представим результаты в таблице. В начале определим, что такое двухфакторная аутентификация.

Двухфакторная аутентификация (2FA) — это метод защиты данных, при котором для входа в систему применяется два независимых способа подтверждения личности пользователя, однако 2FA не заменяет пароль, а дополняет (усиливает) его, повышая безопасность аккаунта и защищая организацию и её пользователей от несанкционированного доступа [1].

Двухфакторная аутентификация требует от пользователя предоставить два различных доказательства своей личности, что значительно повышает безопасность учетных записей. В условиях роста киберугроз выбор реализации правильной технологии 2FA становится критически важным для защиты персональных данных. Однако 2FA имеет свои особенности. Из-за ее усиленной безопасности злоумышленникам всё чаще приходится придумать новые пути обхода. В связи с этим, такая 2FA существенно затрудняет попытки несанкционированного доступа со стороны сторонних пользователей или злоумышленников, несмотря на то, что пароль уже был каким-либо образом скомпрометирован.

Проанализируем подробно три популярные технологии 2FA: SMS-коды, Push-уведомления и электронную почту, рассмотрим их преимущества и

недостатки, выявим общие для всех.

И так, SMS-коды являются стандартной технологией 2FA и применяются с 1996 года [3]. SMS-коды — это одноразовые пароли, которые отправляются пользователю на мобильный телефон [2]. Этот метод широко используется и сейчас, благодаря своей простоте и доступности. Но огромным недостатком SMS-кодов является высокая уязвимость к атакам типа SIM-swap [4]. Такие атаки SIM-jacking, являются опасными для персональных данных пользователя, как в приложениях на телефоне, так и на онлайн-платформах. Данный тип атаки относится к атакам, когда злоумышленники перехватывают контроль над номером телефона жертвы. Далее зная номер телефона жертвы и SMS-код, который приходит на данный номер, можно спокойно получить доступ к любому аккаунту социальных сетей пользователя.

Все Push-уведомления отправляются через мобильное приложение и требуют от пользователя подтвердить вход, нажав кнопку. Этот метод быстр и удобен для пользования. Данная технология 2FA считается наиболее устойчивой к фишингу по сравнению с SMS-кодами, так как они требуют взаимодействия пользователя в приложении, а каналы, по которым передаются данные уведомления, являются зашифрованными. Примером такого канала является применение протокол добровольной идентификации сервера приложений (VAPID), который позволяет серверу приложений идентифицировать свои сообщения [5]. Не смотря на наличие данного уровня защиты между человеком и сервером, существуют сложные атаки, такие как Adversary-in-the-Middle (AiTM), которые могут обмануть пользователей, заставляя его подтверждать ложный доступ кибермошенникам, пробивая данный уровень защиты [6]. После успешной атаки хакер может получить доступ к аккаунту пользователя и его персональным данным, что в дальнейшем будет чревато как финансовым потерям пользователя, так и моральным, в виде ущерба репутации.

Если рассматривать электронную почту как вариант 2FA, то ее также используют для отправки одноразовых кодов пользователю. Этот метод как и SMS-коды прост в реализации, но имеет свои ограничения. Одним из самых главных ограничений является время. Коды, отправляемые на email могут попадать в спам или работать с задержкой во времени из-за нестабильного интернета, чем и затрудняют дальнейшее времяпрепровождение на онлайн-платформах. Email-сообщения передаются также по зашифрованным каналам передачи, поддерживая протоколы шифрования TLS/SSL, которые защищают содержимое письма. Но атаки на электронную почту могут включать подделку писем, используя фишинговые атаки, или использование вредоносного ПО для перехвата кодов, что уменьшает уровень безопасности передачи [4].

В связи со всем вышеизложенным, выведем общие критерии для определения наиболее благоприятной технологии двухфакторной аутентификации для физических лиц.

Таблица 1

Сравнения технологий 2FA

Критерий	SMS-коды	Push-уведомления	Электронная почта
Доступность для пользователей	Высокая	Высокая	Высокая
Зависимость от сети Интернет	Нет	Да	Да
Устойчивость к фишинговым атакам	Низкая	Низкая	Низкая
Задержка во времени	Нет	Да	Да
Возможность дальнейшего использования персональных данных злоумышленником	Да	Да	Да
Передача одноразового кода по зашифрованному каналу	Нет	Да	Да

Поясним подробно значение критериев сравнения в данной таблице.

1) Доступность для пользователей — высокая, означает, что пользователь с легкостью может воспользоваться данной технологией 2FA.

2) Зависимость от сети Интернет — чтобы получать SMS-коды необходима только мобильная сеть, а для Push-уведомления, электронной почты необходимо интернет соединение.

3) Устойчивость к фишинговым атакам — у всех видов 2FA, описанной выше, она низкая.

Делая вывод, можно считать, что все эти технологии являются не стабильными к существующим на данный момент атакам и ведут к финансовым потерям со стороны пользователя при краже персональных данных злоумышленниками. И эти данные подчеркивают важность выбора правильного метода 2FA и необходимость постоянного совершенствования мер безопасности для защиты персональных данных пользователя от новых и развивающихся угроз.

Выбор технологии двухфакторной аутентификации зависит от конкретных потребностей и приоритетов пользователя. SMS-коды и электронная почта просты в использовании, но имеют ограничения по безопасности. Push-уведомления предлагают баланс между удобством и безопасностью, но требуют установки приложения. Важно учитывать все аспекты при выборе метода 2FA для обеспечения наилучшей защиты учетных записей. В настоящее время информационные технологии стремительно развиваются модернизируются и мошеннические способы киберугроз. Поэтому двухфакторная аутентификация продолжает прогрессировать, выделяя несколько основных тенденций в этой области, а точнее внедрение более безопасных методов. SMS-коды, постепенно замещаются более надёжными способами, такими как аппаратные ключи и биометрия (Passkeys), внедряются устройства с поддержкой криптографической аутентификации для входа в системы (пример: «Рутокен Lite»).

Список источников

1. Двухфакторная аутентификация: что это и как внедрить. URL: <https://altcraft.com/ru/glossary/chto-takoe-dvuhfaktornaya-autentifikaciya-2fa> (дата обращения: 16.04.2025).
2. Аутентификация пользователя: что это такое, виды и для чего нужно. URL: <https://i-dgtl.ru/kompaniya/blog/dlya-chego-nuzhna-autentifikatsiya-polzovatelya/> (дата обращения: 14.04.2025).
3. Multi-factor authentication // Wikipedia. URL: https://en.m.wikipedia.org/wiki/Multi-factor_authentication (дата обращения: 06.04.2025).
4. Самые надёжные способы двухфакторной аутентификации. Какие меры защиты аккаунта применять в 2025 году // Технологии — Секрет фирмы. URL: <https://secretmag.ru/technologies/nikakikh-sekretnykh-voprosov-i-sms.htm?ysclid=m9oqc9wwla756467554> (дата обращения: 13.04.2025).
5. Как настроить push-уведомления в PWA // AppMaster. URL: <https://appmaster.io/ru/blog/kak-nastroit-push-uvdomleniia-v-pwa> (дата обращения: 11.04.2025).
6. Как преступники обходят многофакторную аутентификацию // Профессиональные писатели. URL: <https://prowritersins.com/cyber-insurance-blog/adversary-in-the-middle-aitm-phishing/> (дата обращения: 10.04.2025).

Статья поступила в редакцию 20.04.2025; принята к публикации 10.05.2025

Информация об авторах

Матюхина Г.Д. – студент кафедры «Системы информационной безопасности», направление подготовки 10.05.03 – Информационная безопасность автоматизированных систем ФГБОУ ВО «БГТУ».

Воронин В.А. – старший преподаватель кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Вклад авторов

Матюхина Г.Д. – идея, сбор материала, обработка материала, частичное написание статьи (50%).

Воронин В.А. – научное редактирование, частичное написание статьи (50%).

Конфликт интересов отсутствует.

Научная статья

УДК 004.056.5

Преимущества и риски использования биометрии для защиты данных физических лиц

Галина Дмитриевна Матюхина^{1✉}, Максим Валерьевич Ковалев²

^{1, 2} Брянский государственный технический университет, Брянск, Россия

¹ galinochka2303@gmail.com[✉], <https://orcid.org/0009-0001-1295-2944>

² makskovalew@mail.ru, <https://orcid.org/0009-0002-9284-4624>

Аннотация. Рассмотрены риски и преимущества использования биометрической идентификации для защиты персональных данных физических лиц.

Ключевые слова: биометрия, биометрической идентификация, многофакторной аутентификации (MFA), токены.

Для цитирования: Матюхина Г.Д., Ковалев М.В. Преимущества и риски использования биометрии для защиты данных физических лиц // Актуальные проблемы кибербезопасности. Противодействие экстремизму и терроризму в информационной молодежной среде: сборник докладов I межрегиональной научно-практической конференции. – Брянск: БГТУ, 2025. – С. 287 – 290.

В настоящее время наиболее популярным становится использование биометрической идентификации в различных сферах человеческой деятельности, особенно для защиты персональных данных пользователей. Биометрические данные используются в большинстве современных мобильных устройств, а с 2010 года в РФ выдаются биометрические заграничные паспорта. Биометрия становится наиболее популярным методом аутентификации, способствует улучшению безопасности и удобства. Что собой представляет биометрия?

Биометрия — это система идентификации и распознавания человека по уникальным физическим характеристикам или поведенческим факторам, таким как: отпечаток пальца, голос, трехмерный снимок лица или тела, рисунок вен, сетчатка глаза [1]. Все данные сведения, которые характеризуют физиологические и биологические особенности человека являются биометрическими персональными данными в соответствии со ст.11 Федерального закона от 27.07.2006 N 152-ФЗ (ред. от 08.08.2024) "О персональных данных" [9].

Биометрическая идентификация имеет два основных вида распределения по принципу действия биометрических персональных данных:

А. *Статический. Включает в себя следующие:*

- 1) отпечаток пальца;
- 2) радужка глаза;
- 3) сетчатка глаза;
- 4) черты лица;
- 5) термограмма лица;
- 6) рисунок вен.

В. Динамический:

- 1) голос;
- 2) жесты;
- 3) походка;
- 4) почерк;
- 5) характер набора текста на клавиатуре;
- 6) мимика лица при произношении кодовых слов.

А также существует комбинирование этих двух видов биометрической идентификации — применение нескольких биометрических признаков совместно с языковым программированием.

Однако, как и любая технология, биометрия имеет свои преимущества и риски. В данной статье рассмотрено, как можно использовать биометрию для защиты данных физических лиц и с какими рисками это может быть связано.

Одним из наиболее распространенных преимуществ использования биометрии является ее высокий уровень безопасности, который влияет на сохранение всех персональных данных, хранящихся в системе. Все биометрические данные, такие как отпечатки пальцев, радужная оболочка глаза или черты лица, являются уникальными для каждого человека. Поэтому это делает их сложными для подделки, чем значительно повышает уровень безопасности по сравнению с традиционными методами аутентификации, такими как пароли [2]. Помимо этого все эти данные защищены Федеральным законом от 29 декабря 2022 г. № 572-ФЗ "Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации" [8]. В связи с данным законом все данные хранятся в зашифрованном виде и уничтожаются по истечении срока, необходимого для достижения целей их обработки в системах.

Также важно отметить, тот факт, что биометрическая идентификация позволяет пользователям быстро и легко получить доступ к своим устройствам и учетным записям. Позволяет сокращать время и избавляет пользователя от необходимости запоминать сложные пароли или носить с собой физические токены или другие аппаратные средства [3]. Ведь все эти персональные данные всегда с пользователем, что делает их удобным методом аутентификации. Пользователи физически не могут забыть или потерять свои биометрические данные, как это может произойти с паролями или другими устройствами [4].

Биометрическую аутентификацию применяют в сочетании с другими методами аутентификации, используя вторым слоем защиты. Примерами таких взаимодействий можно считать пароли или одноразовые коды совместно с биометрией для создания многофакторной аутентификации (MFA), что добавляет дополнительный уровень безопасности [5].

Говоря о всех преимуществах использования биометрии, мы забываем о рисках, которые есть на данный момент. Биометрические данные пользователей хранятся в системах или базах данных, однако если в систему будет сделан несанкционированный доступ со стороны злоумышленников, то все данные будут доступны им, что может привести к нарушению конфиденциальности пользователя. Хакеры имеют возможности для компрометации данных, могут

использовать их для несанкционированного доступа к учетным записям пользователей, что принесёт финансовые потери [6].

Далее необходимо отметить, что биометрические данные не могут быть изменены в системе, в отличие от паролей, если они будут скомпрометированы, это будет означать, что пользователь не сможет просто «сбросить биометрические данные», как это можно сделать с паролем [7]. Простым языком мы говорим о том, что такие «захваченные» биометрические данные могут быть использованы постоянно. В случае утечки биометрических данных, пользователь имеет право на компенсацию, как морального вреда, так и материальных убытков, связанных с утечкой персональных данных, предусмотренные законодательством РФ через судебные иски против виновных лиц или организаций.

Риск для здоровья пользователя — многие люди считают, что биометрические технологии могут быть опасны для здоровья, сканеры и терминалы идентификации плохо изучены, однако они не опаснее обычных фотоаппаратов. В них не используют лазеры, поэтому нет риска для здоровья. Идентификацию черт лица или радужки глаза сканеры проводят бесконтактно. На данный момент все устройства выпускаются с соответствующей документацией, подтверждающей безопасность для человека (пример: на устройства идентификации по венам от BioSmart имеет медицинское заключение ФГБНУ «НИИ медицины труда»).

Существуют меры по минимизации данных рисков использования биометрической идентификации:

- 1) использовать несколько видов биометрии (пример: система одновременно анализирует лицо, голос и мимику лица при произнесении определенного набора слов или кодового слова;
- 2) использование динамической биометрии значительно усиливает защиту, так как для проведения идентификации необходимо более длительное время;
- 3) шифрование и раздельное хранение данных;
- 4) избегать передачи биометрии сомнительным источникам.

Биометрическая идентификация предлагает значительные преимущества в области безопасности и удобства, но также представляет собой риски, связанные с конфиденциальностью и необратимостью данных. Для успешного внедрения биометрических технологий необходимо тщательно учитывать эти риски и разрабатывать меры для их минимизации. Пользователи должны быть осведомлены о преимуществах и рисках, чтобы принимать обоснованные решения о защите своих данных. В конечном итоге, биометрия может стать мощным инструментом в арсенале кибербезопасности, но только при условии ответственного подхода к ее использованию.

Список источников

1. Биометрия: что такое биометрические данные человека, как их собирают и где используют // Skillbox Media. URL: <https://skillbox.ru/media/code/biometricheskie-dannye-cto-eto-takoe-i-gde-khranitsya-biometriya/?ysclid=m9n2di5t1600480350> (дата обращения: 17.04.2025).
2. Защита биометрических персональных данных // RTM Group. URL:

<https://rtmtech.ru/articles/biodata-protect/> (дата обращения: 10.04.2025).

3. Биометрическая аутентификация – что это такое и зачем она нужна. URL: <https://rt-solar.ru/events/blog/3616/> (дата обращения: 16.04.2025).

4. Защита данных с помощью биометрии: руководство по внедрению. URL: <https://mediapark.uz/blog/post/malumotlarni-himoya-qilish-uchun-biometrik-texnologiyalardan-qanday-foydalanish-kerak> (дата обращения: 14.04.2025).

5. Что такое биометрия? Как она используется в кибербезопасности? URL: <https://www.kaspersky.ru/resource-center/definitions/biometrics> (дата обращения: 12.04.2025).

6. Сбор биометрических данных: риски и последствия. URL: <https://www.tbank.ru/invest/social/profile/basebel/68ec81e9-711a-4f0f-931a-b4c035d5bfab/?author=profile> (дата обращения: 13.04.2025).

7. Угрозы безопасности для систем обработки и хранения биометрических данных // Securelist. URL: <https://securelist.ru/biometric-data-processing-and-storage-system-threats/95221/> (дата обращения: 17.04.2025).

8. Федеральный закон «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации» от 29.12.2022 N 572-ФЗ // КонсультантПлюс. URL: https://www.consultant.ru/document/cons_doc_LAW_436110/314a79f49a806b40b413fda2b160c63163cb3d6d/ (дата обращения: 12.04.2025).

9. Федеральный закон «О персональных данных» от 27.07.2006 N 152-ФЗ // КонсультантПлюс. URL: https://www.consultant.ru/document/cons_doc_LAW_61801/7336c78762a98b5f4f698b8c3800dca1111acc16/?ysclid=m9pzr6i5c5240944402 (дата обращения: 18.04.2025).

Статья поступила в редакцию 20.04.2025; принята к публикации 10.05.2025

Информация об авторах

Матюхина Г.Д. — студент кафедры «Системы информационной безопасности», направление подготовки 10.05.03 — Информационная безопасность автоматизированных систем ФГБОУ ВО «БГТУ».

Ковалев М.В. — ассистент кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Вклад авторов

Матюхина Г.Д. — идея, сбор материала, обработка материала, частичное написание статьи (50%).

Ковалев М.В. — написание статьи, научное редактирование текста (50%).

Конфликт интересов отсутствует.

СЕКЦИЯ 6. ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ КАК ИНСТРУМЕНТ ПОМОЩИ СПЕЦИАЛИСТУ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Научная статья

УДК 004

OSINT: виды разведки, инструменты и правовые ограничения в практике анализа открытых данных

Павел Александрович Аверин^{1✉}, Сергей Игоревич Коновалов²,
Дмитрий Андреевич Лысов³

^{1,2,3} Брянский государственный технический университет, Брянск, Россия

¹stopnotwont@gmail.com[✉], <https://orcid.org/0009-0003-5074-7217>

²velvet1way@gmail.com, <https://orcid.org/0009-0008-5867-635X>

³lysovdmitriia@gmail.com, <https://orcid.org/0009-0003-9666-7191>

Аннотация. В условиях нарастающей цифровизации и роста объемов открытых данных особую значимость приобретает разведка по открытым источникам (Open Source Intelligence, OSINT). Настоящая статья систематизирует ключевые направления OSINT-разведки, анализирует функциональные возможности специализированных инструментов, а также акцентирует внимание на нормативно-правовых и этико-правовых ограничениях, сопровождающих работу с открытой информацией. Подчеркивается роль OSINT в обеспечении информационной безопасности и его интеграция в архитектуру аналитических и защитных систем организаций.

Ключевые слова: OSINT, открытые источники, киберугрозы, информационная безопасность, разведка, правовое регулирование, инструменты анализа.

Для цитирования: Аверин П.А., Коновалов С.И., Лысов Д.А. OSINT: виды разведки, инструменты и правовые ограничения в практике анализа открытых данных // Актуальные проблемы кибербезопасности. Противодействие экстремизму и терроризму в информационной молодежной среде: сборник докладов I межрегиональной научно-практической конференции. – Брянск: БГТУ, 2025. – С. 291 – 294.

Современные условия информационного обмена характеризуются постоянным увеличением объема цифровых следов, оставляемых пользователями и организациями в открытом доступе. В связи с этим концепция разведки по открытым источникам (OSINT) становится центральным компонентом в аналитической и защитной инфраструктуре многих организаций. OSINT представляет собой совокупность методов и средств поиска, сбора, структурирования и интерпретации информации, доступной без необходимости применения скрытых или несанкционированных методов доступа. Эффективность использования OSINT обусловлена как технической оснащённостью аналитика, так и его способностью интерпретировать данные с учётом правовых и этических рамок. Развитие технологий, таких как машинное обучение, Big Data и визуализация связей, предоставляет возможность автоматизировать значительную часть разведывательной

деятельности, однако не устраняет необходимости в экспертной оценке полученной информации.

Многообразие задач, решаемых с помощью OSINT, обуславливает необходимость чёткого разграничения подтипов разведки в зависимости от используемых источников, форматов данных и целей анализа. В современной практике используются такие направления, как анализ официальных государственных источников, включая реестры юридических лиц, судебные акты и лицензии. Эти данные применяются в комплаенс-практиках, проверке благонадёжности и правового статуса субъектов. Не менее значимым является анализ цифровой активности в социальных сетях, позволяющий оценивать общественные настроения, выявлять лидеров мнений, отслеживать распространение информации и идентифицировать связи между пользователями. Существенную роль играет обработка геопространственной информации, включая спутниковые снимки, данные геолокации и картографические материалы. Данные ресурсы используются при мониторинге инфраструктуры, оценке логистических маршрутов и анализе физического перемещения объектов. Актуальным направлением остаётся анализ веб-контента, включая сайты, форумы, блоги и специализированные платформы. Важное значение приобретает техническая разведка, направленная на изучение сетевой инфраструктуры, конфигураций, уязвимостей и иных технических параметров, необходимых для оценки киберрисков. Специализированное направление OSINT посвящено выявлению и атрибуции киберугроз, мониторингу вредоносной активности, включая изучение данных в анонимных и ограниченно индексируемых сетях. Анализ финансовой информации позволяет выявлять подозрительные транзакции, схемы уклонения от налогообложения и иные элементы теневой экономики. Дополнительно анализируются визуальные материалы — фотографии, видео, спутниковые изображения — применяемые в мониторинге и оценке объектов. В ряде случаев исследуются специализированные области, включая рекламную активность, регистрацию доменов, поведение пользователей на игровых платформах и источники угроз.

Современные OSINT-практики предполагают использование широкого спектра инструментов, обеспечивающих как автоматизированный сбор, так и визуализацию и интерпретацию информации. Среди них можно выделить агрегаторы ресурсов и утилит, поисковые системы, ориентированные на выявление уязвимых устройств, специализированные инструменты для поиска и извлечения метаданных из документов, платформы для отображения взаимосвязей между объектами анализа, а также фреймворки с модульной архитектурой, поддерживающие различные методы получения данных. В дополнение к этому применяются инструменты для сбора сведений о доменах, email-адресах, субдоменах и автоматизированные сканеры, интегрируемые с многочисленными источниками данных. Методика углублённого поиска, использующая операторы поисковых систем, позволяет обнаруживать конфиденциальную информацию, размещённую без должной защиты. Применение указанных решений требует как технической компетентности, так и соблюдения ограничений, установленных действующим законодательством.

Несмотря на то, что OSINT оперирует данными, размещёнными в открытом доступе, национальные правовые режимы, в том числе правовая система Российской Федерации, предусматривают определённые ограничения на их сбор и использование. Важнейшими среди них являются положения, касающиеся обработки персональных данных. Наличие открытого доступа не означает автоматического согласия субъекта на обработку информации о нём. Кроме того, законодательством ограничено распространение информации, содержащей государственную или коммерческую тайну. Юридическая правомерность использования информации во многом определяется условиями её размещения, целями обработки и способом распространения. Этические аспекты также играют значительную роль: требуется уважение к частной жизни, недопустимость манипулятивных практик и использование компрометирующих методов.

Интеграция OSINT в архитектуру информационной безопасности организаций позволяет осуществлять превентивный мониторинг цифровых активов, выявлять упоминания бренда в открытом и анонимном сегменте сети, оценивать потенциальные векторы атак, а также оперативно реагировать на инциденты. Особенно востребованы соответствующие практики в структурах обеспечения кибербезопасности, включая центры мониторинга безопасности, платформы управления инцидентами и системы киберразведки.

Таким образом, OSINT представляет собой не только универсальный инструмент информационного анализа, но и ключевой элемент стратегического планирования в условиях современной информационной среды. Его применение требует высокого уровня профессионализма, юридической осведомлённости и критического мышления. В перспективе наблюдается тенденция к дальнейшей автоматизации и интеграции OSINT с инструментами искусственного интеллекта и аналитическими платформами, что будет способствовать расширению сфер его применения как в государственном, так и в частном секторах.

Список источников

1. 10 полезных инструментов для OSINT. URL: <https://codeby.net/threads/10-poleznykh-instrumentov-dlya-osint.66907> (дата обращения: 16.04.2025).
2. 10 инструментов OSINT // Безопасная среда. URL: <https://www.youtube.com/watch?v=8wexh7aHKio> (дата обращения: 16.04.2025).
3. 25+1 лучших OSINT расширений для Google Chrome. URL: <https://tomhunter.ru/press-center/blog/25-1-luchshih-osint-rasshirenij-dlya-google-chrome.html> (дата обращения: 16.04.2025).
4. OSINT экосистема от OSINT-SAN Project. URL: <https://github.com/Bafomet666/OSINT-SAN> (дата обращения: 16.04.2025).
5. Топ-инструменты для OSINT-разведки: подробный обзор. URL: <https://www.securitylab.ru/blog/personal/Technolady/354845.php> (дата обращения: 16.04.2025).

Статья поступила в редакцию 19.04.2025; принята к публикации 10.05.2025

Информация об авторах

Аверин П.А. — студент кафедры «Системы информационной безопасности», специальность 10.05.03 — Информационная безопасность автоматизированных систем, специализация «Безопасность открытых информационных систем» ФГБОУ ВО «БГТУ».

Коновалов С.И. — студент кафедры «Системы информационной безопасности», специальность 10.05.03 - Информационная безопасность автоматизированных систем ФГБОУ ВО «БГТУ».

Лысов Д.А. — старший преподаватель кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Вклад авторов

Аверин П.А. — идея, сбор материала, обработка материала, частичное написание статьи.

Коновалов С.И. — сбор материала, обработка материала, частичное написание статьи.

Лысов Д.А. — частичное написание статьи, научное редактирование текста.

Конфликт интересов отсутствует.

Научная статья

УДК 004

Разведка по открытым источникам (OSINT): сущность, цели и место в современной информационной экосистеме

Павел Александрович Аверин^{1✉}, Сергей Игоревич Коновалов²,
Дмитрий Андреевич Лысов³

^{1,2,3}Брянский государственный технический университет, Брянск, Россия

¹stopnotwont@gmail.com✉, <https://orcid.org/0009-0003-5074-7217>

²velvet1way@gmail.com, <https://orcid.org/0009-0008-5867-635X>

³lysovdmitriia@gmail.com, <https://orcid.org/0009-0003-9666-7191>

Аннотация. В условиях цифровой трансформации и роста информационных потоков разведка по открытым источникам (Open Source Intelligence — OSINT) приобретает всё большую значимость. Статья раскрывает сущность OSINT как дисциплины, её цели, принципы, источники данных и отличия от других видов разведывательной деятельности. Обоснована актуальность OSINT в контексте кибербезопасности, национальной безопасности и бизнес-аналитики.

Ключевые слова: OSINT, разведка, открытые источники, информационная безопасность, киберугрозы, аналитика.

Для цитирования: Аверин П.А., Коновалов С.И., Лысов Д.А. Разведка по открытым источникам (OSINT): сущность, цели и место в современной информационной экосистеме // Актуальные проблемы кибербезопасности. Противодействие экстремизму и терроризму в информационной молодежной среде: сборник докладов I межрегиональной научно-практической конференции. – Брянск: БГТУ, 2025. – С. 295 – 297.

Современное общество характеризуется высокой степенью цифровизации, сопровождающейся экспоненциальным ростом объёма доступной информации. В этих условиях особую значимость приобретает систематизация и анализ сведений, получаемых из открытых источников. OSINT (разведка по открытым источникам) является инструментом, позволяющим не только получать критически важные сведения из легальных и общедоступных ресурсов, но и формировать на их основе выводы, значимые для национальной безопасности, бизнеса, исследовательской журналистики и правоохранительной практики.

OSINT (расшифровывается как open source intelligence, с англ. «разведка по открытым источникам») — разведывательная дисциплина и комплекс мероприятий, инструментов и методов для получения и анализа информации из открытых источников. Он применяется в отношении конкретных людей, организаций, а также событий, явлений и целей [1]. Целью OSINT является извлечение знаний, необходимых для принятия управленческих, оперативных или стратегических решений.

К числу ключевых задач OSINT относятся:

- выявление потенциальных угроз и уязвимостей;
- мониторинг деятельности конкурентов и рыночной конъюнктуры;

- отслеживание изменений в общественном мнении и информационной среде;
- расследование инцидентов, в том числе связанных с мошенничеством и кибератаками.

Открытые источники, используемые в рамках OSINT, подразделяются на несколько категорий:

1. Средства массовой информации — печатные и электронные СМИ, телевидение, радио.
2. Интернет-ресурсы — блоги, форумы, социальные сети, видео-хостинги, вики-проекты.
3. Официальные источники — государственные реестры, публичные отчёты, судебные решения.
4. Академические публикации — научные статьи, диссертации, отчёты конференций.
5. Серая литература — технические документы, внутренние отчёты, бюллетени.
6. Коммерческие базы данных — сведения о компаниях, транзакциях, партнёрах.
7. Наблюдения и визуальные источники — спутниковые снимки, геоданные, аэрофотосъёмка.

Важно отметить, что, согласно Протоколу Калифорнийского университета в Беркли, информация, доступ к которой осуществляется без лицензии или авторизации, считается открытой, при условии соблюдения этических и правовых норм её использования. OSINT представляет собой легитимную дисциплину, отличающуюся от шпионажа и агентурной разведки (HUMINT) по нескольким признакам. Используется исключительно легальный доступ к данным. Не требует специальных технических средств или служебного положения. И применяются системные подходы, исключающие сокрытие источников.

При этом OSINT интегрируется в общую разведывательную экосистему, включая такие направления, как SIGINT (радиоэлектронная разведка), GEOINT (геопространственная), IMINT (визуальная), TECHINT (техническая), что повышает эффективность комплексного анализа угроз.

В сфере информационной безопасности OSINT используется для:

- выявления утечек персональных и конфиденциальных данных;
- анализа экспонированных активов компании;
- мониторинга активности вредоносных субъектов в открытых и закрытых сетях;
- повышения осведомлённости сотрудников через анализ актуальных угроз.

Таким образом, OSINT является важнейшим элементом в системе превентивных мер по защите информации.

Разведка по открытым источникам представляет собой неотъемлемый компонент современного анализа данных. Она обеспечивает высокий уровень осве-

домлённости при низких затратах, позволяя оперативно реагировать на изменения в информационном ландшафте. При этом особое внимание должно уделяться правовым и этическим аспектам использования OSINT, особенно в юрисдикциях с высоким уровнем защиты персональных данных.

Список источников

1. OSINT // skillfactory. URL: <https://blog.skillfactory.ru/glossary/osint/> (дата обращения: 09.04.2025). URL: <https://networkguru.ru/8-luchshikh-programm-dlia-analiza-setevogo-trafika/> (дата обращения: 05.03.2025).
2. Разведка по открытым источникам // geochronic. URL: https://geochronic.ru/index.php?title=%D0%A0%D0%B0%D0%B7%D0%B2%D0%B5%D0%B4%D0%BA%D0%B0_%D0%BF%D0%BE_%D0%BE%D1%82%D0%BA%D1%80%D1%8B%D1%82%D1%8B%D0%BC_%D0%B8%D1%81%D1%82%D0%BE%D1%87%D0%BD%D0%B8%D0%BA%D0%B0%D0%BC (дата обращения: 09.04.2025).
3. Типы и виды OSINT или подразделы открытого поиска // dataqa. URL: <https://rtmtech.ru/articles/dlya-chego-nuzhen-osint/> (дата обращения: 09.04.2025).
4. OSINT: инструменты // habr. URL: <https://habr.com/ru/articles/769690/> (дата обращения: 09.04.2025).

Статья поступила в редакцию 19.04.2025; принята к публикации 10.05.2025

Информация об авторах

Аверин П.А. — студент кафедры «Системы информационной безопасности», специальность 10.05.03 — Информационная безопасность автоматизированных систем, специализация «Безопасность открытых информационных систем» ФГБОУ ВО «БГТУ».

Коновалов С.И. — студент кафедры «Системы информационной безопасности», специальность 10.05.03 - Информационная безопасность автоматизированных систем ФГБОУ ВО «БГТУ».

Лысов Д.А. — старший преподаватель кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Вклад авторов

Аверин П.А. — идея, сбор материала, обработка материала, частичное написание статьи.

Коновалов С.И. — сбор материала, обработка материала, частичное написание статьи.

Лысов Д.А. — частичное написание статьи, научное редактирование текста.

Конфликт интересов отсутствует.

Научная статья

УДК 004

Оценка результативности современных методов обеспечения информационной безопасности с применением межсетевых экранов

Павел Александрович Аверин^{1✉}, Сергей Игоревич Коновалов²,

Кирилл Андреевич Седаков³

^{1,2,3}Брянский государственный технический университет, Брянск, Россия

¹stopnotwont@gmail.com✉, <https://orcid.org/0009-0003-5074-7217>

²velvet1way@gmail.com, <https://orcid.org/0009-0008-5867-635X>

³sekira98@mail.ru, <https://orcid.org/0009-0002-9284-4624>

Аннотация. Статья посвящена исследованию действенности актуальных методик защиты информационной инфраструктуры с применением межсетевых экранов. Межсетевой экран (брандмауэр) представляет собой одно из базовых средств обороны корпоративных сетей от угроз, поступающих из внешних источников. Анализируются основные функции, реализуемые брандмауэрами в процессе защиты сетевой среды: контроль сетевого трафика, блокировка подмен IP-адресов, предотвращение распределённых атак отказа в обслуживании (DDoS), ограничение передачи данных на недоверенные IP-адреса, выполнение глубокого анализа пакетов (DPI), а также поддержка защищённых соединений через VPN. Эти механизмы способствуют предотвращению несанкционированного доступа, утечек информации и распространения вредоносного программного обеспечения.

Ключевые слова: межсетевой экран, информационная безопасность, фильтрация трафика, контроль доступа, VPN, NGFW, предотвращение атак, DPI, защита данных, сетевой трафик.

Для цитирования: Аверин П.А., Коновалов С.И., Седаков К.А. Оценка результативности современных методов обеспечения информационной безопасности с применением межсетевых экранов // Актуальные проблемы кибербезопасности. Противодействие экстремизму и терроризму в информационной молодежной среде: сборник докладов I межрегиональной научно-практической конференции. – Брянск: БГТУ, 2025. – С. 298 – 302.

Межсетевой экран (файрвол, брандмауэр) представляет собой систему фильтрации данных, проходящих между глобальной сетью и внутренней сетью организации [1]. Его основное предназначение заключается в проверке поступающих данных и блокировке потенциально опасного содержимого. Общая схема функционирования брандмауэра представлена на рис. 1.

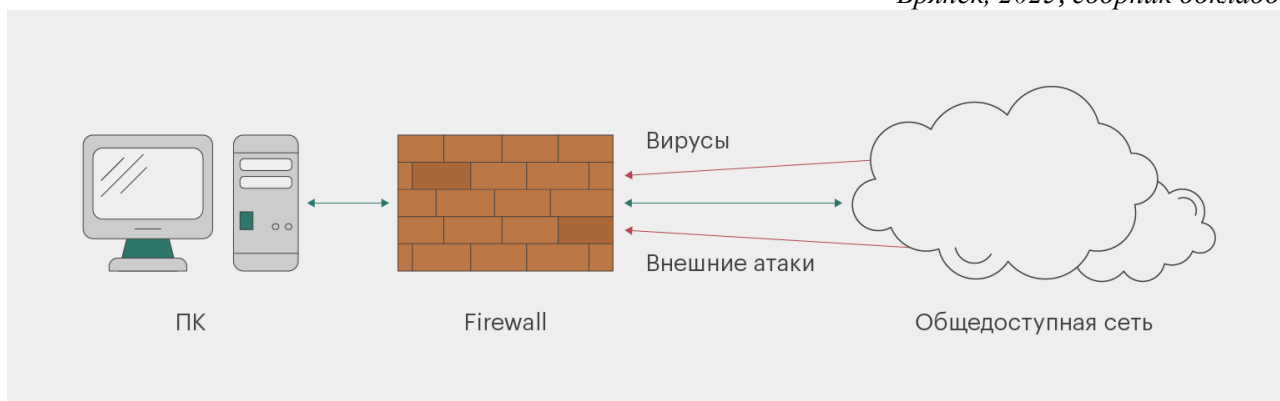


Рис. 1. Схема функционирования межсетевого экрана

Некоторые типы межсетевых экранов обладают функциональностью содержательного анализа трафика, включая возможность обнаружения вредоносных объектов, таких как вредоносное программное обеспечение, фишинговые ресурсы и иные потенциальные угрозы. Реализация подобных механизмов существенно снижает вероятность компрометации корпоративной информационной инфраструктуры и способствует локализации инцидентов на ранних этапах. Кроме того, межсетевые экраны позволяют реализовывать политику ограниченного доступа к нежелательным веб-ресурсам в соответствии с внутренними регламентами организации, обеспечивая контроль за соблюдением нормативных требований и снижая риск социальных атак.

Выделяют следующие основные категории межсетевых экранов:

- аппаратные решения;
- программные реализации;
- межсетевые экраны нового поколения (Next-Generation Firewalls, NGFW).

Аппаратные межсетевые экраны представляют собой специализированные устройства, предназначенные для выполнения функций маршрутизации, фильтрации и анализа сетевого трафика в режиме реального времени. Обычно такие решения функционируют на базе встроенного специализированного программного обеспечения и используются в крупных корпоративных сетях, где критична высокая производительность и надёжность. Наиболее распространёнными представителями данного класса являются решения от производителей Cisco (ASA, FirePower), Fortinet (FortiGate) и аналогичных вендоров. Аппаратные брандмауэры позволяют централизованно управлять политиками безопасности, осуществлять мониторинг событий, а также поддерживают функции внутренней сегментации сети для минимизации возможных векторов атак.

Программные межсетевые экраны реализуются в виде программных компонентов, устанавливаемых на физические или виртуальные серверы. К числу таких решений можно отнести встроенный в операционные системы Windows брандмауэр, а также утилиту iptables в среде Linux. Программные межсетевые экраны находят широкое применение в малых и средних организациях, где за-

траты на внедрение аппаратных решений являются экономически нецелесообразными, а структура сети не требует высокой пропускной способности традиционных устройств.

Межсетевые экраны следующего поколения (NGFW) представляют собой эволюционное развитие классических брандмауэров, сочетая в себе традиционные механизмы фильтрации с функциональностью обнаружения и предотвращения атак, анализом трафика на уровне приложений, возможностями контроля активности пользователей и использования контекстной информации. Благодаря внедрению технологий поведенческого анализа и алгоритмов машинного обучения NGFW способны идентифицировать сложные многоступенчатые угрозы, включая таргетированные атаки и попытки утечки конфиденциальной информации.

Фильтрация сетевого трафика, осуществляемая межсетевыми экранами, осуществляется на основе заданных правил, определяющих допустимые направления и типы соединений. Данная технология позволяет блокировать до 90% нежелательного трафика, однако при использовании злоумышленниками легитимных протоколов и портов эффективность фильтрации может быть существенно снижена. В таких случаях необходима интеграция с другими средствами защиты и проведение углублённого анализа.

Механизм антиспуфинга предназначен для предотвращения подмены сетевых адресов и обеспечивает проверку достоверности источника IP-пакетов. При корректной настройке он позволяет предотвратить до 99% атак, основанных на подделке адресов. Однако в условиях наличия внутренних угроз или некорректной конфигурации антиспуфинг-фильтры могут стать причиной ложных срабатываний и повлиять на стабильность функционирования легитимных сервисов.

Противодействие DDoS-атакам реализуется за счёт блокировки anomalously частых или подозрительных запросов, а также путём применения лимитов на соединения и ресурсов системы. На сетевом уровне возможно снижение нагрузки до 80–90% за счёт отсекаемых массированных низкоуровневых потоков. В случае атак на прикладные уровни (например, на веб-приложения) эффективная защита требует привлечения дополнительных решений: использования распределённых инфраструктур доставки контента (CDN), облачных фильтров и специализированных сервисов защиты от DDoS.

Глубокий анализ пакетов (Deep Packet Inspection, DPI) представляет собой метод анализа содержимого сетевых пакетов, позволяющий идентифицировать вредоносные объекты, недоступные для обнаружения с помощью традиционных сигнатурных методов. DPI способен выявлять до 95% угроз, включая скрытую активность, внедрённую в легитимный трафик. Однако его применение связано с высокой вычислительной нагрузкой и может приводить к снижению пропускной способности, особенно в условиях работы с большим объёмом данных.

Особую сложность представляет анализ зашифрованного трафика, что требует применения специализированных технологий расшифровки на границе сети. В современных решениях используются методы перехвата и временного

дешифрования данных с последующим анализом и повторным шифрованием. Такие подходы позволяют выявлять угрозы внутри защищённых соединений, обеспечивая комплексную проверку безопасности трафика, в том числе в рамках протоколов HTTPS, SSH и аналогичных. В то же время данные технологии требуют строгого соблюдения прав доступа и конфиденциальности, так как возможны риски нарушения приватности пользователей.

VPN-технологии применяются для создания защищённых каналов связи между удалёнными пользователями и корпоративной сетью. Они обеспечивают целостность и конфиденциальность передаваемой информации. Однако при отсутствии системы проверки на стороне клиента возможна передача вредоносного программного обеспечения внутрь корпоративной среды, что требует обязательного внедрения механизмов контроля и фильтрации трафика на входе в защищённый сегмент.

Таким образом, межсетевые экраны выполняют ключевую функцию в обеспечении сетевой безопасности, формируя первый уровень защиты от внешних и внутренних угроз. Их функциональные возможности — от классической фильтрации до поведенческого анализа и обработки зашифрованного трафика — позволяют адаптировать защиту под особенности конкретной информационной инфраструктуры. Эффективная реализация данных решений требует комплексного подхода, включающего регулярный аудит, обновление сигнатур, мониторинг событий и взаимодействие с другими компонентами системы обеспечения информационной безопасности.

Список источников

1. Брандмауэр: что он делает и кому может быть полезен. URL: <https://www.smart-soft.ru/blog/brandmauer/> (дата обращения: 03.11.2024).
2. Что такое протоколы передачи данных. URL: <https://sky.pro/media/chto-takoe-protokoly-peredachi-dannyh/> (дата обращения: 03.11.2024).
3. Межсетевой экран: что такое и как. URL: <https://selectel.ru/blog/firewall/> (дата обращения: 05.11.2024).

Статья поступила в редакцию 19.04.2025; принята к публикации 10.05.2025

Информация об авторах

Аверин П.А. — студент кафедры «Системы информационной безопасности», специальность 10.05.03 – Информационная безопасность автоматизированных систем, специализация «Безопасность открытых информационных систем» ФГБОУ ВО «БГТУ».

Коновалов С.И. — студент кафедры «Системы информационной безопасности», специальность 10.05.03 – Информационная безопасность автоматизированных систем ФГБОУ ВО «БГТУ».

Седаков К.А. — ассистент кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Вклад авторов

Аверин П.А. – идея, сбор материала, обработка материала, частичное написание статьи.

Коновалов С.И. – сбор материала, обработка материала, частичное написание статьи.

Седаков К.А. – частичное написание статьи, научное редактирование текста.

Конфликт интересов отсутствует.

Научная статья

УДК 004.056

Искусственный интеллект в биометрии: новые решения для обеспечения безопасности доступа

**Александр Александрович Брюханов¹✉, Дмитрий Александрович Куликов²,
Владимир Николаевич Чернов³, Вадим Романович Шишов⁴**

^{1,2,3,4} Межвидовой центр подготовки и боевого применения (учебный и испытательный),
Тамбов, Россия

^{1,2,3,4} nauchnajarota@yandex.ru ✉

Аннотация. В современном быстро меняющемся мире, ориентированном на технологии, безопасность физических и цифровых активов важна как никогда. Системы контроля и управления доступом стали важным компонентом комплексных мер безопасности в широком спектре отраслей, поскольку они предоставляют средства для защиты конфиденциальной информации, ресурсов, сотрудников, посетителей и собственности от несанкционированного доступа (НСД), а также снижают вероятность различных инцидентов, которые могут привести к ущербу и отразиться на репутации организации. Биометрия является уникальной, она не может быть забыта или потеряна, и для предъявления такой информации требуется физическое присутствие ее носителя. В данной статье рассматривается анализ системы контроля, концепция биометрии и управления доступом.

Ключевые слова: несанкционированный доступ (НСД), биометрия, система контроля управления доступом (СКУД), идентификация, аутентификация.

Для цитирования: Брюханов А.А., Куликов Д.А., Чернов В.Н., Шишов В.Р. Искусственный интеллект в биометрии: новые решения для обеспечения безопасности доступа // Актуальные проблемы кибербезопасности. Противодействие экстремизму и терроризму в информационной молодежной среде: сборник докладов I межрегиональной научно-практической конференции. – Брянск: БГТУ, 2025. – С. 303 – 307.

Ранее обеспечение безопасного доступа осуществлялось с помощью специальных субъектов, которые осуществляли аутентификацию сотрудников на основе пропусков или специальных списков, принимали решение о предоставлении или запрете доступа в критических точках входа, а также управляли шлагбаумами, турникетами, воротами и дверями вручную. Эти процессы требовали времени и ограничивали пропускную способность точки входа. Сегодня стали использоваться передовые технологии, такие как смарт-карты и биометрия.

С развитием технологий системы контроля и управления доступом стали более сложными и надежными, если раньше единственной целью системы было обеспечение физической безопасности, то сейчас она может осуществлять контроль за рабочим временем сотрудников, отслеживать их время прибытия и ухода, а также составлять различные отчеты.

Биометрия является уникальной, она не может быть забыта или потеряна, и для предъявления такой информации требуется физическое присутствие ее но-

сителя, то есть самого человека, однако, если биометрическая информация оказалась каким-то образом испорчена, например, в результате травмы, восстановить ее невозможно [1].

Таким образом, системы контроля и управления доступом автоматизируют и существенно улучшают контрольно-пропускной режим, исключают возможность несанкционированного и бесконтрольного доступа на территорию объекта, а также повышают уровень безопасности на предприятии.

1. Понятие биометрии и системы контроля и управления доступом

Биометрия – это наука, которая изучает уникальные физические характеристики человека, такие как отпечатки пальцев, лицо, радужная оболочка глаза или голос. Эти особенности помогают идентифицировать людей. Например, когда мы используем отпечаток пальца для разблокировки телефона или для входа в банк, мы пользуемся биометрией. Это удобно и безопасно, потому что такие данные сложно подделать [2].

Искусственный интеллект (ИИ) – это технология, которая позволяет компьютерам и программам учиться и принимать решения, похожие на человеческие. ИИ может обрабатывать большие объемы информации и находить закономерности, что делает его очень полезным в различных сферах, включая биометрию. Например, когда мы сканируем лицо для входа в приложение, ИИ сравнивает это изображение с данными в базе и быстро определяет, кто мы.

Система контроля и управления доступом (СКУД) – совокупность аппаратных, аппаратно-программных и технических средств, главная задача которых – организация пропускного режима и управления доступом на объекте.

К задачам СКУД относятся: контроль входа по средствам шлагбаумов или КПП, установленных на основных путях и введение базы пользователей, имеющих доступ; Базовые элементы любой СКУД: контроллер, идентификатор, считыватель, исполнительное устройство [3].

Вместе биометрия и искусственный интеллект помогают сделать процесс аутентификации более быстрым и безопасным. Это значит, что мы можем быстрее и надежнее получать доступ к своим важным данным. Однако, важно помнить, что с этими технологиями также связаны вопросы безопасности и защиты личной информации.

2. Интеграция искусственного интеллекта в биометрические системы и работа СКУД

Интеграция искусственного интеллекта (ИИ) в биометрические системы – это процесс, когда технологии ИИ помогают улучшить работу систем, которые используют биометрические данные. Давайте разберем, как это происходит и зачем это нужно.

ИИ может анализировать биометрические данные, такие как отпечатки пальцев или лица, с высокой точностью. Это значит, что система может быстрее и правильнее определять, кто перед ней. Например, если вы пытаетесь войти в банковское приложение с помощью распознавания лица, ИИ помогает убедиться, что это именно вы.

В информационной среде обрабатывается огромное количество данных. ИИ может быстро анализировать эти данные и находить закономерности. Это помогает лучше понимать своих повышать уровень безопасности. Также, ИИ может обучаться на примерах, чтобы улучшать свои результаты. Например, если система распознавания лица ошиблась, ИИ может запомнить эту ошибку и стать лучше в будущем. Это помогает уменьшить количество ошибок и повысить безопасность.

ИИ может быстро реагировать на подозрительные действия. Если система замечает что-то необычное, например, попытку входа с незнакомого устройства, она может сразу запросить дополнительную проверку личности, например, с помощью отпечатка пальца.

Интеграция ИИ делает использование биометрических систем более удобным. Например, системы могут работать быстрее и без лишних шагов, что делает процесс входа в приложение или подтверждения транзакций более простым.

Благодаря ИИ биометрические системы становятся более защищенными от мошенничества. ИИ может распознавать попытки обмана, такие как использование фотографий вместо реального лица, что делает систему надежнее.

Для работы СКУД используется специализированное программное обеспечение (ПО), которое настраивается индивидуально, исходя из сложности системы и конкретных целей установки.

В состав СКУД могут входить другие дополнительные средства [4]:

- источники электропитания;
- дверные доводчики;
- световые и звуковые оповещатели;
- устройства преобразования интерфейсов сетей связи;
- видеокамеры;
- источники бесперебойного питания.

Общая схема СКУД приведена на рис. 1.



Рис. 1. Общая схема СКУД

Принцип работы СКУД прост: пользователь предъявляет аутентификационный признак, информация передаётся на контроллер, который принимает решение о предоставлении доступа. Если проход разрешен, система посылает сигнал на исполнительное устройство, и замок открывается.

Таким образом, интеграция искусственного интеллекта в биометрические системы и СКУД помогает сделать их более эффективными, безопасными и удобными для пользователей.

Будущее биометрии, искусственного интеллекта и системы контроля и управления доступом открывает новые горизонты для улучшения безопасности.

Тем не менее, важно помнить о возможных вызовах, таких как вопросы конфиденциальности и безопасности данных. Чтобы максимально использовать преимущества этих технологий, необходимо продолжать работать над их защитой и этичным использованием [5].

В конечном итоге, сочетание биометрии и ИИ может значительно изменить многие сферы. Мы можем с оптимизмом смотреть в будущее, ожидая, что эти инновации принесут пользу всем пользователям.

В процессе написания статьи рассмотрены назначение, состав и классификация СКУД. Проведён сравнительный анализ существующих методов биометрической аутентификации, который показал, что способ аутентификации субъектов по геометрии лица является наиболее эффективным, безопасным, а также удобным для пользователей.

Список источников

1. Ворона, В. А. Системы контроля и управления доступом / В. А. Ворона, В. А. Тихонов. – М.: Горячая линия-Телеком, 2018. – 272 с.
2. ГОСТ Р 51241-2008. Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний. – Введ. 2009-09-01. – М.: Стандартинформ, 2009. – 28 с.
3. Рудаков О. М. Аутентификация на основе биометрических данных // Научная перспектива. 2016. № 6. С. 75 – 77.
4. Кухарев Г. А. Биометрические системы: методы и средства идентификации личности человека. – СПб.: Политехника, 2001. – 240 с.
5. Волхонский В. В. Системы контроля и управления доступом. – СПб.: Университет ИТМО, 2015. – 105 с.

Статья поступила в редакцию 19.04.2025; принята к публикации 10.05.2025

Информация об авторах

Брюханов А.А. - старший оператор научной роты войск РЭБ.

Куликов Д.А. - оператор научной роты войск РЭБ.

Чернов В.Н. - оператор научной роты войск РЭБ.

Шишов В.Р. - оператор научной роты войск РЭБ.

Вклад авторов

Брюханов А.А. – редактирование визуальной части (рисунков), частичное написание статьи (15%).

Куликов Д.А. – научное редактирование текста, частичное написание статьи (35%).

Чернов В.Н. – научное редактирование текста, частичное написание статьи (35%).

Шишов В.Р. – подбор литературных источников, частичное написание статьи (15%).

Конфликт интересов отсутствует.

Научная статья

УДК 004.056.55

Использование искусственного интеллекта в системах видеонаблюдения

Максим Дмитриевич Грива^{1✉}, Алина Михайловна Шапенская²

^{1,2}Брянский государственный технический университет, Брянск, Россия

¹maks.griva.04@mail.ru ✉

²alinashapenskaya@yandex.ru

Аннотация. В статье рассматриваются актуальные направления и перспективы развития систем видеонаблюдения. Освещаются достижения в повышении качества изображения, расширении функционала, внедрении искусственного интеллекта и аналитических инструментов, распространении беспроводных технологий и взаимодействии с Интернетом вещей (IoT), совершенствовании биометрии и увеличении значимости облачных сервисов. Подчеркивается важность вопросов энергетической эффективности и экологической устойчивости систем видеонаблюдения. Представлены выводы о неизбежности перехода к новым стандартам качества и уровню безопасности, формирующим цифровую среду будущего.

Ключевые слова: ip- камера, видеонаблюдение, перспективы развития.

Для цитирования: Грива М.Д., Шапенская А.М. Использование искусственного интеллекта в системах видеонаблюдения // Актуальные проблемы кибербезопасности. Противодействие экстремизму и терроризму в информационной молодежной среде: сборник докладов I межрегиональной научно-практической конференции. – Брянск: БГТУ, 2025. – С. 308 – 310.

Современные системы видеонаблюдения претерпели значительные изменения с момента появления первых аналоговых камер. Основной причиной трансформации стало появление и быстрое развитие технологий искусственного интеллекта (ИИ), которые кардинально изменили подходы к обработке и интерпретации визуальной информации. Именно внедрение ИИ позволило перейти от пассивного наблюдения к активному контролю ситуации, улучшило функциональность и обеспечило более точное реагирование на угрозы и инциденты.

Традиционное видеонаблюдение долгое время оставалось инструментом сбора данных, предоставляющим оператору возможность наблюдать за обстановкой в пределах зоны видимости камеры. Однако человек физически ограничен в своей способности обрабатывать большие объемы визуальной информации одновременно, и человеческий фактор нередко становился источником ошибок и упущений. С появлением ИИ ситуация изменилась коренным образом:

- Система стала самостоятельной, способной эффективно и быстро реагировать на любые отклонения от нормы.
- Появилась возможность автоматической классификации событий, фильтрации тревожных сигналов и уведомления соответствующих служб о происшествиях.
- Значительно возросли возможности точного определения целей и их отслеживания.

Рассмотрим несколько основных областей, где искусственный интеллект показывает наибольшую пользу:

Наиболее очевидное направление применения ИИ — это распознавание лиц и автомобильных номеров. Алгоритмы глубокого обучения способны анализировать видеопотоки и сопоставлять лица или номера автомобилей с базами данных, определяя совпадения и несоответствия. Такое применение находит отклик в правоохранительных органах, службе безопасности крупных компаний и городской инфраструктуре.

Благодаря использованию алгоритмов ИИ, камеры научились эффективно классифицировать движения объектов, выявлять опасные сценарии (например, оставленные предметы, нарушение границ запрещенных зон, агрессивное поведение) и своевременно уведомлять операторов. Подобные инструменты стали неотъемлемой частью защиты бизнес-центров, складских комплексов и публичных пространств.

Одна из наиболее интересных особенностей ИИ заключается в способности прогнозировать потенциальные инциденты. Используя исторические данные и современные методы машинного обучения, камеры теперь могут оценивать ситуацию и заблаговременно сообщать о возможных угрозах. Например, ИИ может предупредить о скоплении толпы в местах массового скопления людей или выявить признаки начинающегося пожара.

Еще одним интересным применением ИИ стало создание роботизированных патрулей, оснащенных мобильными камерами. Они обладают полной автономией и могут передвигаться внутри зданий или на улице, выполняя функции обычного охранника. Роботы способны воспринимать обстановку, регистрировать нарушения и информировать службу безопасности о возникших проблемах.

Используя новейшие технологии, камеры видеонаблюдения теперь способны анализировать выражения лиц, жестикуляцию и позы людей, оценивая их эмоции и настроение. Подобная практика применяется в магазинах для оценки удовлетворенности покупателей или в образовательных учреждениях для мониторинга психоэмоционального состояния учащихся.

Несмотря на впечатляющие успехи, внедрение ИИ в видеонаблюдение сталкивается с рядом серьезных трудностей и ограничений:

- Проблема приватности. Широкомасштабное использование систем распознавания лиц вызывает опасения по поводу сохранности личных данных и возможного злоупотребления информацией.
- Ошибочные срабатывания. Несмотря на высокие показатели точности, алгоритмы иногда допускают ошибки, что может приводить к необоснованным действиям или штрафам.
- Технические сложности. Необходимость поддержки огромных объемов данных, обработки в реальном времени и постоянный обмен большими объемами информации требуют мощных серверов и высокоскоростных каналов связи.

Внедрение искусственного интеллекта в системы видеонаблюдения открыло новую эру в сфере безопасности и контроля обстановки. Мы видим значительное ускорение процессов анализа и реагирования, сокращение рисков и повышение общего уровня защищенности населения и объектов. Вместе с тем остаётся много нерешённых вопросов, связанных с этичностью использования ИИ, защитой личной информации и созданием правовых рамок регулирования.

Тем не менее, ясно одно: технологии искусственного интеллекта будут продолжать развиваться, становясь важнейшим компонентом систем видеонаблюдения завтрашнего дня.

Список источников

1. Абрамян А.В. Тенденции развития систем видеонаблюдения // Научно-технический вестник ИТМО. 2022. № 1. С. 45–53.
2. Александров И.К. Искусственный интеллект в системах видеонаблюдения: проблемы и перспективы / И.К. Александров, В.А. Чиркин // Труды международной конференции «Информационно-коммуникационные технологии». — СПб.: Политех-Пресс, 2021. — С. 145–152.
3. Васильев А.Н. Биометрические технологии в системах видеонаблюдения: анализ тенденций и проблем // Вопросы кибербезопасности. 2022. № 3. С. 38–46.
4. Голубев Я.С. Экологичность и энергоэффективность систем видеонаблюдения: критический обзор // Известия вузов. Электроника. 2023. № 2. С. 112–120.
5. Жданова Е.Ю. Применение облачных технологий в системах видеонаблюдения: современный опыт и прогнозы / Е.Ю. Жданова, Д.О. Семенов // Вестник университета имени О.Е. Кутафина. 2022. № 4. С. 154–162.
6. Иванов С.В. Развитие беспроводных технологий и интернета вещей в системах видеонаблюдения // Новые технологии в науке и технике. 2021. № 2. С. 87–95.

Статья поступила в редакцию 23.04.2025; принята к публикации 10.05.2025

Информация об авторах

Грива М.Д. - студент кафедры «Системы информационной безопасности», направление подготовки 10.03.01 – Организация защиты информации ФГБОУ ВО «БГТУ».

Шапенская А.М. – ассистент кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Вклад авторов

Грива М.Д. - идея, сбор материала, обработка материала, частичное написание статьи (50%).

Шапенская А.М. - написание статьи, научное редактирование текста (50%).

Конфликт интересов отсутствует.

Научная статья

УДК 004.8

Искусственный интеллект как помощник в информационной безопасности в медицинских учреждениях

Ирина Юрьевна Медведева^{1✉}, Кирилл Андреевич Седаков²

^{1, 2}Брянский государственный технический университет, Брянск, Россия

¹Grivabarajka73@gmail.com✉, <https://orcid.org/0009-0002-9344-5634>

²sekira98@mail.ru, <https://orcid.org/0009-0002-9284-4624>

Аннотация. В данной статье поднимается вопрос интеграции искусственного интеллекта в сферу информационной безопасности в медицинских учреждениях.

Ключевые слова: безопасность, искусственный интеллект, медицинские учреждения, информационная безопасность.

Для цитирования: Медведева И.Ю., Седаков К.А. Искусственный интеллект как помощник в информационной безопасности в медицинских учреждениях // Актуальные проблемы кибербезопасности. Противодействие экстремизму и терроризму в информационной молодежной среде: сборник докладов I межрегиональной научно-практической конференции. – Брянск: БГТУ, 2025. – С. 311 – 315.

Современная медицина всё чаще внедряет разные технологические решения: электронные медицинские карты, телемедицина, подключённые к сети диагностические устройства — всё это делает медицинские учреждения более эффективными, но одновременно и более уязвимыми. Киберпреступники всё чаще нацеливаются на больницы, поликлиники и лаборатории, стремясь получить доступ к конфиденциальной информации или нарушить работу критически важной инфраструктуры. В условиях растущих угроз традиционные средства информационной безопасности уже не справляются с задачами своевременного обнаружения и предотвращения атак. Необходимо введение новых инструментов для анализа большого количества данных, выявления аномалий и реагирования на инциденты безопасности. В условиях, когда искусственный интеллект становится неотъемлемой частью цифровой трансформации, особенно актуально рассмотреть его роль в обеспечении Информационной безопасности в медицинских учреждениях.

Медицинские учреждения обрабатывают такие данные как: персональные сведения пациентов, медицинские диагнозы, результаты анализов, биометрические данные и даже генетическую информацию. Утечка такой информации может привести не только к финансовым потерям, но и к серьёзным репутационным и юридическим последствиям. Больницы, поликлиники и другие медицинские учреждения, работающие с персональными данными, обязаны обеспечить защиту информацию от несанкционированного доступ, согласно федеральному закону от 27 июля 2006 года № 152-ФЗ "О персональных данных" [1].

Современные угрозы в киберпространстве становятся всё более сложными, целенаправленными и быстро развивающимися. В таких условиях традиционные средства защиты уже не справляются с задачами своевременного обнаружения и реагирования на инциденты. Искусственный интеллект и машинное обучение становятся важными инструментами в арсенале информационной безопасности, особенно в критически важных отраслях, таких как здравоохранение.

ИИ существует уже давно, и с момента зарождения этой концепции прошло много времени, в ходе которого программы со способностью к обучению претерпели множество изменений, в ходе которых и был достигнут определённый уровень. На сегодняшний день искусственный интеллект может решать огромный спектр задач, что способны закрывать сегодняшние потребности, с возможностью и дальнейшего прогнозирования будущего порядка дел в этой сфере.

От искусственного интеллекта потребуется обработка огромного количества информации, мониторинг событий, анализ и адаптация к новым типам угроз. Все эти механизмы обеспечивают ряд значительных преимуществ: повышается точность обнаружения угроз за счёт анализа аномалий и поведенческих отклонений, снижается количество ложных срабатываний, обеспечивается адаптация к новым и ранее неизвестным типам атак без необходимости ручного обновления сигнатур, ускоряется выявление и реагирование на инциденты, автоматизируется обработка больших объёмов событий безопасности, а также улучшается выявление внутренних угроз и злоупотреблений доступом.

Искусственный интеллект используется и сейчас в информационной безопасности во всё мире, например, системы обнаружения и предотвращения вторжений (IDS/IPS) могут использовать алгоритмы машинного обучения [2] для анализа сетевого трафика, выявляя аномальные паттерны, которые указывают на потенциальные атаки, такие как атаки нулевого дня. SIEM-системы, интегрированные с искусственным интеллектом [3], способны автоматически фильтровать и приоритизировать события безопасности, обнаруживая сложные цепочки атак, что значительно ускоряет реагирование на инциденты. В области поведенческого анализа пользователей (UEBA) искусственный интеллект может отслеживать действия сотрудников, выявляя подозрительные отклонения от нормального поведения, что помогает предотвратить внутренние угрозы. Антивирусные решения и EDR-системы с элементами искусственного интеллекта могут распознавать новые виды вредоносного ПО на основе их поведения, мгновенно реагируя на подозрительную активность.

В России применение искусственного интеллекта в сфере информационной безопасности медицинских учреждений пока находится на начальной стадии [4], однако уже появляются успешные примеры, демонстрирующие потенциал таких технологий. Один из наиболее показательных случаев — пилотный проект, реализованный в одной из крупных федеральных клиник. В рамках этого проекта была внедрена система на базе искусственного интеллекта, предназначенная для анализа логов доступа к медицинским информационным системам,

включая электронные медицинские карты, базы данных пациентов и внутренние сервисы.

Система использовала алгоритмы машинного обучения для построения профилей нормального поведения пользователей — врачей, медсестёр, администраторов и технического персонала. На основе этих профилей искусственный интеллект отслеживал отклонения от привычных паттернов, например, доступ к данным пациентов в нерабочее время, попытки входа с необычных устройств или IP-адресов, а также частые запросы к чувствительной информации без явной медицинской необходимости.

В результате работы системы было выявлено несколько инцидентов, которые ранее могли бы остаться незамеченными. В частности, искусственный интеллект зафиксировал попытки входа в систему с учётных записей сотрудников, находящихся в отпуске, а также случаи, когда один и тот же пользователь пытался получить доступ к медицинским данным большого количества пациентов, не связанных между собой. Эти действия были оперативно переданы службе информационной безопасности, что позволило своевременно заблокировать подозрительную активность и предотвратить возможные утечки персональных данных.

Таким образом, данный проект продемонстрировал, что даже на раннем этапе внедрения искусственного интеллекта возможно значительно повысить уровень защищённости медицинских информационных систем, выявляя как внешние, так и внутренние угрозы, и это может стать основой для масштабирования подобных решений в других учреждениях здравоохранения по всей стране.

Масштабирование применения искусственного интеллекта в информационной безопасности медицинских учреждений стратегически важный шаг, а не просто технологический тренд. С ростом цифровизации здравоохранения усиливаются и требования к защите персональных данных. Масштабирование искусственного интеллекта помогает медицинским учреждениям соответствовать требованиям законодательства (например, ФЗ-152 «О персональных данных», приказам Минздрава и ФСТЭК), а также международным стандартам (ISO/IEC 27001, HIPAA и др.), обеспечивая автоматизированный контроль доступа, аудит действий пользователей и защиту каналов передачи данных.

Так же масштабирование искусственного интеллекта в информационной безопасности даёт возможность создать централизованную, взаимосвязанную систему защиты, в которой данные и сигналы об угрозах поступают из разных учреждений, обрабатываются в едином аналитическом центре и используются для обучения моделей искусственного интеллекта. Это позволяет не только защищать отдельные учреждения, но и формировать коллективный иммунитет всей системы здравоохранения, оперативно реагируя на новые типы атак и распространяя обновления и рекомендации по всей сети. В условиях дефицита квалифицированных специалистов по информационной безопасности, особенно в регионах, искусственный интеллект может взять на себя рутинные и трудоёмкие задачи: фильтрацию событий, корреляцию инцидентов, первичный анализ угроз.

Масштабирование искусственного интеллекта позволяет перераспределить ресурсы, сосредоточив внимание специалистов на стратегических задачах, а не на ручной обработке инцидентов.

Во время интеграции искусственного интеллекта определённо возникнут трудности, к которым надо быть готовым. Многие больницы и поликлиники до сих пор используют устаревшие программные и аппаратные решения, которые не поддерживают современные стандарты безопасности и не имеют возможности для масштабируемой интеграции с ИИ-системами. Такие системы часто построены на закрытых архитектурах, не поддерживают API-интерфейсы и не обеспечивают необходимый уровень совместимости с новыми технологиями. В результате внедрение искусственного интеллекта требует не только установки новых программных решений, но и полной модернизации инфраструктуры, что влечёт за собой значительные затраты времени, ресурсов и организационных усилий. Кроме того, в условиях непрерывной работы медицинских учреждений крайне сложно проводить масштабные ИТ-обновления без риска сбоев в оказании медицинской помощи.

Одной из ключевых проблем масштабирования искусственного интеллекта в информационной безопасности в медицинских учреждениях является высокая стоимость таких решений и острая нехватка квалифицированных специалистов. Разработка, внедрение и сопровождение ИИ-систем требует участия экспертов в данной области, машинного обучения, анализа данных и специфики медицинской отрасли. Однако на рынке труда наблюдается дефицит таких специалистов, особенно в регионах, где уровень цифровой зрелости медицинских учреждений остаётся низким. Даже при наличии готовых решений, их эффективное использование требует постоянного обучения персонала, настройки моделей, анализа результатов и адаптации под конкретные условия учреждения. Всё это увеличивает стоимость владения ИИ-системами, делая их недоступными для многих малобюджетных и региональных организаций здравоохранения, которые и без того испытывают финансовые трудности.

Не менее важными являются этические и правовые риски [5]. Когда искусственный интеллект принимает решения, влияющие на доступ к медицинским данным, блокировку пользователей или реагирование на инциденты, возникает вопрос ответственности: кто будет нести юридические последствия в случае ошибки алгоритма? Например, если искусственный интеллект заблокирует доступ врачу к системе в критический момент или, наоборот, не распознает утечку данных, последствия могут быть крайне серьёзными. Кроме того, алгоритмы искусственного интеллекта часто работают как «чёрные ящики», и их решения сложно объяснить или оспорить, что противоречит принципам прозрачности и подотчётности. Всё это требует разработки чётких нормативных актов, этических стандартов и механизмов контроля, которые пока находятся на стадии формирования.

С учетом быстрого развития технологий и появления новых киберугроз, развитие искусственного интеллекта в области информационной безопасности становится стратегически важным направлением. Эффективная защита здоровья

и жизни людей требует не только усовершенствования существующих систем, но и создания инновационных решений, способных адаптироваться к меняющимся условиям и угрозам. Инвестиции в развитие искусственного интеллекта в информационной безопасности могут значительно повысить уровень защиты данных и доверие пациентов к медицинским учреждениям, что в конечном итоге скажется на качестве оказания медицинской помощи.

Список источников

1. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» // Собрание законодательства Российской Федерации. 2006. № 31. Ст. 3451.
2. Интегрированная IDS/IPS модель. URL: <https://apni.ru/article/152-integrirovannaya-idsips-model-mezhdu-otkritim> (дата обращения: 18.04.2025).
3. Новые технологии в области кибербезопасности // Appercase. URL: <https://www.appercase.ru/news/63776/> (дата обращения: 18.04.2025).
4. Обзор российских систем искусственного интеллекта для здравоохранения // Webiomed. URL: <https://webiomed.ru/blog/obzor-rossiiskikh-sistem-iskusstvennogo-intellekta-dlia-zdravookhraneniia/> (дата обращения: 18.04.2025).
5. Этические проблемы развития технологий искусственного интеллекта в здравоохранении // CyberLeninka. URL: <https://cyberleninka.ru/article/n/eticheskie-problemy-razvitiya-tehnologiy-iskusstvennogo-intellekta-v-zdravookhraneni> (дата обращения: 18.04.2025).

Статья поступила в редакцию 20.04.2025; принята к публикации 10.05.2025

Информация об авторах

Медведева И.Ю. - студент кафедры «Системы информационной безопасности», направление подготовки 10.05.03 – Информационная безопасность автоматизированных систем ФГБОУ ВО «БГТУ».

Седаков К.А. - ассистент кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Вклад авторов

Медведева И.Ю. - идея, сбор материала, обработка материала, частичное написание статьи (50%).

Седаков К.А. - написание статьи, научное редактирование текста (50%).

Конфликт интересов отсутствует.

СЕКЦИЯ 7. ПРОТИВОДЕЙСТВИЕ ЭКСТРЕМИЗМУ И ТЕРРОРИЗМУ В ИНФОРМАЦИОННОЙ МОЛОДЕЖНОЙ СРЕДЕ

Научная статья

УДК 004

Поиск и эксплуатация уязвимостей с использованием Metasploit Framework

Павел Александрович Аверин ^{1✉}, Дарья Дмитриевна Бутузова ²,
Сергей Игоревич Коновалов ³, Алина Михайловна Шапенская ⁴

^{1,2,3,4} Брянский государственный технический университет, Брянск, Россия

¹ stopnotwont@gmail.com [✉], <https://orcid.org/0009-0003-5074-7217>

² enikeevadara9@gmail.com, <http://orcid.org/0009-0000-1789-7297>

³ velvet1way@gmail.com, <https://orcid.org/0009-0008-5867-635X>

⁴ alinashapenskaya@yandex.ru, <https://orcid.org/0009-0007-8434-5848>

Аннотация. В статье рассмотрена платформа Metasploit Framework для эксплуатации уязвимостей, указаны основные определения при работе с фреймворком, выделены основные этапы проведения тестирования на проникновение с помощью Metasploit Framework.

Ключевые слова: тестирование на проникновение, уязвимость, эксплоит, Metasploit Framework.

Для цитирования: Аверин П.А., Бутузова Д.Д., Коновалов С.И., Шапенская А.М. Поиск и эксплуатация уязвимостей с использованием Metasploit Framework // Противодействие экстремизму и терроризму в информационной молодежной среде: сборник докладов I межрегиональной научно-практической конференции. – Брянск: БГТУ, 2025. – С. 316 – 320.

В связи с высокой опасностью киберугроз, которым подвержены крупные компании, средние и малые предприятия, специалистам ИБ следует особое внимание уделить сфере поиска и эксплуатации уязвимостей. Хакеры и злоумышленники располагают множеством автоматизированных инструментов для взлома, поэтому пользователям информационной системы нужно искать действенные способы для убеждения в том, что сеть защищена. Одним из таких способов является тестирование на проникновение.

Статистика третьего квартала 2024 года свидетельствует о продолжающемся росте числа зарегистрированных уязвимостей по сравнению с аналогичным периодом прошлого года. В 2023 году было зафиксировано 6529 уязвимостей, из них 275 критических, тогда как в 2024 году этот показатель увеличился до 7977 уязвимостей, из которых 335 признаны критическими [1]. В отчёте «Эксплойты и уязвимости в третьем квартале 2024 года» от «Лаборатории Касперского» также подчёркивается данный тренд: за первые три квартала 2024 года количество выявленных уязвимостей достигло почти 80% от общего показателя за весь 2023 год, что подтверждает значительный рост (см. рис. 1).

Одним из примеров серьёзных киберинцидентов в третьем квартале 2024 года стала DDoS-атака на инфраструктуру «Ростелекома». Специалисты компании отразили более 1 300 кибератак, среди которых наиболее мощная UDP-Flood достигла пикового значения в 5 Тбит/с или 440 миллионов пакетов в секунду. Атака затронула внешние онлайн-ресурсы компании и использовала уязвимости в инфраструктуре. Этот инцидент подчёркивает необходимость усиления мер кибербезопасности, особенно в отношении защиты критически важных сетевых сервисов. Именно все эти данные указывают на увеличение числа критических уязвимостей, что требует повышенного внимания к мерам их выявления и устранения.

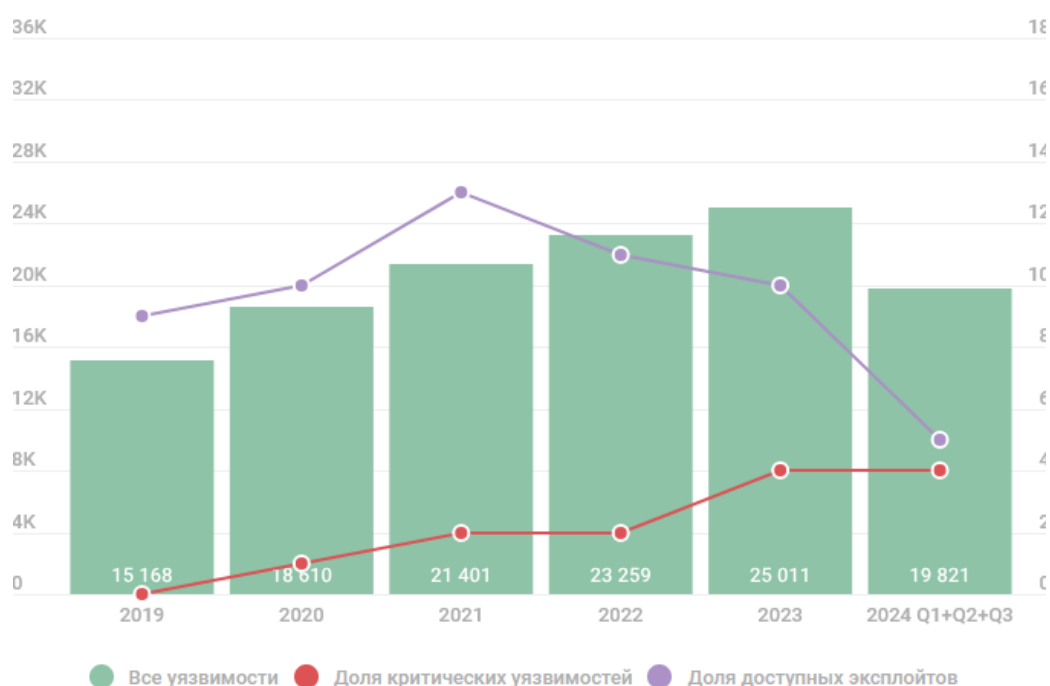


Рис. 1. Количество уязвимостей и доля среди них критических и тех, для которых существуют эксплойты, 2019–2024 гг.

Уязвимость — недостаток программного средства или информационной системы, который может быть использован для реализации угроз в информационной системе [2].

Эксплойты — это подвид вредоносных программ. Они содержат данные или исполняемый код, способный воспользоваться одной или несколькими уязвимостями в программном обеспечении на локальном или удаленном компьютере [3].

С помощью платформы для разработки и использования эксплойтов Metasploit Framework можно создать планы атак и реализовать их.

В состав фреймворка входят:

- библиотеки, основная — Rex, на ней базируются остальные (MSF Core и MSF Base);
- модули, в их числе — эксплойты, пейлоады;

- дополнительное ПО для работы, интерфейсы (по умолчанию доступ через консоль или CLI).

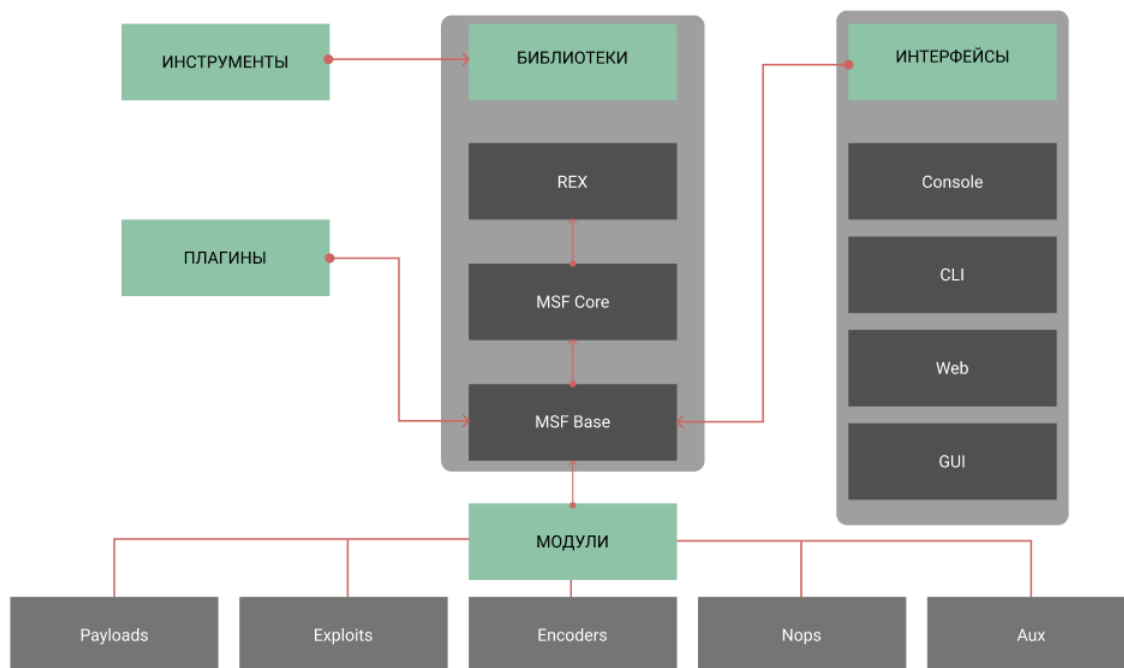


Рис. 2. Схема типичной архитектуры Metasploit

Современная версия Metasploit содержит свыше 1677 эксплойтов для более 25 платформ, включая Android, PHP, Python, Java, Cisco и другие. Фреймворк также содержит около 500 единиц информационного наполнения («пейлоад»). В Metasploit входит:

- пейлоады для командной оболочки — позволяют пользователям запускать сценарии или случайные команды на хосте;
- динамические пейлоады — позволяют тестировщикам генерировать уникальные пейлоады для обхода антивирусного программного обеспечения;
- пейлоады Meterpreter — позволяют пользователям перехватывать управление монитором устройства с помощью контроллера видеопамати, захватывать сеансы, а также скачивать или загружать файлы;
- статические пейлоады — позволяют устанавливать переадресацию портов и обмен данными между сетями [5].

Проведение пентеста осуществляется за счет следующего алгоритма:

1. Сбор информации, сканирование целевой сети или хоста.
2. Поиск уязвимости.
3. Эксплуатация и проведение атак.
4. Создание отчёта.

На этапе сбора информации определяется IP-адрес целевой системы, проводится сканирование узлов, определяются имена компьютеров, обнаруживаются общедоступные сетевые папки, критичные ресурсы [3]. Сканирование портов проводится с помощью команды «db_nmap», которая позволяет сохранять результаты сканирования в базу данных. Из результатов сканирования портов

можно выяснить информацию об открытых сетевых портах, а также предположительную версию операционной системы.

Второй этап содержит поиск и выявление уязвимостей с помощью разных методов. К ним относится метод определения уязвимости по версии продукта, который предполагает поиск информации об выявленных уязвимостях версии продукта в опубликованных открытых источниках; метод анализа конфигурации предполагает проведение анализа содержимого реестра; метод фаззинга проводится с помощью ввода в web-форму различных вариантов SQL-запросов и анализа получаемых сообщений об ошибках; метод попытки эксплуатации заключается в запуске эксплойта против сетевого сервиса без предварительного анализа его соответствия данной службе. Некоторые модули эксплуатации в Metasploit Framework поддерживают метод «check», который можно использовать для определения наличия уязвимости до её эксплуатации.

На третьем этапе проводится эксплуатация уязвимостей в целевой сети, для этого используются эксплойты из раздела «exploit» Metasploit Framework. В фреймворке количество готовых к использованию эксплойтов приближается к двум тысячам. Различные эксплойты можно найти с помощью команды «search» по коду CVE (Common Vulnerabilities and Exposures — это система для идентификации и классификации уязвимостей и экспозиций (выявленных угроз) в программном обеспечении и аппаратных системах), названию или версии сервиса. При эксплуатации уязвимости используется полезная нагрузка (payload). Это понятие подразумевает под собой код, который запускается на скомпрометированной машине. В Metasploit Framework имеются различные полезные нагрузки: удаленная командная строка, создание учетной записи, загрузка системы удаленного администрирования. На четвертом этапе происходит разработка отчёта, в котором указывается информация о названии уязвимости, скриншоты и журналы, демонстрирующие эксплуатацию уязвимости, происходит разработка перечня рисков, к которым может привести эксплуатация уязвимости, создание рекомендаций по устранению уязвимостей за счёт технического и организационного подхода.

Подводя итог Metasploit Framework — это мощнейший инструмент, который могут использовать как киберпреступники, так и «белые хакеры» и специалисты по проникновению для исследования уязвимостей в сетях и на серверах. Поскольку это фреймворк с открытым исходным кодом, его можно легко настроить и использовать на большинстве операционных систем.

Metasploit Framework является полезным средством, с помощью которого специалисты ИБ могут провести всестороннее тестирование на проникновение, создать или использовать готовые эксплойты, провести эксплуатацию уязвимостей и выявить необходимые для защиты предприятия меры.

Список источников

1. Анализ ландшафта уязвимостей в третьем квартале 2024 года // Securelist. URL: securelist.ru (дата обращения: 13.02.2025).

2. Ростелеком отразил более 1 300 кибератак в третьем квартале 2024 года // arbuztoday. URL: https://arbuztoday.ru/rostelekom-otrazil-bolee-1-300-kiberatak-v-tretem-kvartale-2024-goda/?utm_source=chatgpt.com (дата обращения: 23.03.2025).

3. Что такое эксплойты и почему их все так боятся? // kaspersky. URL: <https://www.kaspersky.ru/blog/exploits-problem-explanation/8459/> (дата обращения: 23.03.2025).

4. ГОСТ Р 56545-2015. Защита информации. Уязвимости информационных систем. Правила описания уязвимостей.

5. Масалков А.С. Особенности киберпреступлений в России: инструменты нападения и защита информации. – М.: ДМК Пресс, 2018. – С. 136-144.

6. Черепов А. А. Обзор современных инструментов для проведения пентеста на объекте / А. А. Черепов, А. А. Рябцев, А. И. Банников // Цифровой регион: опыт, компетенции, проекты : сборник трудов V Юбилейной международной научно-практической конференции, Брянск, 25 ноября 2022 года. – Брянск: Брянский государственный инженерно-технологический университет, 2023. – С. 965-969.

Статья поступила в редакцию 19.04.2025; принята к публикации 10.05.2025

Информация об авторах

Аверин П.А. – студент кафедры «Системы информационной безопасности», направление подготовки 10.05.03 - Информационная безопасность автоматизированных систем ФГБОУ ВО «БГТУ».

Бутузова Д.Д. – студент кафедры «Системы информационной безопасности», направление подготовки 10.03.01 - Информационная безопасность ФГБОУ ВО «БГТУ».

Коновалов С.И. – студент кафедры «Системы информационной безопасности», направление подготовки 10.05.03 - Информационная безопасность автоматизированных систем ФГБОУ ВО «БГТУ».

Шапенская А.М. – ассистент кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Вклад авторов

Аверин П.А. – идея, обработка материала, частичное написание статьи.

Бутузова Д.Д. – сбор материала, обработка материала, частичное написание статьи.

Коновалов С.И. – сбор материала, обработка материала, частичное написание статьи.

Шапенская А.М. – научное редактирование, доработка текста.

Конфликт интересов отсутствует.

Научная статья
УДК 378:004

Анализ процесса постэксплуатации в Linux

Павел Александрович Аверин ^{1✉}, Андрей Андреевич Диво ²,
Сергей Игоревич Коновалов ³, Алина Михайловна Шапенская ⁴
^{1, 2, 3, 4}Брянский государственный технический университет, Брянск, Россия
¹ stopnotwont@gmail.com ✉, <https://orcid.org/0009-0003-5074-7217>
² divo_2003@mail.ru, <https://orcid.org/0009-0006-1527-8744>
³ velvet1way@gmail.com, <https://orcid.org/0009-0008-5867-635X>
⁴ alinashapenskaya@yandex.ru, <https://orcid.org/0009-0007-8434-5848>

Аннотация. Современные тенденции в области кибербезопасности свидетельствуют о существенном росте числа атак, нацеленных на системы на базе операционной системы Linux. Особую значимость приобретает этап постэксплуатации, на котором злоумышленник, получив первоначальный доступ, осуществляет закрепление в системе, расширение прав и сбор конфиденциальной информации. В статье рассматриваются наиболее характерные векторы атак, выявленные в 2024 году, включая использование известных уязвимостей программного обеспечения и эксплуатацию недостаточной осведомленности конечных пользователей и системных администраторов. Приведён обзор актуальных инструментов постэксплуатации, таких как Metasploit Framework, Empire и PowerSploit. Особое внимание уделено механизмам защиты, реализуемым с помощью систем принудительного контроля доступа и средств мониторинга поведения приложений. Подчёркивается необходимость автоматизации процессов анализа событий безопасности и совершенствования профессиональной подготовки специалистов, работающих с Linux-инфраструктурами.

Ключевые слова: постэксплуатация, Linux, эксплуатация уязвимостей, киберугрозы, повышение привилегий, Metasploit Framework, Empire, PowerSploit, безопасность информационных систем, SELinux, AppArmor, Falco.

Для цитирования: Аверин П.А., Диво А.А., Коновалов С.И., Шапенская А.М. Анализ процесса постэксплуатации в Linux // Актуальные проблемы кибербезопасности. Противодействие экстремизму и терроризму в информационной молодежной среде: сборник докладов I межрегиональной научно-практической конференции. – Брянск: БГТУ, 2025. – С. 321 – 324.

Операционные системы на базе ядра Linux традиционно считаются устойчивыми и безопасными благодаря открытому исходному коду, модульной архитектуре и активному сообществу разработчиков. Однако эти преимущества не освобождают систему от внимания со стороны киберпреступников, особенно на этапах, следующих за первоначальным вторжением. Пост-эксплуатационная фаза представляет собой критически важный период, в рамках которого атакующий стремится закрепиться в системе, получить расширенные привилегии и получить доступ к конфиденциальной информации, оставаясь при этом незамеченным.

Согласно аналитическим данным, предоставленным «Лабораторией Касперского», в первом квартале 2024 года наблюдалось увеличение атак на Linux-

окружения почти на 130% по сравнению с аналогичным периодом 2023 года. Подавляющее большинство атак реализовывалось с использованием эксплойтов для уже известных уязвимостей, что в значительной степени обусловлено применением устаревших версий программного обеспечения, отсутствием своевременных обновлений и некорректной настройкой систем безопасности. Прогнозы на текущий год демонстрируют устойчивую тенденцию к ежемесячному приросту новых уязвимостей примерно на 25%, что соответствует появлению более двух с половиной тысяч новых потенциальных точек компрометации ежемесячно.

Невысокий уровень информационной грамотности системных администраторов и конечных пользователей способствует тому, что киберпреступники без труда используют тривиальные векторы атак, не требующие значительных вычислительных ресурсов. Проблема усугубляется отсутствием единых методических рекомендаций по безопасной конфигурации Linux-сред, а также недостаточным вниманием к внедрению стандартов информационной безопасности на уровне организаций.

Наиболее широко используемыми средствами пост-эксплуатации в 2024 году стали платформы, ориентированные на удалённое управление и эскалацию привилегий в скомпрометированных системах. Среди них выделяются инструменты, предоставляющие возможность автоматического выполнения команд, управления учётными записями и загрузки вредоносных компонентов. Программные комплексы, такие как Metasploit Framework, позволяют не только развивать успешную атаку, но и организовывать долговременное присутствие в системе. Empire, как система командного управления, ориентирована на скрытное взаимодействие с заражённой системой, обеспечивая сбор системной информации и координацию дальнейших действий. Набор модулей PowerSploit, использующий возможности PowerShell, активно применяется для обхода защитных механизмов, извлечения учётных данных и организации устойчивого канала доступа.

Одной из наиболее опасных задач пост-эксплуатации является повышение привилегий, обеспечивающее атакующему полный контроль над операционной системой. Уязвимости, связанные с обработкой системной памяти, нарушением работы с буферами и недостаточной валидацией входных данных, часто становятся основой для подобных атак. Наиболее показательным примером является уязвимость CVE-2016-5195, также известная как Dirty COW, позволявшая пользователям производить несанкционированные записи в защищённые области памяти, фактически получая root-доступ без авторизации.

Долговременное сохранение присутствия в системе также представляет серьёзную угрозу. Злоумышленники стремятся внедрять скрытые каналы связи, осуществлять модификацию конфигурационных файлов, изменять параметры системы авторизации, включая настройки iptables или содержимое файла /etc/sudoers. Эти действия позволяют злоумышленнику вновь подключаться к системе без повторного взлома, что значительно осложняет процессы обнаружения и расследования инцидентов.

Дополнительную угрозу представляет активное извлечение системной и пользовательской информации. На пост-эксплуатационном этапе собираются сведения о версии ядра, перечне установленных пакетов, конфигурации сетевых интерфейсов, а также учетные данные, криптографические ключи и другие элементы, критически важные с точки зрения обеспечения конфиденциальности.

Современные подходы к защите Linux-систем предполагают реализацию многоуровневой модели безопасности. Использование систем принудительного контроля доступа позволяет значительно ограничить действия даже тех процессов, которые обладают повышенными привилегиями. SELinux, внедрённый в корпоративных дистрибутивах, позволяет гибко управлять разрешениями на уровне взаимодействия между субъектами и объектами, что минимизирует последствия компрометации. Альтернативный подход реализуется с помощью AppArmor, ориентированного на более простое развертывание и управление политиками, что особенно актуально в дистрибутивах с широкой пользовательской базой.

Перспективным направлением является мониторинг поведения процессов с последующей корреляцией событий в системах информационной безопасности. Примером такой реализации выступает Falco — инструмент, способный в реальном времени отслеживать системные вызовы и сигнализировать об отклонениях от заданных шаблонов поведения. Интеграция с существующими SIEM-платформами позволяет создавать автоматические правила реагирования и снижать время обнаружения инцидентов.

Несмотря на наличие перечисленных средств защиты, пост-эксплуатация продолжает представлять собой серьёзную проблему. Противодействие ей требует внедрения механизмов автоматизированного анализа журналов событий, усиления взаимодействия между компонентами инфраструктуры безопасности и развития кадрового потенциала. Вопросы подготовки и сертификации специалистов, ориентированных на администрирование и защиту Linux-сред, должны рассматриваться как приоритетные при построении устойчивой архитектуры кибербезопасности. Успешное решение этих задач возможно только при взаимодействии государства, образовательных учреждений и частного сектора.

Пост-эксплуатационная деятельность злоумышленников в Linux-среде остается одной из наиболее актуальных угроз в современной киберсреде. Несмотря на прогресс в развитии защитных технологий, устойчивость систем в значительной степени определяется уровнем их конфигурации, своевременностью обновлений и профессионализмом обслуживающего персонала. Комплексный подход к безопасности, сочетающий технические средства, мониторинг и непрерывное обучение, является основой эффективного противодействия угрозам, возникающим на поздних стадиях компьютерных атак.

Список источников

1. Постэксплуатация Linux в практике пентеста // OTUS. URL: <https://otus.ru/nest/post/1079/> (дата обращения: 9.02.2025).

2. Постэксплуатация Linux. Поднимаемся от юзера до бога в несколько кликов. URL: <https://xakep.ru/2019/02/18/linux-killchain/> (дата обращения: 9.02.2025).
3. SELinux – описание и особенности работы с системой. URL: <https://habr.com/ru/companies/kingservers/articles/209644/> (дата обращения: 9.02.2025).
4. Безопасный Linux вместе с AppArmor. URL: <https://habr.com/ru/companies/ruvds/articles/532988/> (дата обращения: 9.02.2025).
5. Linux-сафари с Falco: как поймать атакующих за хвост. URL: <https://rt-solar.ru/solar-4rays/blog/4937/> (дата обращения: 9.02.2025).

Статья поступила в редакцию 19.04.2025; принята к публикации 10.05.2025

Информация об авторах

Аверин П.А. – студент кафедры «Системы информационной безопасности», направление подготовки 10.05.03- Информационная безопасность автоматизированных систем ФГБОУ ВО «БГТУ».

Диво А.А. – студент кафедры «Системы информационной безопасности», направление подготовки 10.05.03 - Информационная безопасность автоматизированных систем ФГБОУ ВО «БГТУ».

Коновалов С.И. – студент кафедры «Системы информационной безопасности», направление подготовки 10.05.03 - Информационная безопасность автоматизированных систем ФГБОУ ВО «БГТУ».

Шапенская А.М. – ассистент кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Вклад авторов

Аверин П.А. – идея, обработка материала, частичное написание статьи (25%).

Диво А.А. – сбор материала, обработка материала, частичное написание статьи (25%).

Коновалов С.И. – сбор материала, обработка материала, частичное написание статьи (25%).

Шапенская А.М. – научное редактирование, доработка текста (25%).

Конфликт интересов отсутствует.

Научная статья
УДК 004

Анализ атак на беспроводные сети Wi-Fi с применением техник MitM и DoS/DDoS

Павел Александрович Аверин ^{1✉}, Сергей Игоревич Коновалов ²,
Алина Михайловна Шапенская ³

^{1,2,3}Брянский государственный технический университет, Брянск, Россия

¹stopnotwont@gmail.com✉, <https://orcid.org/0009-0003-5074-7217>

²velvet1way@gmail.com, <https://orcid.org/0009-0008-5867-635X>

³alinashapenskaya@yandex.ru, <https://orcid.org/0009-0007-8434-5848>

Аннотация. Статья посвящена вопросам безопасности Wi-Fi-сетей, анализу современных протоколов аутентификации (WEP, WPA, WPA2, WPA3) и методам защиты от различных видов атак, таких как man-in-the-middle и DDoS. Рассматриваются особенности каждого из протоколов, их уязвимости и способы защиты. Особое внимание уделено методам предотвращения DDoS-атак и важности использования облачных услуг для защиты от сетевых угроз, что позволяет минимизировать риски для бизнеса.

Ключевые слова: Wi-Fi безопасность, протоколы аутентификации, WEP, WPA, WPA2, WPA3, атака man-in-the-middle, DDoS-атаки, защита от атак, фильтрация трафика, облачные услуги, киберугрозы.

Для цитирования: Аверин П.А., Коновалов С.И., Шапенская А.М. Анализ атак на беспроводные сети Wi-Fi с применением техник MitM и DoS/DDoS // Актуальные проблемы кибербезопасности. Противодействие экстремизму и терроризму в информационной молодежной среде: сборник докладов I межрегиональной научно-практической конференции. – Брянск: БГТУ, 2025. – С. 325 – 329.

Беспроводные сети Wi-Fi обеспечивают удобный доступ к интернету без необходимости физического подключения, однако вместе с этим повышается вероятность компрометации передаваемой информации. Передача данных по радиоканалу делает возможным их перехват или модификацию злоумышленниками, что обуславливает высокий уровень риска использования данной технологии.

С течением времени в рамках Wi-Fi были внедрены различные протоколы аутентификации, включая WEP, WPA, WPA2 и WPA3. Каждый из них характеризуется специфическим набором параметров, необходимым для успешной аутентификации, а также различным уровнем криптографической устойчивости. Сравнительный анализ протоколов приведен в табл. 1.

Таблица 1

Сравнение протоколов

	WEP	WPA	WPA2	WPA3
Режимы	WEP-OPEN WEP-Shared	WPA-PSK WPA-Enterprise	WPA2-PSK WPA2-Enterprise	WPA3-Personal WPA3-Enterprise
Алгоритм шифрования	RC4	TKIP	AES-CCMP	AES-CCMP AES-GCMP
Размер ключа	64/128	128	128	128/256
Считается устаревшим	С 2004	С 2012	Актуален	Актуален

Протокол WEP (Wired Equivalent Privacy) применяет алгоритм RC4 и ключи длиной 64 или 128 бит. С 2004 года признан устаревшим вследствие уязвимостей, связанных с генерацией ключей и низкой устойчивостью к статистическим атакам. Его взлом возможен с использованием FMS/KoreK-методик и инъекции ARP-пакетов, что позволяет восстанавливать ключи посредством анализа перехваченного трафика. Для реализации подобных атак активно используется пакет aircrack-ng.

WPA (Wi-Fi Protected Access), использующий шифрование TKIP, на момент появления предлагал более высокий уровень безопасности по сравнению с WEP. Однако с 2012 года считается уязвимым ввиду возможности проведения атак на PSK (предварительно заданный ключ) методом словарного перебора, а также из-за наличия уязвимости Michael, позволяющей модифицировать пакеты. Взлом возможен посредством перехвата процесса аутентификации (Handshake) с последующим офлайн-анализом при помощи инструментов, таких как hashcat.

WPA2, использующий AES-CCMP, на сегодняшний день остается широко применяемым стандартом. Тем не менее, он подвержен атакам в случае использования слабых паролей. Наиболее распространённой является атака на перехваченный Handshake. В 2017 году была выявлена уязвимость KRACK, позволяющая получить доступ к трафику, однако для её реализации требуется физическое присутствие в зоне действия сети.

WPA3 представляет собой современный стандарт, в котором реализована схема SAE (Simultaneous Authentication of Equals), обеспечивающая устойчивость к оффлайн-подбору паролей. Несмотря на выявленные уязвимости, такие как Dragonblood, WPA3 в настоящее время признан наиболее безопасным протоколом для защиты беспроводных сетей.

Одной из наиболее распространённых и опасных категорий атак на Wi-Fi-сети являются атаки посредника (Man-in-the-Middle, MitM). Вторую по значимости угрозу составляют атаки отказа в обслуживании (DoS/DDoS). Ниже представлены характеристики данных атак.

MitM-атака представляет собой вмешательство злоумышленника в процесс взаимодействия между двумя легитимными сторонами (пользователями, приложениями или устройствами). Цель таких атак — несанкционированный до-

ступ к передаваемым данным с возможностью их перехвата, изменения или удаления. Наиболее уязвимыми являются аутентификационные данные, финансовая информация, а также другие конфиденциальные сведения, которые впоследствии могут быть использованы в преступных целях.

Для успешной реализации MitM-атаки злоумышленник, как правило, создает поддельную точку доступа Wi-Fi, не требующую пароля для подключения. Подключившись к такой сети, пользователь фактически передает свои данные напрямую атакующему. Получив доступ к трафику, злоумышленник может применить следующие методы дешифровки и подмены:

- Подмена HTTPS – создание ложного сертификата безопасности для веб-сайта, в результате чего браузер не распознает подделку;
- SSL-перехват – вмешательство в процесс перенаправления с HTTP на HTTPS, позволяющее перехватывать передаваемую информацию;
- SSL Stripping – понижение уровня соединения до незащищённого HTTP-протокола, что делает трафик уязвимым для анализа.

Для снижения риска подобных атак необходимо избегать использования открытых сетей, использовать VPN-сервисы, завершать сессии после работы с важными ресурсами, применять менеджеры паролей и двухфакторную аутентификацию, а также обеспечить защиту конечных устройств с помощью антивирусного ПО и межсетевых экранов.

Атаки отказа в обслуживании (Denial of Service, DoS) направлены на выведение из строя сетевых сервисов путем их перегрузки. В случае DoS-атак инициатором выступает одно устройство, тогда как при DDoS-атаках (Distributed Denial of Service) используется распределенная сеть заражённых узлов (ботнет), что многократно увеличивает мощность воздействия и затрудняет идентификацию источника.

DoS-атаки, как правило, обладают ограниченной эффективностью из-за использования единственного IP-адреса. DDoS-атаки представляют значительно большую угрозу и могут быть направлены как на серверные мощности организаций, так и на сторонние сервисы, обеспечивающие работу приложений, хранилищ и других ИТ-компонентов.

Принцип DDoS-атаки заключается в генерации большого количества фиктивных запросов к целевому серверу, что приводит к истощению его ресурсов и потере доступности. Атаки могут быть реализованы на различных уровнях модели OSI/ISO, которая подразделяется на семь уровней.

Низкоуровневые атаки (1–4 уровни OSI):

- Физический уровень — реализуются посредством физического воздействия на оборудование или помех в радиоканале (например, Wi-Fi);
- Канальный уровень — включают вмешательство в работу коммутаторов и концентраторов;
- Сетевой уровень — используют протокол IP; распространённые атаки: Ping Flood, Smurf, Ping of Death;
- Транспортный уровень — направлены на исчерпание ресурсов путем эксплуатации TCP/UDP-соединений.

Высокоуровневые атаки (5–7 уровни OSI):

- Сеансовый уровень — целенаправленное нарушение связи между приложениями (например, протокол SMPP);
- Уровень представления — воздействие на формат и кодировку данных с целью их повреждения;
- Прикладной уровень — вмешательство в работу приложений с возможностью кражи, подмены или разрушения данных.

Высокоуровневые атаки особенно опасны для организаций, поскольку направлены не только на нарушение доступности, но и на компрометацию данных, что может привести к прямым убыткам.

Эффективная защита от DoS/DDoS требует значительных вычислительных ресурсов и внедрения эвристических механизмов анализа трафика. В большинстве случаев целесообразно использовать подписные сервисы по фильтрации трафика, предоставляемые операторами связи и облачными платформами, обладающими необходимой экспертизой и инфраструктурой.

Безопасность беспроводных сетей Wi-Fi представляет собой важнейшее направление в области защиты информации. Несмотря на развитие стандартов аутентификации и шифрования, сохраняется высокий уровень угроз, обусловленный применением таких атак, как MitM и DDoS. Постоянное совершенствование методов перехвата и разрушения сетевой инфраструктуры требует применения комплексных мер защиты, включая использование актуальных протоколов (WPA3), отказ от незащищённых соединений, применение VPN, а также использование облачных решений по обеспечению отказоустойчивости и фильтрации трафика. Только системный подход к защите может обеспечить надёжную работу сетей в условиях возрастания количества киберугроз.

Список источников

1. MITM-атака (атака «человек посередине») // kaspersky. URL: <https://encyclopedia.kaspersky.ru/glossary/man-in-the-middle-attack/> (дата обращения: 08.03.2025).
2. Что такое атака man-in-the-middle и ее предотвращение // cloudav. URL: <https://www.cloudav.ru/mediacenter/security/man-in-the-middle-attack/> (дата обращения: 08.03.2025).
3. Чем отличается DOS от DDOS-атаки // rusonyx. URL: <https://www.rusonyx.ru/blog/post/dos-i-ddos-ataki-kak-oni-osushchestvlyayutsya-i-kak-ne-stat-zhertvoy-napadeniya/> (дата обращения: 08.03.2025).
4. Как работает DDoS-атака // kaspersky. URL: <https://www.kaspersky.ru/resource-center/threats/ddos-attacks> (дата обращения: 08.03.2025).

Статья поступила в редакцию 19.04.2025; принята к публикации 10.05.2025

Информация об авторах

Аверин П.А. – студент кафедры «Системы информационной безопасности», направление подготовки 10.05.03 - Информационная безопасность автоматизированных систем ФГБОУ ВО «БГТУ».

Коновалов С.И. – студент кафедры «Системы информационной безопасности», направление подготовки 10.05.03 - Информационная безопасность автоматизированных систем ФГБОУ ВО «БГТУ».

Шапенская А.М. – ассистент кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Вклад авторов

Аверин П.А. – идея, обработка материала, частичное написание статьи.

Коновалов С.И. – сбор материала, обработка материала, частичное написание статьи.

Шапенская А.М. – научное редактирование, доработка текста.

Конфликт интересов отсутствует.

Научная статья
УДК 004

Применение программного обеспечения Wireshark для анализа сетевого трафика

Павел Александрович Аверин ^{1✉}, Сергей Игоревич Коновалов ²,
Алина Михайловна Шапенская ³

^{1,2,3} Брянский государственный технический университет, Брянск, Россия

¹ stopnotwont@gmail.com✉, <https://orcid.org/0009-0003-5074-7217>

² velvet1way@gmail.com, <https://orcid.org/0009-0008-5867-635X>

³ alinashapenskaya@yandex.ru, <https://orcid.org/0009-0007-8434-5848>

Аннотация. Анализ сетевого трафика представляет собой ключевой метод для выявления неполадок в функционировании сетевой инфраструктуры, диагностики инцидентов информационной безопасности и обеспечения контроля за состоянием корпоративных сетей. В статье изложены теоретические основы анализа трафика, рассмотрено его значение в контексте обеспечения кибербезопасности, а также приведён обзор наиболее распространённых программных решений, включая Wireshark, Tcpdump, Kismet, EtherApe и SolarWinds Network Bandwidth Analyzer. Особое внимание уделено функциональным возможностям Wireshark — одного из наиболее мощных инструментов для перехвата и анализа сетевых пакетов, поддерживающего свыше 2000 протоколов. Описаны базовые приёмы работы с программой, включая применение фильтров, поиск по содержимому пакетов и маркировку данных. Материал предназначен для специалистов в области сетевой безопасности, системных администраторов и иных профессионалов, осуществляющих мониторинг и анализ сетевого взаимодействия.

Ключевые слова: анализ трафика, Wireshark, сетевые протоколы, безопасность сети, мониторинг трафика, фильтрация пакетов, утилиты анализа трафика.

Для цитирования: Аверин П.А., Коновалов С.И., Шапенская А.М. Применение программного обеспечения Wireshark для анализа сетевого трафика // Актуальные проблемы кибербезопасности. Противодействие экстремизму и терроризму в информационной молодежной среде: сборник докладов I межрегиональной научно-практической конференции. – Брянск: БГТУ, 2025. – С. 330 – 333.

Современные корпоративные информационные системы подвержены риску несанкционированного доступа. В условиях роста числа киберугроз важно обеспечивать своевременное выявление признаков вторжения и предпринимать меры по их нейтрализации. Эффективным инструментом для реализации данных задач выступает анализ сетевого трафика, который позволяет не только фиксировать активность потенциальных злоумышленников на ранних этапах, но и обеспечивать контроль соблюдения регламентов информационной безопасности со стороны сотрудников.

Анализ сетевого трафика представляет собой комплекс технических и программных мероприятий, направленных на перехват, интерпретацию и последующую обработку данных, передаваемых по сети. Этот процесс применяется как в целях обеспечения защиты информационных ресурсов, так и, в отдельных случаях, в противоправной деятельности [1].

Данный подход позволяет выявлять сетевые аномалии, включая задержки, потери пакетов и ошибки маршрутизации, а также детектировать возможные атаки, попытки несанкционированного доступа, утечки данных. Кроме того, анализ трафика способствует оптимизации загрузки каналов связи, контролю за соблюдением политик безопасности и обнаружению нежелательного или запрещенного сетевого взаимодействия.

Необходимость использования средств анализа трафика возникает в ситуациях, когда наблюдается проблема в функционировании сети, но установить её источник – конкретное устройство или протокол – оперативно не представляется возможным. В подобных случаях используется специализированное программное обеспечение, в том числе:

SolarWinds Network Bandwidth Analyzer — программный комплекс, включающий базовое решение Network Performance Monitor и модуль NetFlow Traffic Analyzer. Инструмент ориентирован на мониторинг производительности и анализ сетевого трафика, предлагая пользователю взаимодополняющие функциональные возможности.

Wireshark — мощный и широко применяемый инструмент, отличающийся сбалансированным сочетанием доступности исходных данных и их визуального представления. Поддерживает детальный анализ большого количества протоколов, обеспечивая высокую точность исследования сетевого трафика.

Tcpdump — инструмент командной строки, первоначально разработанный для UNIX-систем, однако также доступный на платформе Windows. Поддерживает основные функции захвата и записи сетевых пакетов.

Kismet — программное обеспечение для анализа беспроводных сетей, обладающее расширенными возможностями, включая перехват трафика от скрытых сетей и сетей без широковещательной передачи SSID.

EtherApe — аналог WireShark с акцентом на графическое представление сетевых соединений. Распространяется по модели открытого программного обеспечения и характеризуется наглядностью визуализации сетевой активности.

Особое внимание следует уделить анализатору Wireshark, поддерживающему декодирование более чем 2000 сетевых протоколов, включая:

- Ethernet (канальный уровень);
- IP и IPv6 (сетевой уровень);
- TCP, UDP, ICMP (транспортный уровень);
- HTTP, HTTPS, DNS, FTP, SSH (прикладной уровень).

Wireshark использует библиотеку pcap, ограничивающую набор поддерживаемых стандартов, однако обеспечивает интерпретацию трафика в режиме реального времени с выводом информации в удобном формате.

На практике анализ перехваченного трафика чаще всего осуществляется в офлайн-режиме. Сначала данные сохраняются в файл (дамп), после чего проводится детальное исследование. Такой подход минимизирует риск потери информации вследствие неправильной настройки фильтров или технических сбоев, а также предоставляет возможность многократного анализа одного и того же сеанса передачи данных.

Ключевые функции работы с Wireshark включают:

Поиск по пакетам (Ctrl+F): предоставляет выбор между поиском по строкам и применением фильтров отображения, что упрощает навигацию в большом объеме данных.

Отметка пакетов (Ctrl+M): позволяет визуально выделять отдельные пакеты. Переключение между помеченными элементами осуществляется с помощью комбинаций Shift+Ctrl+N (вперед) и Shift+Ctrl+B (назад).

Фильтрация трафика: дает возможность ограничить анализ заданным набором условий, что особенно актуально при работе с большими дампами для ускорения поиска и повышения точности результатов.

Наиболее эффективно изучение возможностей Wireshark происходит в условиях тестирования в пределах локальной сети. При этом важно освоить различные режимы работы сетевого адаптера: управляемый, мостовой, режим прямого подключения и мониторинговый режим. Конкретный выбор зависит от технических характеристик оборудования и задач исследования.

Анализ сетевого трафика представляет собой важнейший элемент обеспечения информационной безопасности и управления сетевой инфраструктурой. Он позволяет выявлять технические неполадки, фиксировать подозрительную активность, предотвращать утечки информации и обеспечивать оптимальную работу сетевых ресурсов.

Овладение методами сетевого анализа и практическими навыками работы с соответствующим программным обеспечением способствует повышению уровня защищенности информационных систем, минимизации последствий инцидентов и укреплению комплексной киберустойчивости организаций.

Список источников

1. Что такое анализ сетевого трафика, или Как найти потенциальный канал утечки информации? // cyberden. URL: <https://cyberden.pw/chto-takoe-analiz-setevogo-trafika> (дата обращения: 05.03.2025).
2. 8 лучших программ для анализа сетевого трафика // networkguru. URL: <https://networkguru.ru/8-luchshikh-programm-dlia-analiza-setevogo-trafika/> (дата обращения: 05.03.2025).
3. Как пользоваться Wireshark // timeweb. URL: <https://timeweb.com/ru/community/articles/rukovodstvo-po-ispolzovaniyu-wireshark> (дата обращения: 05.03.2025).
4. Анализ сетевого трафика в управлении производительностью приложений // Хабр. URL: <https://habr.com/ru/companies/prolan/articles/184048/> (дата обращения: 05.03.2025).

Статья поступила в редакцию 19.04.2025; принята к публикации 10.05.2025

Информация об авторах

Аверин П.А. – студент кафедры «Системы информационной безопасности», направление подготовки 10.05.03 - Информационная безопасность автоматизированных систем ФГБОУ ВО «БГТУ».

Коновалов С.И. – студент кафедры «Системы информационной безопасности», направление подготовки 10.05.03 - Информационная безопасность автоматизированных систем ФГБОУ ВО «БГТУ».

Шапенская А.М. – ассистент кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Вклад авторов

Аверин П.А. – идея, обработка материала, частичное написание статьи.

Коновалов С.И. – сбор материала, обработка материала, частичное написание статьи.

Шапенская А.М. – научное редактирование, доработка текста.

Конфликт интересов отсутствует.

Научная статья
УДК 004

Современные методы компрометации паролей и средства их нейтрализации

Павел Александрович Аверин ^{1✉}, Сергей Игоревич Коновалов ²,
Алина Михайловна Шапенская ³

^{1,2,3} Брянский государственный технический университет, Брянск, Россия

¹ stopnotwont@gmail.com ✉, <https://orcid.org/0009-0003-5074-7217>

² velvet1way@gmail.com, <https://orcid.org/0009-0008-5867-635X>

³ alinashapenskaya@yandex.ru, <https://orcid.org/0009-0007-8434-5848>

Аннотация. В работе рассматриваются актуальные методы компрометации паролей, их уязвимости и способы защиты от несанкционированного доступа. Анализируются подходы, применяемые при атаках методом перебора, включая словарные и брутфорс-атаки, а также использование радужных таблиц и вредоносного программного обеспечения. Особое внимание уделено роли пароля как базового средства аутентификации в информационных системах, несмотря на развитие альтернативных технологий. Предложены эффективные меры защиты, включая создание уникальных сложных паролей, применение многофакторной аутентификации, шифрование и своевременное обновление программного обеспечения.

Ключевые слова: пароль, аутентификация, безопасность, перебор, словарная атака, брутфорс, радужные таблицы, вредоносное ПО, защита информации, шифрование, MFA.

Для цитирования: Аверин П.А., Коновалов С.И., Шапенская А.М. Современные методы компрометации паролей и средства их нейтрализации // Актуальные проблемы кибербезопасности. Противодействие экстремизму и терроризму в информационной молодежной среде: сборник докладов I межрегиональной научно-практической конференции. – Брянск: БГТУ, 2025. – С. 334 – 337.

Пароли по-прежнему играют ключевую роль в обеспечении аутентификации пользователей в современных информационных системах. Несмотря на расширение применения биометрических решений и технологий многофакторной аутентификации, парольная защита остается основным механизмом контроля доступа к учетным записям. При этом широко распространены проблемы, связанные с недостаточной стойкостью паролей, их прогнозируемостью, а также нарушениями при их хранении и обработке, что способствует возникновению угроз несанкционированного доступа к конфиденциальной информации.

Методы получения доступа к учетным данным неуклонно совершенствуются в ответ на развитие технологий информационной безопасности. Наряду с традиционными техниками перебора возможных значений, применяются более сложные схемы эксплуатации уязвимостей программного и аппаратного обеспечения. Существенную опасность также представляют методы социальной инженерии, направленные на использование поведенческих особенностей пользователей с целью получения их учетных данных.

Под термином "пароль" следует понимать последовательность символов, предназначенную для ограничения доступа к персонализированным ресурсам и данным пользователя в сети. В то же время, "взлом" предполагает реализацию комплекса действий, направленных на выявление и эксплуатацию уязвимых компонентов систем с целью получения несанкционированного доступа к информации.

Одним из наиболее распространенных способов компрометации паролей остается метод перебора — последовательное тестирование различных комбинаций символов до получения правильного значения. Вариацией данной техники являются генеративные алгоритмы, создающие возможные пароли на основе шаблонов, включающих буквы, цифры и специальные символы. Также широко используются словарные атаки, основанные на применении заранее подготовленных списков часто встречающихся паролей. Программы, реализующие данный метод, автоматически сопоставляют хеши паролей с этими списками до нахождения совпадения. Эффективной мерой противодействия подобным атакам является использование уникальных, нестандартных и сложных паролей.

Таблица 1

Сколько раз распространенные пароли утекали в сеть

Пароль	Сколько раз попадал в сеть
123456	23,5 млн
123456789	7,8 млн
password	3,7 млн
12345678	2,9 млн
111111	3,1 млн
123123	2,2 млн
12345	2,3 млн

Атака методом перебора всех возможных вариантов (brute force) представляет собой процесс последовательного тестирования паролей без предварительного ограничения перечня возможных значений. В отличие от словарных атак, данный подход охватывает все допустимые комбинации символов. С увеличением длины пароля временные затраты на успешный подбор возрастают экспоненциально, что снижает эффективность метода.

Среди эффективных способов противодействия атакам грубой силы можно выделить введение ограничений на число допустимых попыток ввода, реализация уникальных паролей для каждой учетной записи, а также активация многофакторной аутентификации.

Так называемые радужные таблицы (rainbow tables) — это базы данных, содержащие предварительно рассчитанные хеши часто используемых паролей. С их помощью возможно оперативное сопоставление хешей с исходными значениями без необходимости обратного преобразования. Современные системы хранения паролей используют хеш-функции, такие как SHA-1, MD5, SHA-256 и

другие, которые преобразуют текстовые пароли в уникальные строки фиксированной длины. Например, строка «12345» при хешировании по алгоритму MD5 примет вид «827ccb0eea8a706c4c34a16891f84e7b».

Однако получение хеша не означает полной недоступности пароля, поскольку атакующий может воспользоваться радужными таблицами, содержащими хеши наиболее распространенных значений. Для повышения устойчивости к таким атакам рекомендуется добавление соли — случайного значения, соединяемого с паролем перед хешированием.

Одним из опаснейших векторов атак остается вредоносное программное обеспечение, распространяемое посредством электронной почты, мессенджеров, небезопасных веб-сайтов или сетей обмена файлами. После установки на устройство оно может выполнять функции кражи учетных данных, регистрации нажатий клавиш (кейлоггеры), удалённого управления системой и иных вредоносных операций.

Значительную угрозу также представляют уязвимые беспроводные сети. Слабозащищённые точки доступа Wi-Fi и незащищённые маршрутизаторы могут стать объектом атак, направленных на перехват трафика или проникновение в локальную сеть. Один из методов, получивший распространение, — вардрайвинг, при котором осуществляется активный поиск незащищённых беспроводных сетей.

Кроме того, злоумышленники прибегают к использованию программ, способных находить и эксплуатировать уязвимости операционных систем и сетевых протоколов. Примером может служить установка троянского программного обеспечения, открывающего скрытый доступ к системе и позволяющего похищать информацию.

Атаки на электронную почту также остаются актуальными. Несмотря на внедрение протоколов шифрования, при наличии уязвимостей в каналах передачи злоумышленники могут осуществлять перехват сообщений.

Кейлоггеры, в свою очередь, отслеживают действия пользователя на клавиатуре, что позволяет атакующим перехватывать вводимые пароли и прочую конфиденциальную информацию. Полученные данные могут передаваться на удалённые серверы злоумышленников.

Заражённые устройства, или так называемые "зомби-компьютеры", могут объединяться в ботнеты — сети управляемых машин, используемых для рассылки спама, проведения распределённых атак отказа в обслуживании (DDoS) и других противоправных действий.

Комплексная система защиты должна включать следующие меры:

- использование уникальных и сложных паролей;
- активация двух- или многофакторной аутентификации;
- ограничение числа неудачных попыток ввода;
- регулярное обновление программного обеспечения;
- применение антивирусных решений;
- защита беспроводных сетей протоколами WPA2/WPA3;
- загрузка программ исключительно из проверенных источников;
- шифрование электронной переписки;
- использование виртуальных клавиатур и фаерволов.

Соблюдение этих рекомендаций существенно снижает вероятность компрометации учетных данных и обеспечивает более высокий уровень информационной безопасности.

Несмотря на развитие альтернативных методов аутентификации, пароли остаются основным средством идентификации пользователей. Однако их использование сопряжено с рядом уязвимостей, включая слабую криптостойкость, повторяемость и ошибки в обработке. Методы атак, такие как словарные атаки, грубая сила, использование радужных таблиц и вредоносного ПО, подтверждают необходимость внедрения многоуровневой защиты. Применение уникальных паролей, многофакторной аутентификации и современных средств защиты от сетевых угроз позволяет существенно повысить безопасность информационных систем и минимизировать риски утечек данных.

Список источников

1. Что такое взлом пароля // keepersecurity. URL: <https://www.keepersecurity.com/blog/ru/2023/09/08/what-is-a-password-breach/> (дата обращения: 12.03.2025).
2. Что такое взлом и как его предотвратить? // kaspersky. URL: <https://www.kaspersky.ru/resource-center/definitions/what-is-hacking> (дата обращения: 12.03.2025).
3. Радужная таблица // kaspersky. URL: <https://encyclopedia.kaspersky.ru/glossary/rainbow-table/> (дата обращения: 12.03.2025).
4. Как хакеры могут взломать пароль за час // kaspersky. URL: <https://www.kaspersky.ru/blog/password-can-be-hacked-in-one-hour/37700/> (дата обращения: 12.03.2025).

Статья поступила в редакцию 19.04.2025; принята к публикации 10.05.2025

Информация об авторах

Аверин П.А. – студент кафедры «Системы информационной безопасности», направление подготовки 10.05.03 - Информационная безопасность автоматизированных систем ФГБОУ ВО «БГТУ».

Коновалов С.И. – студент кафедры «Системы информационной безопасности», направление подготовки 10.05.03 - Информационная безопасность автоматизированных систем ФГБОУ ВО «БГТУ».

Шапенская А.М. – ассистент кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Вклад авторов

Аверин П.А. – идея, обработка материала, частичное написание статьи (33%).

Коновалов С.И. – сбор материала, обработка материала, частичное написание статьи (33%).

Шапенская А.М. – научное редактирование, доработка текста (34%).

Конфликт интересов отсутствует.

Научная статья
УДК 378:004

Постэксплуатация в Windows

Павел Александрович Аверин ^{1✉}, Данила Васильевич Староверов ²,
Сергей Игоревич Коновалов ³, Алина Михайловна Шапенская ⁴
^{1,2,3,4} Брянский государственный технический университет, Брянск, Россия
¹stopnotwont@gmail.com✉, <https://orcid.org/0009-0003-5074-7217>
²danila.star2004@mail.ru, <https://orcid.org/0009-0007-1619-3459>
³velvet1way@gmail.com, <https://orcid.org/0009-0008-5867-635X>
⁴alinashapenskaya@yandex.ru, <https://orcid.org/0009-0007-8434-5848>

Аннотация. Статья описывает методы и инструменты пост-эксплуатации в Windows, такие как PowerShell Empire, Metasploit, Cobalt Strike и Mimikatz. Эти инструменты помогают закреплять доступ, повышать привилегии и собирать данные. Основные техники включают автозапуск вредоносного ПО, эксплуатацию уязвимостей и перемещение по сети. Для защиты рекомендуются мониторинг активности, ограничение прав пользователей и внедрение систем безопасности.

Ключевые слова: постэксплуатация, Windows, злоумышленники, закрепление доступа, сбор данных, PowerShell Empire, Metasploit, Cobalt Strike, Mimikatz.

Для цитирования: Аверин П.А., Староверов Д.В., Коновалов С.И., Шапенская А.М. Постэксплуатация в Windows // Актуальные проблемы кибербезопасности. Противодействие экстремизму и терроризму в информационной молодежной среде: сборник докладов I межрегиональной научно-практической конференции. – Брянск: БГТУ, 2025. – С. 338 – 341.

Пост-эксплуатация – это действия злоумышленников, которые следуют после того, как атакуемая инфраструктура была скомпрометирована [1]. Для большего понимания, пост-эксплуатация в Windows – это этап после первоначального проникновения в систему, когда атакующий стремится закрепить свой доступ, повысить привилегии, собрать конфиденциальную информацию и обеспечить возможность повторного входа. Для этих целей используются различные инструменты и техники.



Рис. 1. Статистка обращений пострадавших компаний

Первый рассмотренный инструмент для пост-эксплуатации: PowerShell Empire. Powershell Empire предоставляет модульную платформу для пост-эксплуатации, используя возможности средства автоматизации ОС Windows PowerShell [2]. Он запускается в памяти, что снижает вероятность его обнаружения. Этот инструмент может загружать модули, управлять процессами, собирать пароли и даже настраивать автозапуск вредоносного кода.

Metasploit Framework – один из самых популярных инструментов для атак, включающий модули пост-эксплуатации, такие как Incognito. Он позволяет захватывать токены пользователей, манипулировать учетными записями и выполнять команды с привилегиями администратора. Например, с помощью Incognito можно перехватить права администратора, просто внедрившись в процесс с нужными токенами. Также в Metasploit встроены механизмы для обхода UAC (User Account Control), что помогает атакующему работать без лишних ограничений.

Cobalt Strike Beacon – компонент популярного решения Cobalt Strike. Это коммерческий инструмент, который специалисты по тестированию на проникновение используют, чтобы эмулировать действия атакующих, а злоумышленники – чтобы решать задачи на разных этапах киберинцидента [4]. Он работает через так называемые «маячки» (Beacon), которые позволяют удаленно управлять зараженной системой, обходить антивирусы и выполнять произвольные команды. В Cobalt Strike встроены мощные средства для скрытного перемещения по сети, эксплуатации уязвимостей и длительного закрепления в системе. Этот инструмент особенно популярен среди профессионалов, моделирующих атаки на уровне АРТ-группировок.

Mimikatz – это приложение с открытым исходным кодом, которое позволяет пользователям просматривать и сохранять учетные данные аутентификации, такие как тикеты Kerberos [5]. Эта техника позволяет атакующему получить логины и пароли пользователей прямо из процесса LSASS. Кроме того, с помощью Mimikatz можно проводить атаки типа Pass-the-Hash и Pass-the-Ticket, позволяя злоумышленнику аутентифицироваться в системе без знания пароля. Это один из самых распространенных инструментов для атак на корпоративные сети.

Пост-эксплуатация в Windows включает несколько ключевых техник, которые позволяют атакующему закрепиться в системе, скрыть свое присутствие и получить контроль над сетью.

Закрепление в системе – злоумышленник настраивает автозапуск через реестр (HKCU\Software\Microsoft\Windows\CurrentVersion\Run), создаёт запланированные задачи (schtasks), встраивается в службы или добавляет скрытые учетные записи (net user /add).

Повышение привилегий – использование уязвимостей, обхода UAC или перехвата токенов с помощью Mimikatz для получения прав администратора.

Сбор учетных данных – извлечение паролей и хешей из памяти процесса LSASS, атаки Pass-the-Hash и Pass-the-Ticket, дампинг SAM.

Обход защиты – маскировка вредоносного кода, запуск процессов в памяти, обфускация PowerShell-команд и использование легитимных процессов (rundll32.exe, regsvr32.exe).

Перемещение по сети – распространение атаки на другие машины через PsExec, WMI, перехват учетных данных администраторов и эксплуатация доверенных связей в Active Directory.

В пост-эксплуатации Windows злоумышленники используют различные инструменты и техники, чтобы закрепиться в системе, повысить привилегии, собрать учетные данные и скрыть свое присутствие. PowerShell Empire, Metasploit, Cobalt Strike и Mimikatz позволяют атакующим управлять процессами, обходить антивирусы и перехватывать учетные записи пользователей. Основные методы включают автозапуск вредоносного кода, эксплуатацию уязвимостей для повышения привилегий, извлечение паролей из памяти и перемещение по сети для распространения атаки. Для защиты необходимо контролировать активность в системе, ограничивать права пользователей и использовать средства мониторинга безопасности.

Список источников

1. Постэксплуатация // securitylab. URL: <https://www.securitylab.ru/glossary/postekspluatatsiya/> (дата обращения: 10.02.2025).
2. PowerShell Empire: продвинутая постэксплуатация Windows систем // habr. URL: <https://habr.com/ru/articles/351592/> (дата обращения: 10.02.2025).
3. Постэксплуатация скомпрометированных Windows систем. Metasploit Incognito // codeby. URL: https://codeby.net/threads/post-ekspluatatsiya-skompromentirovannykh-windows-sistem-metasploit-incognito.61804/?utm_source=chatgpt.com (дата обращения: 10.02.2025).
4. Атаки с применением Cobalt Strike снова обрушились на российские компании // bi.zone. URL: <https://bi.zone/news/ataki-s-primeneniem-cobalt-strike-snova-obrushilis-na-rossiyskie-kompanii/> (дата обращения: 10.02.2025).

5. Приручение черного дракона. Этичный хакинг с Kali Linux. Часть 7. Постэксплуатация. Закрепление в системе // habr. URL: <https://habr.com/ru/articles/700004/> (дата обращения: 10.02.2025).

6. Хакеры начинают использовать фреймворк постэксплуатации Navos в атаках // startpack. URL: <https://startpack.ru/articles/20230216-havoc> (дата обращения: 10.02.2025).

Статья поступила в редакцию 19.04.2025; принята к публикации 10.05.2025

Информация об авторах

Аверин П.А. – студент кафедры «Системы информационной безопасности», направление подготовки 10.05.03 - Информационная безопасность автоматизированных систем ФГБОУ ВО «БГТУ».

Староверов Д.В. – студент кафедры «Системы информационной безопасности», направление подготовки 10.05.03 - Информационная безопасность автоматизированных систем ФГБОУ ВО «БГТУ».

Коновалов С.И. – студент кафедры «Системы информационной безопасности», направление подготовки 10.05.03 - Информационная безопасность автоматизированных систем ФГБОУ ВО «БГТУ».

Шапенская А.М. – ассистент кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Вклад авторов

Аверин П.А. – идея, обработка материала, частичное написание статьи (25%).

Староверов Д.В. – сбор материала, обработка материала, частичное написание статьи (25%).

Коновалов С.И. – сбор материала, обработка материала, частичное написание статьи (25%).

Шапенская А.М. – научное редактирование, доработка текста (25%).

Конфликт интересов отсутствует.

Научная статья

УДК 004

Оценка соответствия требованиям приказа ФСТЭК России № 21

Павел Александрович Аверин ^{1✉}, Дарья Алексеевна Терехова ^{2✉},

Сергей Игоревич Коновалов ³, Алина Михайловна Шапенская ⁴

^{1,2,3,4} Брянский государственный технический университет, Брянск, Россия

¹ stopnotwont@gmail.com ✉, <https://orcid.org/0009-0003-5074-7217>

² daraterehova5@gmail.com ✉, <https://orcid.org/0009-0006-7482-0409>

³ velvet1way@gmail.com, <https://orcid.org/0009-0008-5867-635X>

⁴ alinashapenskaya@yandex.ru, <https://orcid.org/0009-0007-8434-5848>

Аннотация. Для обеспечения защиты ПДн от её неправомерного использования злоумышленниками, в организации должны быть приняты соответствующие меры по ее защите. Для этого проводится оценка соответствия требованиям приказам ФСТЭК, в данном случае 21-го приказа ФСТЭК, который устанавливает организационные и технические меры по обеспечению безопасности ПДн.

Ключевые слова: ФСТЭК, организационные и технические меры, оценка соответствия требованиям, персональные данные (ПДн), защита информации (ЗИ), средство защиты информации (СЗИ), аттестация соответствия.

Для цитирования: Аверин П.А., Терехова Д.А., Коновалов С.И., Шапенская А.М. Оценка соответствия требованиям приказа ФСТЭК России № 21 // Актуальные проблемы кибербезопасности. Противодействие экстремизму и терроризму в информационной молодежной среде: сборник докладов I межрегиональной научно-практической конференции. – Брянск: БГТУ, 2025. – С. 342 – 345.

Обеспечение безопасности персональных данных (ПДн) при их обработке в информационных системах является важной задачей для государственных и коммерческих организаций. В условиях постоянного роста киберугроз и развития цифровых технологий соблюдение требований законодательства в области защиты информации становится необходимым элементом стабильной и безопасной работы любой структуры. Одним из ключевых нормативных актов, регламентирующих эту сферу, является Приказ ФСТЭК России от 18.02.2013 г. №21, который устанавливает комплекс организационных и технических мер, направленных на предотвращение неправомерного доступа, утечки, модификации или уничтожения персональных данных.

Данный приказ применяется в организациях, деятельность которых связана с обработкой персональных данных, включая государственные учреждения, медицинские и образовательные организации, банки, страховые компании, промышленные предприятия, IT-компании и другие субъекты, работающие с информацией ограниченного доступа. Его требования учитываются при разработке и эксплуатации информационных систем, построении политики информационной безопасности, выборе технических средств защиты, а также в рамках процедур оценки соответствия и аттестации

объектов информатизации.

Приказ ФСТЭК России от 18.02.2013 г. №21 (в ред. Приказа ФСТЭК России от 23.03.2017 №49, от 14.05.2020 № 68) является документом, утверждающим и устанавливающим состав и содержание организационных и технических мер по обеспечению безопасности ПДн при их обработке в информационных системах для каждого из уровней защищенности. Данные меры принимаются для защиты от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения и от иных неправомерных действий в отношении ПДн.

В состав мер входят:

- идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ);
- управление доступом субъектов доступа к объектам доступа (УПД);
- ограничение программной среды (ОПС);
- защита машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные (ЗНИ);
- регистрация событий безопасности (РСБ);
- антивирусная защита (АВЗ);
- обнаружение (предотвращение) вторжений (СОВ);
- контроль (анализ) защищенности персональных данных (АНЗ);
- обеспечение целостности информационной системы и персональных данных (ОЦЛ);
- обеспечение доступности персональных данных (ОДТ);
- защита среды виртуализации (ЗСВ);
- защита технических средств (ЗТС);
- защита информационной системы, ее средств, систем связи и передачи данных (ЗИС);
- выявление инцидентов и реагирование на них (ИНЦ);
- управление конфигурацией информационной системы и системы и системы защиты ПД (УКФ).

Приказ ФСТЭК №21 учитывает уровни защищенности, установленные постановлением Правительства РФ от 01.11.2012 №1119. Организации обязаны соблюдать требования, соответствующие их уровню защищенности, в зависимости от объема и критичности обрабатываемых персональных данных.

Проверку соответствия требованиям ФСТЭК проводят аккредитованные организации, имеющие лицензию на аттестацию объектов информатизации. Согласно Приказу ФСТЭК России от 29.04.2021 №77, такая проверка называется аттестацией соответствия (или аудитом). Она подтверждает, что организация выполняет требования безопасности и корректно обрабатывает данные.

Основные этапы аттестации:

- обследование объекта информатизации;
- проектирование системы защиты информации;

- установка и настройка средств защиты;
- тестирование на возможные угрозы и утечки.

По завершении процедуры организация получает аттестат соответствия сроком на три года. Затем необходимо повторно пройти проверку, чтобы продлить его действие.

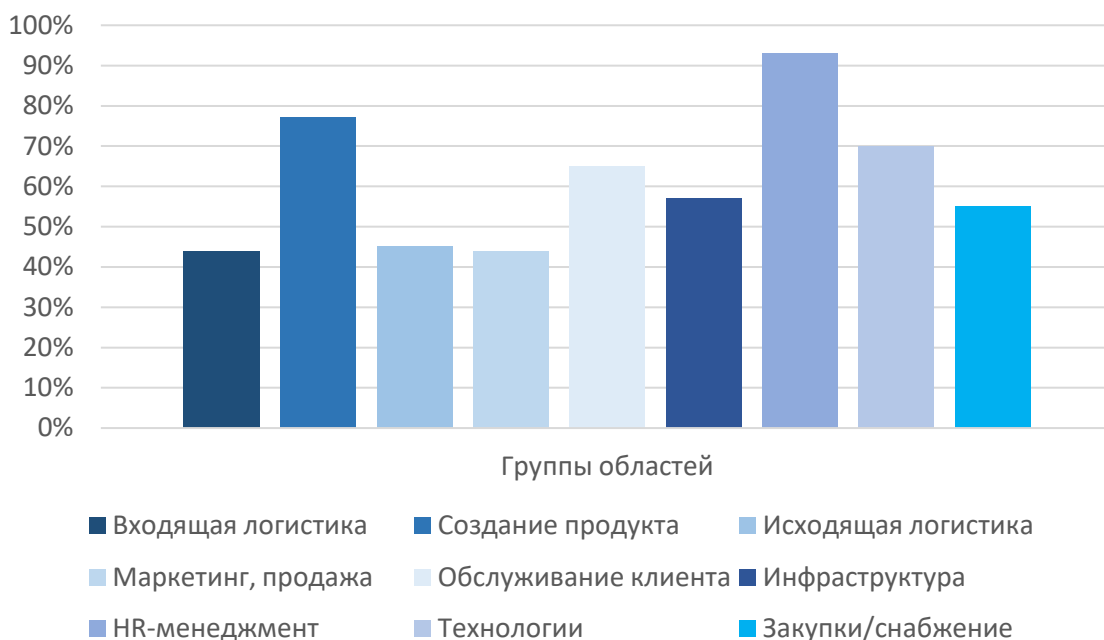


Рис. 1. Исполнение приказа № 21 в различных областях

Степень выполнения требований может отличаться в зависимости от сферы деятельности. Например, в HR-менеджменте уровень соответствия приказу достигает 93%, тогда как в сфере логистики — всего 41%. Это связано с тем, что в кадровой сфере работа с персональными данными ведется особенно строго.

Соблюдение норм информационной безопасности — это не просто формальная обязанность, а защита репутации компании и ее клиентов. Нарушение требований может привести к утечке данных, штрафам, потере доверия партнеров и клиентов. Поэтому важно вовремя проходить аттестацию соответствия и внедрять современные меры защиты.

Список источников

1. Приказ ФСТЭК России от 18 февраля 2013 г. N 21. URL: <https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-18-fevralya-2013-g-n-21> (дата обращения: 18.02.2025).
2. Приказ ФСТЭК России от 29 апреля 2021 г. N 77. URL: <https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-29-aprelya-2021-g-n-77> (дата обращения: 18.02.2025).
3. Аттестация ИСПДн по требованиям безопасности. URL: <https://info-security.su/uslugi/attestatsiya-obektov-informatizatsii/attesta-tsiya-informatsionnoy-sistemy-personalnyh-dannyh-ispdn/> (дата обращения: 18.02.2025).

4. Постановление Правительства РФ от 01.11.2012. URL: https://www.consultant.ru/document/cons_doc_LAW_137356/ (дата обращения: 18.02.2025).

5. Приказ ФСТЭК № 21. Контроль соответствия. URL: <https://service.securitm.ru/docs/fstec-21> (дата обращения: 24.02.2025).

6. Сабельфильд Н. В. Оценка соответствия параметров средств защиты информации требованиям безопасности // Актуальные проблемы авиации и космонавтики. 2018. Т. 2, № 14. С. 238-240.

Статья поступила в редакцию 19.04.2025; принята к публикации 10.05.2025

Информация об авторах

Аверин П.А. – студент кафедры «Системы информационной безопасности», направление подготовки 10.05.03 - Информационная безопасность автоматизированных систем ФГБОУ ВО «БГТУ».

Терехова Д.А. – студент кафедры «Системы информационной безопасности», направление подготовки 10.03.01 - Информационная безопасность ФГБОУ ВО «БГТУ».

Коновалов С.И. – студент кафедры «Системы информационной безопасности», направление подготовки 10.05.03 - Информационная безопасность автоматизированных систем ФГБОУ ВО «БГТУ».

Шапенская А.М. – ассистент кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Вклад авторов

Аверин П.А. – идея, обработка материала, частичное написание статьи.

Терехова Д.А. – сбор материала, обработка материала, частичное написание статьи.

Коновалов С.И. – сбор материала, обработка материала, частичное написание статьи.

Шапенская А.М. – научное редактирование, доработка текста.

Конфликт интересов отсутствует.

Научная статья

УДК 378:004

Кибербезопасность и молодежь: противодействие цифровому экстремизму и террористическому влиянию в Интернете

Евгений Вячеславович Анищенко

Брянский государственный технический университет, Брянск, Россия

zhenya.anishchenko@mail.ru, <https://orcid.org/0009-0003-4663-6266>

Аннотация. В условиях цифровизации социальных процессов молодежь становится одной из наиболее уязвимых групп, подверженных влиянию экстремистских и террористических идеологий в интернете. В статье рассматриваются ключевые угрозы кибербезопасности, связанные с распространением деструктивного контента, методы вербовки через социальные сети и мессенджеры, а также стратегии противодействия цифровой радикализации. Особое внимание уделяется роли государственных институтов, образовательных организаций и IT-компаний в профилактике киберэкстремизма. Анализируются как технологические решения (алгоритмы модерации, искусственный интеллект), так и социально-психологические подходы (медиаграмотность, воспитательные программы).

Ключевые слова: киберэкстремизм, цифровая радикализация, информационная безопасность молодежи.

Для цитирования: Анищенко Е.В. Кибербезопасность и молодежь: противодействие цифровому экстремизму и террористическому влиянию в Интернете // Актуальные проблемы кибербезопасности. Противодействие экстремизму и терроризму в информационной молодежной среде: сборник докладов I межрегиональной научно-практической конференции. – Брянск: БГТУ, 2025. – С. 346 – 348.

В современном цифровом мире проблема кибербезопасности молодежи приобретает особую остроту. Интернет-пространство стало новой ареной для распространения экстремистских и террористических идей, где молодежь оказывается наиболее уязвимой целевой аудиторией. Социальные сети, мессенджеры и онлайн-игры активно используются радикальными группами для вербовки новых сторонников, что требует разработки комплексных мер противодействия.

Основные угрозы связаны с целенаправленной пропагандой в цифровой среде. Алгоритмы социальных сетей, предназначенные для персонализации контента, нередко используются для распространения деструктивных материалов. Закрытые чаты в Telegram и Discord, анонимные форумы в даркнете становятся площадками для координации незаконной деятельности. Особую опасность представляет геймификация радикального контента, когда экстремистские идеи внедряются через популярные среди молодежи онлайн-игры и виртуальные сообщества.

Для противодействия этим угрозам применяется комплекс мер. На законодательном уровне это блокировка запрещенного контента согласно федеральным законам. Технологические решения включают использование искусственного интеллекта для автоматического выявления и фильтрации опасных материалов.

Важную роль играют образовательные программы, направленные на повышение медиаграмотности среди молодежи, такие как проект "Кибердружина".

В эпоху тотальной цифровизации проблема противодействия экстремизму и терроризму в интернет-пространстве приобретает новые, более сложные формы. Особую тревогу специалистов по кибербезопасности вызывает стремительная эволюция методов вовлечения молодежи в деструктивную деятельность через цифровые каналы.

Одним из наиболее опасных трендов последних лет стало появление так называемого "гибридного экстремизма", который сочетает традиционные методы вербовки с передовыми цифровыми технологиями. Речь идет об использовании нейросетей для создания персонализированного пропагандистского контента, применении технологий deepfake для производства фальшивых новостных роликов, а также использовании big data для точного таргетинга на уязвимые группы молодежи. Особенность современной ситуации заключается в том, что экстремистские группировки зачастую опережают государственные структуры в освоении новых цифровых инструментов. Парадоксально, но именно популярные среди молодежи платформы, позиционирующие себя как "нейтральные" или "развлекательные", становятся основными каналами распространения радикального контента. Короткие видеоформаты в TikTok, стримы на Twitch, чат-боты в мессенджерах - все эти инструменты используются для завуалированной пропаганды экстремистских идей. При этом контент часто маскируется под мотивационные ролики, материалы о саморазвитии или даже геймифицированные квесты. Особую сложность представляет борьба с децентрализованными сетями распространения запрещенной информации. В отличие от ранних этапов развития интернета, когда можно было блокировать конкретные сайты или сообщества, современные экстремистские структуры используют распределенные системы хранения данных, криптографические методы защиты информации и постоянно меняющиеся каналы коммуникации. Это требует принципиально новых подходов к мониторингу и противодействию. Ключевая роль в профилактике цифрового экстремизма принадлежит различным институтам общества. Государство координирует взаимодействие с IT-компаниями для оперативного реагирования на новые угрозы. Образовательные учреждения внедряют программы по цифровой гигиене в учебные планы. Не менее важна позиция родителей, которые должны проявлять внимание к онлайн-активности подростков и поддерживать с ними открытый диалог. Эффективная борьба с киберэкстремизмом требует сочетания технологических, правовых и воспитательных мер. Особое значение имеет развитие у молодежи критического мышления и устойчивости к информационным манипуляциям. Только комплексный подход позволит создать безопасную цифровую среду для подрастающего поколения и противостоять угрозам экстремизма и терроризма в интернет-пространстве.

Ключевым аспектом становится понимание психологических механизмов цифровой социализации современной молодежи. Поколение Z и Alpha формируют свою идентичность в условиях перманентного онлайн-присутствия, что создает уникальные уязвимости:

- 1) фрагментация цифрового сознания;
- 2) клиповое восприятие информации;
- 3) потребность в цифровой самоидентификации;
- 4) кризис авторитетов в информационном пространстве.

Эти особенности требуют разработки специальных "антивирусных" технологий цифровой социализации, основанных на принципах:

- 1) Превентивной аналитики цифрового поведения;
- 2) Геймификации позитивного контента;
- 3) Создания цифровых наставнических систем;
- 4) Развития альтернативных онлайн-сообществ.

Технологический ответ этим вызовам должен включать:

- 1) Разработку предиктивных систем анализа цифровых следов.
- 2) Создание цифровых двойников для моделирования процессов радикализации.

3) Применение технологий эмоционального ИИ для раннего выявления групп риска.

Перспективным направлением является развитие "гуманитарных технологий" - междисциплинарных решений, сочетающих достижения компьютерных наук с глубоким пониманием социальных и психологических процессов. Это требует принципиально новых форматов сотрудничества между технологами, педагогами, психологами и специалистами по безопасности.

Список источников

1. Асмолов А.Г., Цибульский Г.Э. Психология терроризма и противодействие ему в цифровой среде // Вестник МГУ. Серия 14. Психология. 2021. С. 12–15.
2. Власов В.С., Кузнецов А.А. Киберэкстремизм в молодежной среде: методы противодействия // Информационная безопасность регионов. 2022. С. 8–10.
3. Зубков А.И., Петров М.А. Цифровая радикализация: механизмы и профилактика // Журнал исследований социальной политики. 2023. С. 10 –12.
4. Касперская Н.И. Кибербезопасность и борьба с терроризмом в интернете. – СПб.: Питер, 2020. - С. 200–250.
5. Российский журнал криминологии. Киберпреступность и экстремизм: новые вызовы (спецвыпуск). 2023. С. 150–200.

Статья поступила в редакцию 19.04.2025; принята к публикации 10.05.2025

Информация об авторе

Анищенко Е. В. – магистрант кафедры «Системы информационной безопасности», направление подготовки 10.04.01 – Информационная безопасность ФГБОУ ВО «БГТУ».

Научная статья

УДК 004.9

Автоматизированный анализ текстов в социальных сетях для выявления признаков вербовки в экстремистские организации

Диана Игоревна Денисеня^{1✉}, Дмитрий Андреевич Лысов²,
Павел Дмитриевич Горелов³, Карина Владимировна Морозова⁴

^{1,2,3,4} Брянский государственный технический университет, Брянск, Россия

¹d.diana1519@gmail.com ✉, <https://orcid.org/0009-0004-6440-7632>

²lysovdmitriia@gmail.com, <https://orcid.org/0009-0003-9666-7191>

³pashkayr@yandex.ru, <https://orcid.org/0009-0008-7487-6124>

⁴marus.korotkova@yandex.ru, <https://orcid.org/0009-0007-2396-4469>

Аннотация. Статья посвящена актуальной проблеме использования социальных сетей для распространения экстремистских идей и вербовки в радикальные организации.

Ключевые слова: социальные сети, экстремизм, вербовка, обработка естественного языка (NLP), машинное обучение.

Для цитирования: Денисеня Д.И., Лысов Д.А., Горелов П.Д., Морозова К.В. Автоматизированный анализ текстов в социальных сетях для выявления признаков вербовки в экстремистские организации // Актуальные проблемы кибербезопасности. Противодействие экстремизму и терроризму в информационной молодежной среде: сборник докладов I межрегиональной научно-практической конференции. – Брянск: БГТУ, 2025. – С. 349 – 351.

В контексте современных процессов глобализации и цифровой трансформации общества социальные сети интегрировались в повседневную жизнь миллионов людей, предоставляя платформы для коммуникации, информационного обмена и самовыражения. Однако, несмотря на их позитивные аспекты, социальные сети могут быть использованы для распространения экстремистских идей и вербовки в радикальные организации. В последние годы отмечается увеличение количества случаев, когда социальные сети используются в качестве средства для привлечения новых adeптов экстремистских группировок. Данное явление представляет собой значительную угрозу для национальной и международной безопасности, а также для социальной стабильности в целом. В связи с этим возникает необходимость разработки эффективных методов автоматизированного анализа текстов в социальных сетях, направленных на своевременное выявление признаков вербовки и предотвращение распространения экстремистской пропаганды.

Автоматизированный анализ текстов в социальных сетях для выявления признаков вербовки в экстремистские организации представляет собой междисциплинарную задачу, требующую интеграции методов обработки естественного языка (NLP), машинного обучения и анализа больших данных [1]. Основная цель такого анализа заключается в обнаружении подозрительных сообщений, содержащих экстремистскую пропаганду, а также в идентификации пользователей, которые могут быть вовлечены в процесс вербовки. Для достижения этой цели

необходимо решить несколько ключевых задач. Во-первых, требуется разработка алгоритмов, способных распознавать специфическую лексику, характерную для экстремистских сообщений. Это включает в себя использование методов токенизации (это процесс разделения текста на отдельные элементы (токены), такие как слова, фразы или символы, что позволяет системе обрабатывать текст на уровне отдельных компонентов), лемматизации (процесс приведения слов к их базовой или основополагающей форме (лемме), что помогает унифицировать текст и упростить его анализ) и морфологического анализа текста (изучение структуры слов, включая их корни, приставки, суффиксы и другие морфемные компоненты, что позволяет понять грамматические и семантические особенности текста) [3]. Во-вторых, необходимо создание моделей машинного обучения, обученных на больших объёмах данных, которые могут классифицировать тексты на основе их содержания. В-третьих, важно учитывать контекст и семантику сообщений, что требует применения методов анализа тональности (процесс определения эмоционального или смыслового оттенка текста, например, позитивного, негативного или нейтрального) и семантического анализа (то изучение значений слов и фраз в контексте, что позволяет выявить скрытые смыслы и намерения автора).

Одним из ключевых этапов автоматизированного анализа текстов является сбор и предобработка данных. Социальные сети генерируют огромные объёмы текстовой информации, которая может быть неструктурированной и содержать помехи. Для эффективного анализа необходимо выполнить предварительную обработку данных, включающую удаление дубликатов, нормализацию текста и фильтрацию нерелевантной информации. После этого данные могут быть использованы для обучения моделей машинного обучения. В последние годы активно применяются глубокие нейронные сети, такие как рекуррентные нейронные сети (RNN) и трансформеры, которые позволяют достигать высокой точности в задачах классификации текстов [2].

Для выявления признаков вербовки в экстремистские организации важно учитывать не только содержание отдельных сообщений, но и контекст их распространения. Например, анализ сетевых взаимодействий между пользователями может помочь выявить группы лиц, которые активно распространяют экстремистские идеи. Для этого могут быть использованы методы анализа социальных сетей, такие как анализ центральности и кластеризация (метод анализа данных, который заключается в разделении объектов (например, пользователей или сообщений) на группы (кластеры) на основе их сходства) [4]. Эти методы позволяют идентифицировать ключевых участников сети и выявить скрытые связи между ними. Кроме того, важно учитывать динамику изменения содержания сообщений во времени, что требует применения методов временного анализа. Одним из основных вызовов в автоматизированном анализе текстов в социальных сетях является многоязычность и культурная специфика сообщений. Экстремистские организации могут использовать различные языки и диалекты, а также специфическую терминологию, которая может быть трудно распознаваема для автоматических систем. Для решения этой проблемы необходимо разрабатывать

многоязычные модели, способные адаптироваться к различным языковым и культурным контекстам. Кроме того, важно учитывать этические и правовые аспекты анализа данных, такие как конфиденциальность и защита персональных данных пользователей. Использование различных процессов и методов в комплексе позволяет значительно повысить эффективность в борьбе с вербовкой в социальных сетях. Поэтому не стоит заикливаться лишь на одном процессе.

Список источников

1. Neuro-linguistic programming. URL: https://en.wikipedia.org/wiki/Neuro-linguistic_programming (дата обращения: 18.04.2025).
2. Stacked RNNs in NLP. URL: <https://www.geeksforgeeks.org/stacked-rnns-in-nlp/> (дата обращения: 18.04.2025).
3. Tokenization and lemmatization in NLP. URL: <https://www.tutorialspoint.com/what-is-tokenization-and-lemmatization-in-nlp> (дата обращения: 18.04.2025).
4. Кластеризация. URL: <https://education.yandex.ru/handbook/ml/article/klasterizaciya> (дата обращения: 19.04.2025).
5. Ананьин О.Ю. Вербовка молодежи в террористические организации посредством социальных сетей: проблемы профилактики // Вестник экономической безопасности. 2022. С. 6

Статья поступила в редакцию 20.04.2025; принята к публикации 10.05.2025

Информация об авторах

Денисеня Д.И. – студент кафедры «Компьютерные технологии и системы», направление подготовки 09.03.02 – Информационные системы и технологии ФГБОУ ВО «БГТУ».

Лысов Д.А. – старший преподаватель кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Горелов П.Д. – студент кафедры «Системы информационной безопасности», направление подготовки 10.03.01 – Информационная безопасность ФГБОУ ВО «БГТУ».

Морозова К.В. – студент кафедры «Системы информационной безопасности», направление подготовки 10.03.01 – Информационная безопасность ФГБОУ ВО «БГТУ».

Вклад авторов

Денисеня Д.И. - идея, сбор материала, обработка материала, частичное написание статьи (25%).

Лысов Д.А. - написание статьи, научное редактирование текста (25%).

Горелов П.Д. - идея, сбор материала, обработка материала, частичное написание статьи (25%).

Морозова К.В. - идея, сбор материала, обработка материала, частичное написание статьи (25%).

Конфликт интересов отсутствует.

Научная статья

УДК 327.8

Социально-культурные аспекты противодействия экстремизму и терроризму в молодежной среде

**Владислав Павлович Киселев^{1✉}, Александр Александрович Бузылев^{2✉},
Дмитрий Андреевич Лысов^{3✉}, Алексей Петрович Горлов^{4✉}**

^{1,2,3,4}Брянский государственный технический университет, Брянск, Россия

¹vkiselev1213@gmail.com[✉], <https://orcid.org/0009-0002-5845-1149>

²buzylev2018@yandex.ru[✉], <https://orcid.org/0009-0005-3301-7006>

³lysovdmitriia@gmail.com[✉], <https://orcid.org/0009-0003-9666-7191>

⁴apgorlov@gmail.com[✉], <https://orcid.org/0009-0003-3100-3466>

Аннотация. В статье рассматриваются социально-культурные аспекты противодействия экстремизму и терроризму в молодежной среде. Особое внимание уделяется образовательным, коммуникативным, культурным, психологическим и информационным методам, направленным на формирование у молодежи толерантности, критического мышления и чувства социальной ответственности.

Ключевые слова: экстремизм, терроризм, молодежь, толерантность, взаимодействие, поддержка.

Для цитирования: Киселев В.П., Бузылев А.А., Лысов Д.А., Горлов А.П. Социально-культурные аспекты противодействия экстремизму и терроризму в молодежной среде // Актуальные проблемы кибербезопасности. Противодействие экстремизму и терроризму в информационной молодежной среде: сборник докладов I межрегиональной научно-практической конференции. – Брянск: БГТУ, 2025. – С. 352 – 354.

Социально-культурные аспекты противодействия экстремизму и терроризму в молодежной среде играют важную роль в профилактике и снижении радикальных настроений. Основой успешной борьбы с экстремизмом является воспитание гуманного мировоззрения, терпимости и уважения к культурным, национальным и религиозным различиям.

Основные направления социально-культурного противодействия:

- культурные технологии помогают создать общественное пространство, ориентированное на гуманизм, где люди могут развиваться и формировать духовные и нравственные ценности;
- коммуникативные технологии включают общение между людьми и вовлечение молодежи в творческие сообщества, которые удовлетворяют их потребности в творчестве и социальной интеграции;
- образовательные и информационные меры помогают развивать кросс-культурные знания и критическое мышление, формируя у молодежи негативное отношение к экстремистским идеям;
- управленческие технологии помогают готовить лидеров молодежных организаций и развивать партнерство между государством и общественными институтами;

- художественная самодеятельность и этнические творческие мероприятия помогают укреплять культурную идентичность и межкультурный диалог. Практические меры профилактики:
 - проведение уроков и тренингов по толерантности, направленных на развитие навыков позитивного диалога и эмпатии;
 - активное вовлечение молодежи в социально-культурные проекты, международные фестивали и научные конференции, способствующие межкультурному взаимопониманию;
 - мониторинг экстремистских настроений и раннее выявление рисков, включая контроль за экстремистским контентом в интернете;
 - формирование правовой культуры и расширение юридического образования для молодежи с целью повышения уважения к правам и свободам других людей;
 - пропаганда здорового образа жизни и занятия спортом как альтернативы экстремистским идеологиям;
 - поддержка творческих проектов, которые помогают выразить свои мысли и чувства через музыку, театр, живопись;
 - помощь психологов и социальных работников помогает молодежи справляться с трудностями и стрессом;
 - обучение молодежи, как безопасно пользоваться интернетом и не попадаться на провокации;
 - создание и распространение материалов, которые объясняют опасность экстремизма и терроризма;
 - активная работа СМИ и социальных сетей по продвижению мирных и дружелюбных идей.

Значение социально-культурной деятельности

Социально-культурная деятельность считается важным инструментом в педагогике, который помогает развивать толерантность и межкультурное образование, а также предотвращать распространение экстремистских идей среди молодежи. Она создает условия для социальной интеграции и снижает риск радикализации и экстремизма среди молодых людей.

Роль общества и государства

Для того чтобы молодежь была защищена от экстремизма, нужна поддержка не только со стороны семьи и учебных учреждений, но и государства, общественных организаций и СМИ. Важно создавать условия, где молодежь чувствует себя нужной и важной, где она может развиваться и чувствовать себя свободно.

Таким образом, использование комплексного социально-культурного подхода, который включает в себя различные образовательные программы, способы общения, управленческие стратегии и творческие методы, является эффективным способом борьбы с экстремизмом и терроризмом среди молодежи. Он помогает развивать у молодых людей устойчивые ценности и способствует установлению межкультурного диалога, что делает их менее восприимчивыми к радикальным идеям.

Список источников

1. disserCat: электронная библиотека диссертаций. URL: <https://www.dissercat.com/content/sotsialno-kulturnaya-profilaktika-ekstremizma-v-molodezhnoi-srede>.
2. CYBERLENINKA. URL: <https://cyberleninka.ru/article/n/sotsiokulturnye-aspekty-protivodeystviya-ekstremizmu-v-molodezhnoy-srede/viewer>.
3. ГАРАНТ.РУ. URL: <https://www.garant.ru/products/ipo/prime/doc/411135491/>.
4. АВТОР24: справочник. URL: https://spravochnick.ru/gosudarstvennoe_i_municipalnoe_upravlenie/socialno-kulturnaya_profilaktika_ekstremizma_v_molodezhnoy_srede/.

Статья поступила в редакцию 23.04.2025; принята к публикации 10.05.2025

Информация об авторах

Киселев В.П. – студент кафедры «Системы информационной безопасности», направление подготовки 10.03.01 – Информационная безопасность ФГБОУ ВО «БГТУ».

Бузылев А.А. – студент кафедры «Системы информационной безопасности», направление подготовки 10.04.01 – Информационная безопасность ФГБОУ ВО БГТУ.

Лысов Д.А. – старший преподаватель кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Горлов А.П. – к.т.н., доцент кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Вклад авторов

Киселев В.П. – идея, сбор материала, обработка материала, частичное написание статьи (25%).

Бузылев А.А. – сбор материала, обработка материала, частичное написание статьи (25%).

Лысов Д.А. – написание статьи, научное редактирование текста (25%).

Горлов А.П. – написание статьи, научное редактирование текста (25%).

Конфликт интересов отсутствует.

Научная статья
УДК 343.97

Влияние экстремистских ценностей на подростков через социальные сети: анализ и последствия

Данила Алексеевич Сычев

Брянский государственный технический университет, Брянск, Россия
danila.sychev.13@gmail.com, <https://orcid.org/0009-0008-8816-3731>

Аннотация. В современном цифровом мире социальные сети играют ключевую роль в формировании мировоззрения подростков. Однако наряду с позитивными аспектами, такими как общение, образование и самовыражение, социальные сети становятся платформой для распространения экстремистских идей. В данной статье рассматриваются механизмы влияния экстремистских ценностей на подростков через социальные сети, анализируются психологические и социальные последствия такого воздействия, а также предлагаются возможные меры противодействия. Для иллюстрации теоретических положений приводятся конкретные примеры из российской практики.

Ключевые слова: экстремизм, подростки, социальные сети.

Для цитирования: Сычев Д.А. Влияние экстремистских ценностей на подростков через социальные сети: анализ и последствия // Актуальные проблемы кибербезопасности. Противодействие экстремизму и терроризму в информационной молодежной среде: сборник докладов I межрегиональной научно-практической конференции. – Брянск: БГТУ, 2025. – С. 355 – 358.

Социальные сети стали неотъемлемой частью жизни подростков, предоставляя им доступ к информации, общению и развлечениям. Однако открытость и анонимность этих платформ создают благоприятные условия для распространения экстремистских идей. Подростки, находящиеся в поиске идентичности и подверженные влиянию сверстников, особенно уязвимы к манипуляциям со стороны экстремистских групп. Цель данной статьи — изучить, как экстремистские ценности влияют на подростков через социальные сети, и предложить пути минимизации этого влияния.

Схема вербовки подростков

В социальных сетях и мессенджерах вербуют несовершеннолетних для совершения диверсий на объектах транспортной инфраструктуры. Пойти на преступление их просят за деньги, а заказы как правило поступают от «кураторов» из других стран.

Схема вовлечения подростков в преступную деятельность начинается с простой переписки в чатах, социальных сетях, телеграмм-каналах, подготовленные вербовщики из других государств, как правило оценивают психологический, настрой подростка, его интересы, изучают психологический портрет через информацию на персональной странице социальных сетей, после чего пытаются наладить контакт, «втереться в доверие» под различными предложениями.

Как правило преступники пытаются вовлечь подростков в возрастной группе от 10 до 18 лет, то есть молодых людей, которые еще не могут полностью отдавать отчет своим действиям из-за недостаточно развитой эмоционально-волевой сферы. Данная возрастная группа наиболее восприимчива и легко поддается на уговоры пойти на преступление. Зачастую вербовщики пытаются вовлечь группу подростков, за обещание крупного денежного вознаграждения, либо путем воздействия уговорами. Преступные действия стараются завуалировать под некие задания, которые подросток должен выполнить, соблюдая конспирацию, при этом данные действия поощряют денежным вознаграждением.

Проще всего злоумышленникам удастся вовлечь в преступную деятельность подростков, которые страдают от дефицита внимания. Длительное время преступники могут путем переписки с подростком, используя специальную тактику и психологические приемы формировать у подростка иной тип мышления и склонность к совершению преступления.

Механизмы влияния экстремизма через социальные сети

Социальные сети предоставляют экстремистским группам уникальные возможности для вербовки и распространения своих идей. Основные механизмы влияния включают:

1. Социальные сети используют алгоритмы, которые показывают пользователям контент, основанный на их интересах. Это может привести к тому, что подростки, случайно столкнувшиеся с экстремистскими материалами, начинают получать всё больше подобного контента. Например, в 2022 году в России был зафиксирован случай, когда 16-летний подросток из Новосибирска, интересовавшийся историей Второй мировой войны, начал получать рекомендации от YouTube, связанные с неонацистскими идеологиями. В конечном итоге это привело к его участию в радикальной группировке, пропагандирующей насилие.

2. Экстремистские группы часто используют анонимные аккаунты и закрытые сообщества, где подростки чувствуют себя частью чего-то большего. Например, в 2023 году в Санкт-Петербурге была раскрыта сеть Telegram-каналов, где подростки обсуждали радикальные идеи и планировали акты вандализма. Многие участники этих чатов были подростками, испытывавшими одиночество и искавшими поддержку в онлайн-сообществах.

3. Экстремистский контент часто строится на сильных эмоциях, таких как гнев, страх или чувство несправедливости. Например, в 2022 году в Дагестане 17-летний подросток был завербован через "ВКонтакте" экстремистской группировкой, использующей исламистскую риторику. Вербовщики использовали его чувство несправедливости по отношению к социальному неравенству, чтобы убедить его присоединиться к их борьбе.

4. Экстремистские группы используют игровые элементы и вирусные челленджи, чтобы привлечь внимание подростков. В 2022 году в TikTok появился челлендж, связанный с пропагандой националистических идей. Подростки из разных регионов России делились видео с агрессивными лозунгами, что привело к широкому распространению подобного контента среди молодежи.

Психологические и социальные последствия

Психологические последствия вступления подростков в экстремистские группы часто проявляются в виде глубоких эмоциональных и когнитивных нарушений. Под воздействием радикальной идеологии у подростков формируется искаженное восприятие реальности, что приводит к деформации морально-этических норм и ценностей. У многих развивается так называемое "черно-белое" мышление, при котором мир делится на "своих" и "чужих", что способствует усилению агрессии и нетерпимости.

Кроме того, подростки, вовлеченные в экстремистскую деятельность, часто сталкиваются с посттравматическим стрессовым расстройством (ПТСР), вызванным участием в насильственных действиях или наблюдением за ними. Это может сопровождаться чувством вины, тревожностью, депрессией и суицидальными мыслями. Важно отметить, что выход из экстремистской группы не всегда приводит к мгновенному восстановлению психического здоровья. Многие подростки продолжают испытывать трудности с адаптацией к мирной жизни, что требует длительной психологической реабилитации.

Социальные последствия вступления подростков в экстремизм не менее значимы. Во-первых, такие подростки часто теряют связь с семьей и прежним кругом общения, что приводит к социальной изоляции. Родственники и друзья, не разделяющие радикальных взглядов, становятся "чужими", что усиливает чувство одиночества и отчуждения. Во-вторых, участие в экстремистской деятельности накладывает отпечаток на репутацию подростка, что затрудняет его реинтеграцию в общество даже после выхода из группы.

Кроме того, подростки, вовлеченные в экстремизм, часто сталкиваются с правовыми последствиями своих действий, включая уголовную ответственность. Это не только ограничивает их возможности для дальнейшего образования и трудоустройства, но и формирует у них чувство социальной несправедливости, что может способствовать рецидиву радикального поведения.

Меры противодействия

В условиях роста влияния социальных сетей на общественное сознание проблема распространения экстремистских идей становится все более актуальной. Социальные сети используются для пропаганды радикальных взглядов, вербовки и манипуляции, что требует разработки эффективных мер противодействия.

1. Мониторинг и анализ контента.

Внедрение систем автоматизированного мониторинга с использованием искусственного интеллекта позволяет выявлять и блокировать экстремистский контент. Это помогает предотвратить его распространение и снизить влияние на аудиторию.

2. Правовое регулирование.

Совершенствование законодательства, обязывающего платформы удалять экстремистские материалы, и установление ответственности за их распространение являются важными шагами. Международное сотрудничество также необходимо для борьбы с транснациональным характером экстремизма.

3. Образовательные программы.

Повышение медиа грамотности населения, особенно молодежи, через образовательные инициативы помогает развить критическое мышление и устойчивость к радикальной пропаганде.

4. Продвижение позитивного контента.

Активное распространение контента, направленного на укрепление толерантности и межкультурного диалога, создает альтернативу экстремистской пропаганде.

Таким образом, противодействие экстремизму в социальных сетях требует комплексного подхода, включающего технологические, правовые, образовательные и социальные меры. Совместные усилия государства, общества и международного сообщества способны минимизировать риски и обеспечить безопасность в цифровом пространстве.

Социальные сети, являясь мощным инструментом коммуникации, могут стать платформой для распространения экстремистских идей среди подростков. Это требует внимания со стороны общества, государства и технологических компаний. Только совместными усилиями можно минимизировать риски радикализации и обеспечить безопасное цифровое пространство для подрастающего поколения.

Список источников

1. Абдрахманов Д.М. Экстремизм. 100 ответов на насущные вопросы об экстремизме и терроризме: информационно-справочное пособие / Д.М. Абдрахманов, К.В. Максимов, М.М. Нугуманов, Э.Н. Сафина. – Уфа: Мир печати, 2018.

2. Профилактика экстремизма среди несовершеннолетних // Азбука воспитания: официальный сайт. URL: <https://lyl.su/i5Bx> (дата обращения: 06.03.2025).

3. Особенности профилактики и борьбы с проявлениями экстремизма и терроризма в молодежной среде // Центральный административный округ города Москвы: официальный сайт. URL: <https://lyl.su/ZOPC> (дата обращения: 06.03.2025).

Статья поступила в редакцию 17.04.2025; принята к публикации 10.05.2025

Информация об авторе

Сычев Д.А. – студент кафедры «Системы информационной безопасности», направление подготовки 10.05.03 – Информационная безопасность автоматизированных систем ФГБОУ ВО «БГТУ».

СЕКЦИЯ 8. БЕСПИЛОТНЫЕ ЛЕТАТЕЛЬНЫЕ АППАРАТЫ*

Научная статья

УДК 623.7:004.8

Роль искусственного интеллекта в оснащении беспилотных летательных аппаратов

Олег Андреевич Аненков

Брянский государственный технический университет, Брянск, Россия

anenvovoleg04@gmail.com, <https://orcid.org/0009-0001-4816-2987>

Аннотация. Данная статья представляет собой анализ использования искусственного интеллекта (ИИ) в Вооруженных силах Российской Федерации в беспилотных летательных аппаратах (БПЛА).

В статье рассказывается о способах применения искусственного интеллекта в БПЛА российской армии, а также о его роли в повышении эффективности боевых операций и обеспечении стратегического преимущества на современном поле боя. Также проведен анализ достоинств и недостатков БПЛА с ИИ на борту, а также сложностей внедрения данной техники в Вооруженные силы. Особое внимание уделено ключевым направлениям, таким как автономные системы и разведка.

Ключевые слова: искусственный интеллект (ИИ), Вооруженные силы Российской Федерации, автономные системы, беспилотные летательные аппараты (БПЛА), разведка и наблюдение, логистика и снабжение, машинное обучение, глубокое обучение, современные военные технологии, стратегическое преимущество.

Для цитирования: Аненков О.А. Роль искусственного интеллекта в оснащении беспилотных летательных аппаратов // Актуальные проблемы кибербезопасности. Противодействие экстремизму и терроризму в информационной молодежной среде: сборник докладов I межрегиональной научно-практической конференции. – Брянск: БГТУ, 2025. – С. 359 – 363.

Искусственный интеллект (англ. artificial intelligence) - это способность компьютера обучаться, принимать решения и выполнять действия, свойственные человеческому интеллекту.

Искусственный интеллект (ИИ) используется на всех этапах создания военного оборудования - от разработки и производства до эксплуатации и модернизации.

Точные данные о количестве военной техники с искусственным интеллектом в Вооруженных силах Российской Федерации (ВС РФ) в процентном соотношении не публикуются, однако по оценкам экспертов, доля техники с элементами ИИ в современных армиях мира (включая Россию) пока не превышает 10-20%. Однако эта цифра сильно варьируется в зависимости от типа техники. Например, беспилотные системы (БПЛА, роботы) чаще оснащаются ИИ, чем традиционная техника, а в системах ПВО, разведки и управления ИИ внедряется быстрее, чем в линейных подразделениях.

* Секция организована при поддержке Центра взаимодействия с научными ротами БГТУ.
© Аненков О. А., 2025

Ниже приведены подробные примеры и механизмы использования ИИ в БПЛА.

1. Разведка и наблюдение

Анализ данных: ИИ обрабатывает информацию от БПЛА, автоматически обнаруживая и классифицируя цели. Например, БПЛА «Орлан-10» использует искусственный интеллект для анализа видео и фотоснимков, что позволяет оперативно выявлять вражеские позиции, а спутниковые системы, оснащенные ИИ, способны отслеживать передвижения войск и техники противника, обеспечивая стратегическое преимущество.

Прогнозирование угроз: ИИ анализирует данные и предсказывает возможные действия противника.

2. Навигация и планирование

Беспилотные летательные аппараты (БПЛА) используют ИИ для: автономной навигации и планирования маршрутов, распознавания целей и передачи данных в реальном времени. Примеры БПЛА: «Орион» и «Охотник».

Как работает ИИ в БПЛА и спутниковых системах:

ИИ используется для **автоматического распознавания целей** на земле и в воздухе. Алгоритмы анализируют видео в реальном времени, выделяя движущиеся объекты (технику, пехоту) и классифицируя их.

БПЛА могут **автономно планировать маршруты**, избегая зон ПВО и других угроз, что повышает их живучесть и эффективность.

В случае с **тяжелым БПЛА «Охотник»** ИИ помогает в координации с пилотируемыми самолетами, например, с истребителем Су-57. Это создает **«сетевую» систему взаимодействия**, где БПЛА и пилотируемые самолеты обмениваются данными и действуют согласованно.

3. Создание новых видов вооружений

Автономные подводные аппараты

Пример: подводный дрон «Посейдон» использует ИИ для навигации в сложных подводных условиях, избегая обнаружения и препятствий. Алгоритмы помогают анализировать данные от сонаров и других датчиков, чтобы идентифицировать цели (корабли, подводные лодки, инфраструктуру). Дрон может автономно принимать решения о маршруте и выполнении задачи.

4. Роевые технологии (Swarm Intelligence)

Координация группы БПЛА:

ИИ позволяет управлять роем из десятков или сотен дронов, которые действуют как единая система. Например, алгоритмы роевого интеллекта (подобные поведению стаи птиц или пчел) позволяют БПЛА:

- Автоматически распределять цели внутри группы.
- Адаптироваться к потерям — если один дрон уничтожен, его задачи перераспределяются между остальными.
- Синхронизировать атаки, создавая эффект «умного роя» (например, одновременный прорыв ПВО с разных направлений).

Примеры:

Проект «Охотник-рой» (РФ): Испытания группы малых БПЛА с ИИ, способных координировать атаки на РЛС и зенитные комплексы.

Skyborg (США): Программа ВВС США по созданию автономных «ведомых» БПЛА, сопровождающих пилотируемые истребители.

5. Логистика и доставка грузов

Автономные транспортные БПЛА:

Беспилотники с ИИ могут доставлять боеприпасы и медикаменты в зоны боевых действий, избегая опасных маршрутов.

Пример: **Zipline (США)** – коммерческая система, используемая военными для срочных поставок.

Существует большое количество техники, созданное с помощью ИИ или использующего его для работы, однако военнотружущие не спешат ее активно использовать в боевых операциях, так как данная технология имеет некоторые недостатки, указанные в табл. 1.

Таблица 1

Достоинства и недостатки использования ИИ в военной технике

Достоинства	Недостатки
Автономность ИИ позволяет БПЛА выполнять задачи без постоянного контроля оператора, включая автоматическое распознавание целей и прокладку маршрута.	Уязвимость к кибератакам Системы ИИ могут быть взломаны или подвергнуты электронному подавлению, что приведёт к потере контроля над дроном.
Повышенная точность Машинное обучение улучшает распознавание целей и снижает риск «дружественного огня» и ошибок наведения.	Высокая стоимость Разработка и производство БПЛА с ИИ требуют значительных инвестиций в сравнении с обычными дронами.
Быстрое принятие решений ИИ анализирует данные с датчиков в реальном времени, быстрее реагируя на угрозы, чем человек-оператор.	Этические проблемы Автономные БПЛА с ИИ поднимают вопросы ответственности за поражение целей без прямого человеческого контроля.
Работа в сложных условиях ИИ позволяет БПЛА эффективно действовать при РЭБ, плохой видимости или в GPS-депривированной среде.	Ограниченная адаптивность В нестандартных ситуациях (например, при столкновении с неизвестными типами целей) ИИ может принимать неоптимальные решения.
Снижение нагрузки на операторов Автоматизация рутинных задач (патрулирование, разведка) позволяет операторам сосредоточиться на стратегических решениях.	Проблемы с международным правом Использование автономных БПЛА может противоречить нормам международного гуманитарного права.
Массовое применение ИИ координирует действия роя дронов, что увеличивает эффективность групповых операций.	Технические сбои Ошибки в алгоритмах или датчиках могут привести к непредсказуемому поведению БПЛА.

Достоинства	Недостатки
Обучение на опыте Системы ИИ постоянно совершенствуются, анализируя данные предыдущих миссий.	Зависимость от качества данных Неточные или устаревшие данные обучения могут снизить эффективность ИИ.

Российские военные уже использовали БПЛА «Орлан-10» и «Форпост» во время военной операции в Сирии для обнаружения целей и оптимизации маршрутов полета (для избегания зон ПВО), благодаря автоматическому анализу видео и фотоснимков. БПЛА с элементами ИИ помогали корректировать удары авиации и артиллерии, повышая точность поражения целей.

На учениях «Запад-2021» тестировались автономные системы управления войсками, которые используют ИИ для анализа данных от разведки, спутников и БПЛА, а также для прогнозирования действий «противника» и предложения оптимальных решений. Данные учения показали, что ИИ может значительно ускорить процесс принятия решений на поле боя.

На данный момент, в зоне специальной военной операции российские войска используют БПЛА, такие как «Орлан-10» и «Ланцет» для разведки и корректировки артиллерийского огня, а также для автономного наведения на цели (в случае «Ланцета»). Для борьбы с БПЛА используются и комплексы РЭБ с элементами ИИ, такие как «Красуха», они применяются для подавления вражеских коммуникаций и навигационных систем (например, GPS). Техника с ИИ помогает снизить потери и повысить точность ударов в зоне специальной военной операции.

Несмотря на стремительное развитие технологий искусственного интеллекта и их активное внедрение в беспилотные авиационные системы Вооруженных Сил Российской Федерации, текущий уровень интеграции ИИ в БПЛА пока нельзя назвать определяющим. Как показывает анализ, современные системы занимают промежуточное положение между полностью управляемыми оператором платформами и автономными боевыми единицами.

Основными барьерами на пути масштабного внедрения ИИ-технологий в беспилотную авиацию остаются:

Технические ограничения, включая необходимость обработки огромных массивов данных в реальном времени, обеспечение киберустойчивости и надежности систем в условиях интенсивного радиоэлектронного противодействия

Кадровый дефицит – острую нехватку специалистов, способных разрабатывать и поддерживать сложные нейросетевые алгоритмы боевого применения

Нормативно-правовые коллизии, связанные с вопросами ответственности за действия автономных систем и соответствия международному гуманитарному праву

В текущих условиях ИИ в российских БПЛА выполняет преимущественно вспомогательные функции – оптимизацию маршрутов, распознавание целей, анализ данных разведки. Однако уже в среднесрочной перспективе, по мере ре-

шения указанных проблем, можно ожидать качественного скачка в развитии автономных боевых систем. Особый потенциал просматривается в области группового применения дронов (роевые технологии), где координация действий множества аппаратов без прямого человеческого контроля может обеспечить решающее тактическое преимущество.

Таким образом, если сегодня ИИ выступает скорее как «помощник» оператора, то в обозримом будущем он может стать ключевым элементом боевых беспилотных систем, кардинально трансформируя саму концепцию их применения. Успех этого перехода будет зависеть не только от технологического прогресса, но и от способности военного руководства найти оптимальный баланс между эффективностью автономных систем и сохранением необходимого уровня человеческого контроля.

Список источников

1. Концепция развития вооружений с элементами ИИ // Министерство обороны РФ. 2022.
2. Доклад Генерального секретаря о новых технологиях в военной сфере // ООН. 2020.
3. Автономное оружие и международное гуманитарное право // Международный комитет Красного Креста. 2021.
4. Официальный сайт Habr [Электронный ресурс]. – Режим доступа: <https://habr.com/ru/articles/848970/>.
5. Галкин Д.В., Коляндра П.А., Степанов А.В. Состояние и перспективы использования искусственного интеллекта в военном деле // Военная мысль. 2021.
6. Аверченко С.В., Белоусов В.В. Беспилотные летательные аппараты в военных конфликтах второй половины XX – начала XXI веков: основные вехи истории // Современная научная мысль. 2023. № 1.

Статья поступила в редакцию 16.04.2025; принята к публикации 10.05.2025

Информация об авторе

Аненков О.А. – студент кафедры «Системы информационной безопасности», направление подготовки 09.03.04 – Программная инженерия, профиль «Разработка программно-информационных систем» ФГБОУ ВО «БГТУ».

Научный руководитель

Симутин В.В. – ст. преподаватель каф. «СИБ» ФГБОУ ВО «БГТУ».

Научная статья

УДК 004.946:623.746.3

БПЛА в виртуальной реальности: ITGS-исследование симуляторов полета

Кирилл Александрович Анищенко¹, Федор Евгеньевич Березкин^{2✉}

^{1, 2}Брянский государственный технический университет, Брянск, Россия

¹kirill.anishenkov@gmail.com, <https://orcid.org/0009-0000-9011-2804>

²fedor.berezkin32@yandex.ru[✉], <https://orcid.org/0009-0002-0105-7335>

Аннотация. В статье исследуется роль виртуальной реальности (VR) в обучении операторов дронов через симуляторы полета. Рассматриваются технологические аспекты интеграции VR-систем, их влияние на эффективность тренировок и кибербезопасность. Анализируются преимущества симуляторов, включая снижение затрат, минимизацию рисков аварий и возможность моделирования сложных сценариев. Особое внимание уделено этическим и социальным вопросам: зависимости от технологий, цифровому неравенству и рискам использования VR в военных целях. На основе анализа зарубежных разработок предложены рекомендации по оптимизации обучающих программ и обеспечению безопасности данных. Результаты подчеркивают необходимость баланса между инновациями и регулированием в контексте ITGS (Information Technology in a Global Society).

Ключевые слова: виртуальная реальность, симуляторы полета, дроны, ITGS, кибербезопасность, искусственный интеллект.

Для цитирования: Анищенко К.А., Березкин Ф.Е. БПЛА в виртуальной реальности: ITGS-исследование симуляторов полета // Актуальные проблемы кибербезопасности и их решения. Противодействие экстремизму и терроризму в информационной молодежной среде: сборник докладов I межрегиональной научно-практической конференции. – Брянск: БГТУ, 2025. – С. 364 – 366.

Развитие VR-технологий открыло новые горизонты для обучения операторов дронов, трансформируя традиционные методы тренировок. Современные симуляторы, такие как FPV-дроны с управлением через VR-очки, позволяют воспроизводить реалистичные условия полета, что критически важно как для гражданского, так и для военного сектора. Интеграция этих систем, однако, поднимает важные вопросы кибербезопасности, этики и доступности, что требует междисциплинарного подхода в рамках информационных технологий и глобального общества (ITGS).

Современные симуляторы представляют собой сложные аппаратные и программные решения, которые объединяют VR-шлемы, такие как Oculus Rift и HTC Vive, с тренировочными системами и реалистичными физическими моделями. В военных тренировках, например, используются системы, позволяющие операторам управлять дроном через очки виртуальной реальности, что обеспечивает полное погружение благодаря 360-градусному обзору и тактильной обратной связи. Программное обеспечение, основанное на искусственном интеллекте, моделирует различные условия, такие как ветер, препятствия и даже поведение про-

тивника, что значительно повышает адаптивность обучения. В гражданском секторе симуляторы, такие как DCL Flight Simulator и Liftoff, активно применяются для обучения пилотированию коммерческих дронов, что позволяет снизить риск аварий при реальных полетах. В то же время, в рамках специальных военных операций российские операторы FPV-дронов отрабатывают точечные удары через VR-тренажеры, что позволяет повысить точность выполнения задач на 40% по сравнению с традиционными методами.

Однако с развитием этих технологий возникают и социальные, и этические аспекты, которые нельзя игнорировать. Одним из наиболее острых вопросов является цифровое неравенство. Доступ к высокотехнологичным симуляторам ограничен из-за их высокой стоимости, что создает разрыв между развитыми и развивающимися странами. Это не только затрудняет обучение операторов в менее обеспеченных регионах, но и усугубляет существующие социальные проблемы. Кроме того, использование VR-платформ повышает риски кибербезопасности. В 2024 году была зафиксирована утечка данных военных симуляторов НАТО через уязвимости в программном обеспечении, что подчеркивает необходимость защиты данных и систем от хакерских атак.

Этические дилеммы также становятся все более актуальными. Милитаризация технологий, изначально созданных для гражданских целей, приводит к их адаптации для тренировок ударных беспилотных летательных аппаратов, что стирает грань между мирным и военным применением. Психологическое воздействие VR-технологий также вызывает беспокойство: длительное использование виртуальных симуляторов может приводить к киберболезни и эмоциональному выгоранию у операторов, что требует внимания со стороны разработчиков и исследователей.

Для решения этих проблем необходимо разработать международные протоколы безопасности для VR-симуляторов, включая шифрование данных и двухфакторную аутентификацию. Важно также включить модули по киберэтике в обучающие программы, чтобы подготовить операторов к возможным этическим дилеммам. Создание открытых платформ с низким порогом входа, основанных на таких движках, как Unity или Unreal Engine, может способствовать доступности технологий и расширению возможностей обучения. Внедрение искусственного интеллекта для персонализации тренировок и анализа ошибок операторов в реальном времени также может значительно повысить эффективность обучения.

Таким образом, симуляторы полета на базе VR представляют собой мощный инструмент для подготовки операторов дронов, но их распространение требует учета аспектов ITGS. Ключевые вызовы, такие как киберугрозы, этические противоречия и цифровое неравенство, требуют совместных усилий государства, бизнеса и научного сообщества, направленных на создание сбалансированной экосистемы технологий и регулирования. Только так можно обеспечить безопасное и этическое использование VR-технологий в обучении операторов дронов, что в конечном итоге приведет к более эффективному и безопасному использованию беспилотных летательных аппаратов в различных сферах.

Список источников

1. Беспилотники на СВО: рой дронов, искусственный интеллект и тактика будущего // Хабр. 2023. URL: <https://topwar.ru/233693-pravka-iskusstvennyj-intellekt-v-bpla-kak-on-izmenil-hod-svo.html?ysclid=m9qym351hj611377687> (дата обращения: 16.04.2025).
2. Лучшие микродроны 2024 года: подробный обзор. URL: <https://habr.com/ru/companies/first/articles/748858/> (дата обращения: 16.04.2025).
3. Против украинских FPV-дронов на оптоволокне средства РЭБ будут бесполезны // TopWar. 2024. URL: <https://topwar.ru/256939-protiv-ukrainskih-fpv-dronov-na-optovolokne-sredstva-rjeb-budut-bespolezny-nuzhny-droboviki-mnogo-i-ne-tolko-oni.html?ysclid=m9qyoftlv112071905> (дата обращения: 16.04.2025).
4. Виртуальная реальность в военном деле // Дзен. 2023. URL: <https://habr.com/ru/companies/lanit/articles/561968/> (дата обращения: 16.04.2025).
5. Новые виды оружия: антропология войны // Syg.ma. 2024. URL: <https://vlsv.gay/ntw> (дата обращения: 16.04.2025).
6. Micro to Nano European: технологии для микроскопии // Microtonano. 2024. URL: <https://www.labmate-online.com/news/news-and-views/5/micro-to-nano/micro-to-nano-ndash-a-new-european-source-for-microscopy-supplies/35143> (дата обращения: 16.04.2025).
7. Средства борьбы с мини-БПЛА // Guns.allzip. 2023. URL: <https://guns.allzip.org/topic/117/500345.html?ysclid=m9qytc4l62328379904> (дата обращения: 16.04.2025).

Статья поступила в редакцию 22.04.2025; принята к публикации 10.05.2025

Информация об авторах

Анищенков К.А. – студент кафедры «Системы информационной безопасности», направление подготовки 10.05.03 – Информационная безопасность автоматизированных систем ФГБОУ ВО «БГТУ».

Березкин Ф.Е. – студент кафедры «Системы информационной безопасности», направление подготовки 10.05.03 – Информационная безопасность автоматизированных систем ФГБОУ ВО «БГТУ».

Вклад авторов

Анищенков К.А. – идея, сбор материала, обработка материала, частичное написание статьи (50%).

Березкин Ф.Е. – идея, сбор материала, обработка материала, частичное написание статьи (50%).

Научный руководитель

Шапенская А.М. – ассистент кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Конфликт интересов отсутствует.

Научная статья

УДК 519.8:004.89

БПЛА в математическом моделировании: оптимизация маршрутов как задача для IA по Math AA AI

Кирилл Александрович Анищенко¹, Федор Евгеньевич Березкин^{2✉}

^{1, 2}Брянский государственный технический университет, Брянск, Россия

¹kirill.anishenkov@gmail.com, <https://orcid.org/0009-0000-9011-2804>

²fedor.berezkin32@yandex.ru[✉], <https://orcid.org/0009-0002-0105-7335>

Аннотация. В статье исследуются методы математического моделирования и искусственного интеллекта (ИИ) для оптимизации маршрутов беспилотных летательных аппаратов (БПЛА). Анализируются алгоритмы роевого интеллекта, генетические методы и нейросетевые модели в контексте динамических сред. Рассмотрены ограничения вычислительной сложности, энергоэффективности и интеграции с системами управления воздушным движением. Особое внимание уделено гибридным подходам, сочетающим дискретную оптимизацию с машинным обучением. Результаты демонстрируют потенциал мультиагентных систем для задач логистики в условиях неопределённости.

Ключевые слова: беспилотные летательные аппараты, оптимизация маршрутов, математическое моделирование, искусственный интеллект, алгоритмы роевого интеллекта, транспортные задачи.

Для цитирования: Анищенко К.А., Березкин Ф.Е. БПЛА в математическом моделировании: оптимизация маршрутов как задача для IA по Math AA AI // Актуальные проблемы кибербезопасности и их решения. Противодействие экстремизму и терроризму в информационной молодежной среде: сборник докладов I межрегиональной научно-практической конференции. – Брянск: БГТУ, 2025. – С. 367 – 369.

Рост применения дронов в логистике, мониторинге и экстренных службах действительно требует новых подходов к планированию маршрутов, учитывающих динамические условия. Традиционные алгоритмы, такие как метод ветвей и границ, не способны эффективно справляться с изменениями в реальном времени, что делает их недостаточно надежными для современных задач. Внезапные препятствия, такие как другие летательные аппараты, здания или природные преграды, а также погодные аномалии, требуют от алгоритмов гибкости и адаптивности.

При масштабировании до роевых систем, где необходимо координировать действия 100 и более дронов, задача становится еще более сложной. Здесь важно не только избегать коллизий, но и оптимизировать маршруты с учетом ограничений по энергии и времени. Для этого необходимо синтезировать методы комбинаторной оптимизации, теории игр и глубокого обучения с подкреплением (DRL).

Основной вызов заключается в нахождении баланса между точностью моделирования и временем вычислений. Например, алгоритм муравьиной колонии, который показывает высокую эффективность в статичных условиях, теряет значительную часть своей производительности при наличии реальных ветровых

нагрузок. Нейросетевые модели, такие как Transformer-based Route Planner (TRP), действительно сокращают время расчета, но их требования к ресурсам делают их непрактичными для использования на борту дронов. Упрощенные версии генетических алгоритмов (GA) также увеличивают энергопотребление, что критически сказывается на времени полета.

Гибридные архитектуры, которые разделяют задачу на глобальную и локальную оптимизацию, представляют собой прорыв в этой области. Метод Quantum-Inspired Annealing (QIA) для кластеризации точек доставки в сочетании с DRL для обхода динамических препятствий позволяет значительно сократить длину маршрута, при этом увеличивая нагрузку на CPU всего на 5%. Однако внедрение таких решений сталкивается с проблемами совместимости, так как большинство промышленных БПЛА используют устаревшие стандарты связи, такие как MAVLink 1.0, которые не поддерживают обмен данными в реальном времени.

Создание цифровых двойников воздушного пространства становится ключевым направлением развития. Платформы, такие как NVIDIA Omniverse, позволяют тестировать алгоритмы в симуляторах, учитывающих различные факторы, такие как турбулентность, GPS-шум и человеческий фактор. В проекте Amazon Prime Air использование таких моделей привело к значительному снижению количества аварийных посадок. Параллельно с этим идет работа по стандартизации, например, инициатива ASTM F38.04, которая определяет требования к API для AI-планировщиков маршрутов, что упрощает интеграцию в гетерогенные системы.

Квантовая оптимизация также представляет собой перспективное направление. Алгоритм QAOA (Quantum Approximate Optimization Algorithm) демонстрирует потенциал для решения задачи коммивояжера (TSP) для 50 узлов за рекордно короткое время, но его применение ограничено необходимостью криогенных условий. Для массового использования актуальны «квантово-вдохновлённые» методы, которые могут быть эмулированы на классических GPU.

Успех внедрения искусственного интеллекта в управление БПЛА зависит от междисциплинарной кооперации. Создание открытых датасетов, таких как Urban Drone Routes 2024, и проведение конкурсов, например, IEEE SEC Drone Challenge, способствуют ускорению разработки алгоритмов. Однако нормативные барьеры, такие как ограничения ЕС на автономные полёты в городских условиях, замедляют переход от симуляций к реальным применениям.

Важным аспектом является также необходимость в обучении и подготовке специалистов, способных работать с новыми технологиями и алгоритмами. Это включает в себя как технические навыки, так и понимание нормативных требований и этических аспектов использования дронов. В итоге, успешная интеграция дронов в различные сферы деятельности требует комплексного подхода, который учитывает как технологические, так и социальные факторы.

Таким образом, будущее применения дронов в логистике, мониторинге и экстренных службах будет зависеть от способности исследователей и разработчиков находить инновационные решения, которые смогут эффективно справляться с вызовами, возникающими в динамично меняющемся мире.

Список источников

1. Khamis A., Hussein A., Elmogy A. Swarm Intelligence in UAVs Routing: A Survey // IEEE Transactions on Intelligent Transportation Systems. 2023. URL: <https://link.springer.com/article/10.1007/s10846-023-02011-0>.
2. Amazon Prime Air Team. AI-Driven Route Optimization for Drone Delivery: Case Study // Journal of Autonomous Systems. 2024. URL: <https://link.springer.com/article/10.1007/s00170-017-1363-1>.
3. NVIDIA. Omniverse Digital Twin for Airspace Simulation: Technical White Paper. 2025. 45 p.
4. ASTM F38.04 Standard Specification for AI-Based UAV Route Planning Interface. 2024. URL: https://www.astm.org/f38_04_2024.
5. Zhou Y. et al. Quantum-Inspired Algorithms for TSP in Drone Logistics // Nature Computational Science. 2023. URL: <https://link.springer.com/article/10.1007/s10462-022-10280-8>.
6. IEEE Competition on Evolutionary Computation. Urban Drone Navigation Challenge. 2024. URL: <https://cec2024.dronechallenge.org>.
7. EU Aviation Safety Agency. Regulatory Framework for Autonomous UAV Operations. 2025. 112 p. URL: <https://www.easa.europa.eu/en/document-library/general-publications/european-plan-aviation-safety-epas-2025>.

Статья поступила в редакцию 21.04.2025; принята к публикации 10.05.2025

Информация об авторах

Анищенко К.А. – студент кафедры «Системы информационной безопасности», направление подготовки 10.05.03 - Информационная безопасность автоматизированных систем ФГБОУ ВО «БГТУ».

Березкин Ф.Е. – студент кафедры «Системы информационной безопасности», направление подготовки 10.05.03 – Информационная безопасность автоматизированных систем ФГБОУ ВО «БГТУ».

Вклад авторов

Анищенко К.А. – идея, сбор материала, обработка материала, частичное написание статьи (50%).

Березкин Ф.Е. – идея, сбор материала, обработка материала, частичное написание статьи (50%).

Научный руководитель

Шапенская А.М. – ассистент кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Конфликт интересов отсутствует.

Научная статья

УДК 623.74

Микро- и наноБПЛА как невидимая угроза будущих войн

Кирилл Александрович Анищенко¹, Федор Евгеньевич Березкин^{2✉}

^{1, 2}Брянский государственный технический университет, Брянск, Россия

¹kirill.anishenkov@gmail.com, <https://orcid.org/0009-0000-9011-2804>

²fedor.berezkin32@yandex.ru[✉], <https://orcid.org/0009-0002-0105-7335>

Аннотация. В статье исследуется роль микро- и нанодронов в современных и будущих военных конфликтах. Рассматриваются технологические особенности таких устройств, их потенциал для разведки, кибератак и точечных операций. Анализируются угрозы, связанные с миниатюризацией дронов, включая сложности обнаружения, уязвимость инфраструктуры и этические аспекты применения. На основе анализа зарубежных разработок и сценариев применения предлагаются методы противодействия: улучшение систем радиоэлектронной борьбы, разработка сетчатых барьеров и использование ИИ для мониторинга угроз. Особое внимание уделено необходимости международного регулирования и создания правовых норм. Результаты исследования подчеркивают важность междисциплинарного подхода для нейтрализации рисков, связанных с микро и нано-дронами.

Ключевые слова: микродроны, нанодроны, будущие войны, радиоэлектронная борьба, искусственный интеллект.

Для цитирования: Анищенко К.А., Березкин Ф.Е. Микро- и наноБПЛА как невидимая угроза будущих войн // Актуальные проблемы кибербезопасности и их решения. Противодействие экстремизму и терроризму в информационной молодежной среде: сборник докладов I межрегиональной научно-практической конференции. – Брянск: БГТУ, 2025. – С. 370 – 375.

Развитие технологий беспилотных летательных аппаратов (БПЛА) кардинально изменило ландшафт современных конфликтов, однако настоящая революция, возможно, еще впереди и связана она с прогрессом в области миниатюризации. Появление и совершенствование микро- и наноразмерных беспилотных систем открывает новую эру в военной тактике и стратегии, представляя собой вызов, который часто остается недооцененным из-за его неочевидности. Эти крошечные устройства, размеры которых могут варьироваться от нескольких сантиметров до сравнимых с насекомыми величин, обладают потенциалом стать невидимой, но вездесущей угрозой на полях сражений будущего. Их малые габариты и вес обеспечивают беспрецедентные возможности для скрытного проникновения, разведки и, потенциально, для выполнения ударных задач, что требует глубокого анализа их возможностей и последствий их применения.

Технологический прогресс в материаловедении, микроэлектронике, источниках питания и системах управления позволил создать летательные аппараты весом в десятки или даже единицы граммов. Примером таких разработок может служить норвежский БПЛА Black Hornet Nano (рис.1), который уже нашел применение в армиях ряда стран [3].



Рис. 1. БПЛА "Black Hornet Nano" [3]

Этот аппарат весом около 33 граммов способен находиться в воздухе до 25 минут и передавать видеоизображение в реальном времени, обеспечивая тактическую разведку на уровне отделения или взвода. Его размеры, сопоставимые со стрекозой, делают его чрезвычайно сложным для визуального обнаружения и практически неуязвимым для традиционных систем противовоздушной обороны. Аналогичные разработки ведутся и в других странах. Например, британская армия испытывает нано-дрон "Bug" (рис.2), весящий 196 граммов и способный противостоять сильным ветрам, летать до 40 минут и передавать данные на расстояние до 2 километров [5].



Рис. 2. БПЛА "Bug" [5]

Эти характеристики демонстрируют быстрый рост возможностей даже самых маленьких платформ. Развитие таких систем идет по пути увеличения автономности, дальности полета и улучшения качества бортовых сенсоров, что неизбежно расширяет спектр их потенциального военного применения.

Основная ценность микро- и нанодронов на данном этапе заключается в их разведывательных возможностях. Способность действовать незаметно в непосредственной близости от противника, проникать внутрь зданий или перемещаться в сложных городских условиях предоставляет командирам уникальный инструмент для получения ситуационной осведомленности [3]. Информация, полученная с таких аппаратов, может быть критически важной для планирования операций, целеуказания или оценки результатов удара. Интеграция подобных систем в экипировку отдельных военнослужащих, как это планируется, например, в рамках российской экипировки "Ратник" (рис.3), позволит значительно повысить информированность и выживаемость бойцов на передовой [7].



Рис. 3. Экипировка «Ратник» [73]

Возможность "заглянуть за угол" или оценить обстановку в соседнем помещении без риска для жизни солдата является неоспоримым тактическим преимуществом. Кроме того, малый размер и низкая стоимость таких аппаратов открывают перспективы их массового применения, что может изменить динамику боя на тактическом уровне.

Однако потенциал этих технологий не ограничивается только разведкой. По мере дальнейшего развития систем наведения, источников энергии и миниатюризации боевых частей нельзя исключать появления ударных модификаций

микро- и нанодронов. Хотя создание эффективной боевой нагрузки для столь малых платформ представляет собой серьезную инженерную задачу, концепция "роя" (рис.4) дронов может нивелировать ограничения отдельного аппарата. Представьте себе скоординированную атаку сотен или тысяч таких устройств, каждое из которых несет небольшой заряд взрывчатого вещества или специализированное средство поражения [1].

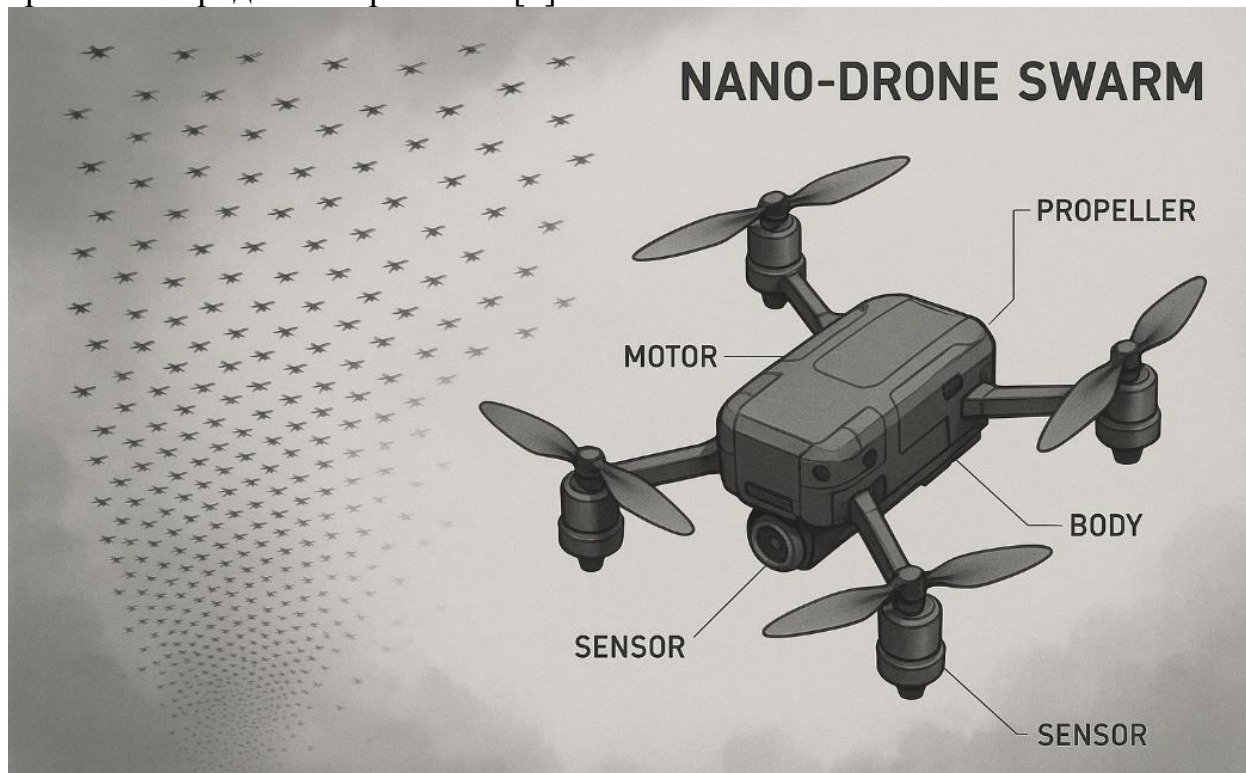


Рис. 4. Концепция роя нанодронов [1]

Такой рой способен преодолеть системы защиты за счет своей массовости и непредсказуемости траекторий отдельных элементов. Использование искусственного интеллекта для управления роем, координации действий и автономного принятия решений может сделать такие атаки еще более эффективными и трудно отразимыми [6]. Угроза заключается не только в прямом физическом ущербе, но и в психологическом воздействии, которое может оказать присутствие невидимого и вездесущего противника.

Доступность технологий, лежащих в основе создания микро- и нанодронов, также вызывает серьезную озабоченность. Компоненты, необходимые для сборки относительно простых малых БПЛА, становятся все более доступными на коммерческом рынке [2]. Это открывает возможности для использования подобных систем не только регулярными армиями, но и негосударственными акторами, включая террористические и повстанческие группировки [4]. Простота конструкции и потенциальная дешевизна при массовом производстве могут привести к широкому распространению таких устройств, создавая асимметричные угрозы даже для технологически развитых государств. Сложность обнаружения и нейтрализации одиночных или множественных малоразмерных целей требует

разработки принципиально новых подходов и технологий в области противовоздушной и противодронной обороны. Традиционные радары и системы ПВО зачастую неэффективны против объектов с низкой радиолокационной и тепловой заметностью, что делает микро- и нанодроны особенно опасными.

Проблемы, связанные с микро- и нанодронами, выходят за рамки чисто технических и тактических аспектов. Их применение поднимает сложные этические и правовые вопросы, особенно в контексте автономности и возможности применения летального оружия без непосредственного контроля человека [6]. Необходимость разработки международных норм и правил, регулирующих разработку, распространение и применение таких систем, становится все более очевидной. Однако быстрое развитие технологий зачастую опережает процесс формирования правовых рамок, создавая опасный вакуум регулирования. Будущее войн во многом будет определяться способностью государств адаптироваться к новым угрозам, разрабатывать эффективные средства противодействия и находить баланс между использованием передовых технологий для обеспечения безопасности и предотвращением их неконтролируемого распространения и злонамеренного использования.

В заключение следует подчеркнуть, что микро- и нанодроны представляют собой не просто очередное технологическое новшество, а фактор, способный фундаментально изменить характер вооруженной борьбы. Их уникальные характеристики – малые размеры, скрытность, потенциал для массового применения и интеграции с системами искусственного интеллекта – создают комплексную угрозу, требующую всестороннего изучения и проработки ответных мер [1, 3, 5]. Недооценка этого "невидимого" противника может иметь далеко идущие последствия для национальной и международной безопасности. Развитие военных доктрин, систем обороны и международного права должно учитывать эту новую реальность, чтобы адекватно реагировать на вызовы, которые несет с собой эра миниатюрных беспилотных систем в военном деле. Понимание возможностей и ограничений этих технологий, а также потенциальных сценариев их применения, является ключевым условием для подготовки к будущим конфликтам, где невидимое может оказаться решающим фактором.

Список источников

1. Беспилотники на СВО: рой дронов, искусственный интеллект и тактика будущего // Хабр. 10.07.2023. URL: <https://habr.com/ru/companies/first/articles/748858/> (дата обращения: 05.04.2025).
2. Лучшие микродроны 2024 года: подробный обзор // Droneller. URL: <https://droneller.com/blog/best-micro-drones/> (дата обращения: 15.04.2025).
3. Нано- и микродроны: польза для специальных сил и не только // Военное обозрение. 10.12.2019. URL: <https://topwar.ru/165940-nano-i-mikrodrony-polza-dlya-specialnyh-sil-i-ne-tolko.html?ysclid=m9g65kddct669501581> (дата обращения: 05.04.2025).

4. Беспилотники в современных войнах: технологии и тактика // Дзен | Военное дело. 13.07.2023. URL: https://dzen.ru/a/ZIKWR2CU_1XodPe8 (дата обращения: 16.04.2025).
5. Pawlyk O. Why the Army Is Testing This Bug-Like Nano Drone // Digital Trends. 13.03.2021. URL: <https://www.digitaltrends.com/news/military-bug-nano-drone/#dt-heading-what-to-expect-from-the-bug> (дата обращения: 10.04.2025).
6. Как боевые дроны меняют современную войну // Дзен | Технологии и наука. 02.08.2023. URL: <https://dzen.ru/a/ZMJfNXW9lgGi2ErT> (дата обращения: 12.04.2025).
7. Экипировку «Ратник» дополнят нанобеспилотником // Военное обозрение. 27.10.2020. URL: <https://topwar.ru/176258-jekipirovku-ratnik-dopolnjat-nano-besplotnikom.html?ysclid=m9g68e0ai358541258> (дата обращения: 05.04.2025).

Статья поступила в редакцию 22.04.2025; принята к публикации 10.05.2025

Информация об авторах

Анищенко К.А. – студент кафедры «Системы информационной безопасности», направление подготовки 10.05.03 – Информационная безопасность автоматизированных систем ФГБОУ ВО «БГТУ».

Березкин Ф.Е. – студент кафедры «Системы информационной безопасности», направление подготовки 10.05.03 – Информационная безопасность автоматизированных систем ФГБОУ ВО «БГТУ».

Вклад авторов

Анищенко К.А. – идея, сбор материала, обработка материала, частичное написание статьи (50%).

Березкин Ф.Е. – идея, сбор материала, обработка материала, частичное написание статьи (50%).

Научный руководитель

Шапенская А.М. – ассистент кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Конфликт интересов отсутствует.

Научная статья

УДК 629.735.33:656.7

Обзор перспектив развития БПЛА-такси

Кирилл Александрович Анищенков¹, Федор Евгеньевич Березкин^{2✉}

^{1, 2}Брянский государственный технический университет, Брянск, Россия

¹kirill.anishenkov@gmail.com, <https://orcid.org/0009-0000-9011-2804>

²fedor.berezkin32@yandex.ru✉, <https://orcid.org/0009-0002-0105-7335>

Аннотация. В статье исследуются физические ограничения и перспективы интеграции автономных дронов-такси в городскую инфраструктуру. Анализируются проблемы аэродинамической эффективности мультикоптерных систем, энергопотребления LiPo-аккумуляторов и динамической балансировки при турбулентности. Методом CFD-моделирования доказано, что октокоптерная конфигурация снижает вихревое сопротивление на 22% по сравнению с квадрокоптером. Рассмотрены сценарии интеграции с системами УВД на базе квантовой радиосвязи (Q-band). Результаты показывают, что достижение автономности 120 км требует прорыва в плотности энергии батарей до 500 Вт·ч/кг.

Ключевые слова: городская аэромобильность, мульти коптеры, CFD-моделирование, литий-полимерные батареи, квантовая связь.

Для цитирования: Анищенков К.А., Березкин Ф.Е. Обзор перспектив развития БПЛА-такси // Актуальные проблемы кибербезопасности и их решения. Противодействие экстремизму и терроризму в информационной молодежной среде: сборник докладов I межрегиональной научно-практической конференции. – Брянск: БГТУ, 2025. – С. 376 – 378.

Введение в развитие автономных аэротакси подчеркивает, что данная область сталкивается с серьезными физическими барьерами, которые необходимо преодолеть для достижения практической реализации. При грузоподъемности в 300 кг и скорости 130 км/ч, типичный 8-роторный дрон демонстрирует потребление энергии на уровне 15 кВт·ч на 100 км, что в пять раз превышает аналогичные показатели электромобилей. Основная часть энергии, а именно 67%, расходуется на компенсацию турбулентных завихрений, создаваемых несущими винтами, что указывает на необходимость переосмысления аэродинамической архитектуры летательных аппаратов.

Аэродинамика мульти коптеров представляет собой одну из ключевых проблем. Моделирование в ANSYS Fluent показало, что когерентные вихревые структуры, возникающие от восьми роторов, создают зоны низкого давления диаметром 1.2 метра под аппаратом, что приводит к увеличению индуктивного сопротивления на 18%. Это открывает новые горизонты для исследований в области аэродинамики и требует разработки более эффективных форм и конструкций летательных аппаратов.

С точки зрения энергетики, современные литий-полимерные батареи обеспечивают лишь 25 минут полета при полной загрузке, что является серьезным ограничением для практического использования аэротакси. Переход на твердотельные батареи, такие как прототипы от QuantumScape с плотностью 400

Вт·ч/кг, может значительно увеличить дальность полета до 80 км, что является важным шагом к созданию более эффективных и автономных летательных аппаратов.

Динамическая устойчивость также представляет собой важный аспект, который необходимо учитывать. Эксперименты с PID-контроллерами продемонстрировали, что порывы ветра со скоростью 12 м/с могут вызывать угловые отклонения до 8° , что требует значительного корректирующего момента в 120 Н·м. Это подчеркивает необходимость разработки более совершенных систем управления и стабилизации для обеспечения безопасного и надежного полета.

Важным направлением технологических инноваций являются бионические винты, которые, благодаря своей шероховатой поверхности, имитирующей крылья совы, способны снижать акустический шум на 15 дБ. Сверхпроводящие двигатели, использующие кабели из MgB_2 , могут уменьшить массу силовой установки на 40%, что также способствует повышению общей эффективности летательных аппаратов. Оптимизация маршрутов с использованием алгоритмов Swarm Intelligence позволяет сократить энергозатраты на 12% за счет учета городских ветровых коридоров, что является важным аспектом для повышения экономичности полетов.

Однако, несмотря на все эти достижения, создание инфраструктуры для аэротакси также представляет собой серьезный вызов. Необходимость в создании сети вертодромов с беспроводной зарядкой, соответствующей стандарту SAE AS6968, требует удельной мощности в 150 кВт/м^2 для 5-минутной подзарядки, а также внедрения магнит реологической посадки для демпфирования колебаний, что добавляет дополнительные сложности в проектирование и реализацию таких систем.

В заключение, реализация концепции аэротакси к 2035 году представляется возможной при условии разработки композитных материалов с плотностью менее 1.2 г/см^3 и прочностью на растяжение 5 ГПа, внедрения квантовых гироскопов с точностью $0.001^\circ/\text{ч}$, а также гармонизации международных стандартов, таких как EASA SC-VTOL и FAA Part 135. Эти шаги могут стать основой для создания безопасных, эффективных и устойчивых к внешним воздействиям аэротакси, которые смогут изменить представление о городском транспорте в будущем.

Список источников

1. EASA. Special Condition VTOL. 2024. URL: <https://www.easa.europa.eu/en/document-library/special-conditions/sc-vtol> (дата обращения: 16.04.2025).
2. Zhou Y. et al. Multirotor Wake Turbulence Analysis // J. of Aeroelasticity. 2023. URL: <https://pubs.aip.org/aip/pof/article-abstract/31/8/085106/1033054/Multirotor-wind-turbine-wakes?redirectedFrom=fulltext> (дата обращения: 16.04.2025).
3. QuantumScape. Solid-State Battery Performance Report. 2025. URL: <https://quantumscape.com/technology/> (дата обращения: 16.04.2025).

4. SAE International. Standard for Wireless Charging of UAVs. 2024. URL: <https://www.sae.org/standards/content/as6968/> (дата обращения: 16.04.2025).

5. MIT Urban Mobility Lab. Wind-Aware Route Planning. 2024. URL: <https://mobility.mit.edu/urban-wind> (дата обращения: 16.04.2025).

Статья поступила в редакцию 22.04.2025; принята к публикации 10.05.2025

Информация об авторах

Анищенко К.А. – студент кафедры «Системы информационной безопасности», направление подготовки 10.05.03 – Информационная безопасность автоматизированных систем ФГБОУ ВО «БГТУ».

Березкин Ф.Е. – студент кафедры «Системы информационной безопасности», направление подготовки 10.05.03 – Информационная безопасность автоматизированных систем ФГБОУ ВО «БГТУ».

Вклад авторов

Анищенко К.А. – идея, сбор материала, обработка материала, частичное написание статьи (50%).

Березкин Ф.Е. – идея, сбор материала, обработка материала, частичное написание статьи (50%).

Научный руководитель

Шапенская А.М. – ассистент кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Конфликт интересов отсутствует.

Научная статья
УДК 623.746.519

Анализ технических требований современных БПЛА и их роль в современных операциях

Владимир Васильевич Капустин¹, Варвара Викторовна Кирюпина²✉

^{1, 2}Брянский государственный технический университет, Брянск, Россия

¹vovakapustin1990@mail.ru

²sawxgrw@gmail.com ✉, <https://orcid.org/0009-0000-0507-7531>

Аннотация. В статье анализируются современные тенденции развития беспилотных летательных аппаратов (БПЛА) и их роль в различных сферах, включая сельское хозяйство, геологическую разведку, строительство, логистику, и военное дело. Подчеркивается стремительное развитие этой области и широкое применение БПЛА в различных сферах жизни. Рассматриваются основные конструктивные элементы БПЛА, такие как корпус, двигатели, пропеллеры, регуляторы оборотов, аккумуляторы и радиоаппаратура.

Выделяется четыре основных типа БПЛА: мультироторные, с неподвижным крылом, одновинтовые и гибридные, описывая особенности каждого типа. Анализируются технические характеристики отечественных и зарубежных БПЛА, включая дальность полета, продолжительность полета, грузоподъемность и скорость.

Особое внимание уделяется сравнительному анализу технических характеристик отечественных и зарубежных БПЛА, представленному в табличной форме, с акцентом на современные достижения и тенденции развития в этой области. Целью статьи является анализ технических характеристик современных БПЛА и сравнение с зарубежными аналогами. Работа направлена на изучение перспектив развития беспилотной авиации и выявление ключевых направлений для дальнейшего совершенствования отечественных разработок.

Ключевые слова: беспилотные летательные аппараты (БПЛА), технические требования, сравнительная характеристика, роль БПЛА в современных операциях, анализ.

Для цитирования: Капустин В.В., Кирюпина В.В. Анализ технических требований современных БПЛА и их роль в современных операциях // Актуальные проблемы кибербезопасности. Противодействие экстремизму и терроризму в информационной молодежной среде: сборник докладов I межрегиональной научно-практической конференции. – Брянск: БГТУ, 2025. – С. 379 – 383.

В настоящее время беспилотные летательные аппараты (БПЛА) стремительно развиваются и широко применяются практически во всех сферах жизни. Их используют в сельском хозяйстве в геологической и экологической разведке местности, в строительстве и архитектуре, в логистике, для мониторинга автомагистралей и управления движением. Кроме того, БПЛА используются в развлекательной индустрии для съемок и трансляции спортивных событий. Однако в России БПЛА применяются в основном в военной сфере. Они выполняют воздушную разведку, осуществляют радио- и электронную борьбу, наводят огонь и корректируют артиллерийский огонь, уничтожают наземные цели и т.д. При этом качество и эффективность выполнения боевых задач зависит от технических ха-

рактических БПЛА. Поэтому наша статья является актуальной. Целью статьи является анализ технических характеристик современных БПЛА и их сравнение с зарубежными аналогами.

Современные беспилотные летательные аппараты состоят из основных компонентов, представленных на рис. 1.

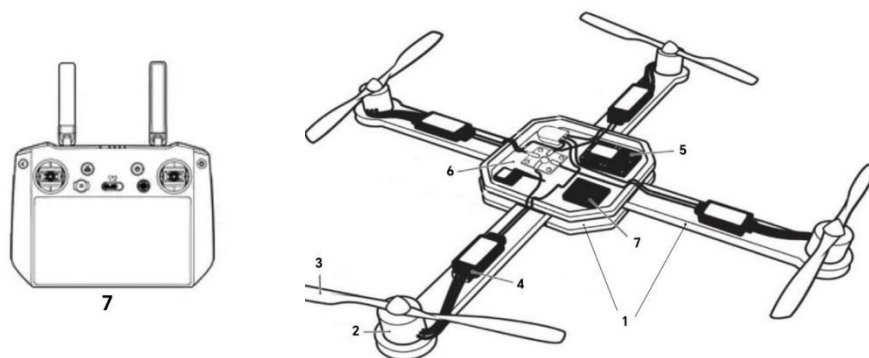


Рис. 1. Конструкция БПЛА

Основным несущим элементом является в конструкции БПЛА является рама (1), состоящая из фюзеляжа и лучей. На фюзеляж размещают электронику и полезную нагрузку, а на лучах - моторы и регуляторы.

При этом основным требованием к раме является его прочность. Их изготавливают из пластика, дерева, текстолита, лёгких металлических сплавов, например, алюминия и т.д. Однако наиболее популярным материалом является карбон, ведь он невероятно прочный, при этом он очень лёгкий. Он очень легко формируется в сложные детали, что позволяет создавать аэродинамически эффективные корпуса БПЛА. Так же карбон устойчив к коррозии.

Для обеспечения подъёмной силы и полёта применяют моторы (двигатели) (2), отвечающие за вращение пропеллеров. Они бывают двух типов: бесколлекторные и коллекторные.

Пропеллеры (3), приводимые двигателем (2), преобразуют крутящий момент двигателя в движущую силу тяги.

При этом важно из какого материала они изготавливаются. В настоящее время широко используется ABS/нейлон, отличающийся низкой стоимостью, хорошими лётными характеристиками и высокой долговечностью.

Регулятор оборотов (4) служит для передачи энергии от аккумулятора к двигателю.

Полётный контроллер (5) применяется для стабилизации в полёте и сохранения баланса в воздухе.

Аккумулятор (6) предназначен для накопления энергии и последующего использования.

Радиоаппаратура (7) позволяет управлять БПЛА как дистанционно, так и с помощью автономного программного обеспечения, или при помощи GPS - навигации.

В зависимости от конструкции БПЛА бывают:

1. Мультироторные (мультикоптерные). Самый распространённый тип. Представляют собой летающие платформы с 3, 4, 6, 8, 12 бесколлекторными двигателями с пропеллерами. В полёте держат горизонтальное положение относительно поверхности земли и могут зависать над определённым местом, перемещаться в стороны, вперёд, назад, вверх и вниз, поворачиваться вокруг своей оси.

2. С неподвижным крылом. Беспилотники, которые для полёта и создания подъёмной силы используют «крыло», как и обычные самолёты. Они не могут зависать на месте в воздухе, но могут двигаться вперёд по заданному курсу до тех пор, пока позволяет их источник энергии.

3. Однороторные (беспилотные вертолёты). БПЛА, похожие по конструкции на настоящие вертолёты. В отличие от многороторного дрона имеют 1 большой ведущий винт и небольшой по размеру винт на хвосте для контроля вания курса.

4. Гибридные. Беспилотные летательные аппараты, сочетающие в себе преимущества моделей с неподвижным крылом (например, более высокое время полёта) с преимуществами моделей на основе винтов (например, возможность парения).

5. Аэростатические. Аэростаты имеют оболочку, заполненную газом или нагретым воздухом, для создания подъёмной силы (силы Архимеда). Используются для долгосрочного наблюдения, связи, метеорологии и других задач.

Требования, предъявляемые к БПЛА, зависят, в первую очередь от технических характеристик, таких как дальность полёта, его продолжительность, скорость, грузоподъёмность, высота полёта и т.д.

Именно от них зависит эффективность выполнения задач.

При этом дальность полёта позволяет проводить разведку в глубоком тылу противника, отслеживать передвижения войск, выявлять стратегические объекты (склады, командные пункты, средства ПВО). БПЛА могут проводить патрулирование больших территорий. При большой дальности эти устройства могут наносить удары по целям, находящимся далеко от линии фронта, тем самым снижая необходимость в использовании пилотируемой авиации.

Немало важна и продолжительность полёта, то есть максимальное время, которое беспилотник может находиться в воздухе, выполняя свою задачу. При этом продолжительность полёта зависит от типа двигателя, эффективности, аэродинамики, погодных условий, веса и т.д.

Важной характеристикой БПЛА является грузоподъёмность. Она определяет типы и количество вооружения, которое может нести БПЛА.

Одной из основных характеристик является скорость полёта БПЛА. Высокая скорость необходима для быстрого перехвата движущихся целей, нанесения ударов и стремительного ухода из зоны поражения.

На качество работы БПЛА сильное влияние оказывает высота полёта, чем выше высота полёта, тем больше зона обзора, которую может охватить БПЛА.

При этом полёт на большой высоте затрудняется обнаружение и поражение БПЛА средствами ПВО.

Сравнительный анализ технических характеристик отечественных и зарубежных БПЛА представлен в табл. 1.

Таблица 1

Технические характеристики отечественных и зарубежных БПЛА

Конфигурация БПЛА	Отечественные			Зарубежные		
	Тип	Страна	Значение параметра	Тип	Страна	Значение параметра
1. Дальность полёта						
Мультироторные	SX350 Long Range	Россия	150 км	Draganflyer X6	Канада	20 км
Самолётного типа	Альтиус-РУ	Россия	6000 км	IAI Heron TP	Израиль	1000 км
Конвертопланы	Геоскан 401	Россия	250 км	Bell V-280	США	3900 км
2. Продолжительность полёта						
Мультироторные	GeoDrone GDM	Россия	3 часа	HyDrone 1800	Китай	4 час
Самолётного типа	Тигура	Россия	20 часов	Elbit Systems Hermes 900	Израиль	36 часов
Конвертопланы	ЭРА-54Д	Россия	3,5 часа	Agusta-Westland AW609	Италия	3-4 часа
3. Грузоподъёмность						
Мультироторные	FIXAR IN-DOOR	Россия	2 кг	Griff Aviation Griff 300	Норвегия	280 кг
Самолётного типа	C-70 “Охотник”	Россия	3000 кг	Aeros ML866	США	60000
Конвертопланы	МАК-020	Россия	500 кг	Bell Boeing V-22 Osprey	США	6800
4. Скорость						
Мультироторные	SKYF Drone	Россия	70 км/ч	Drotek AirTruck	Франция	110 км/ч
Самолётного типа	Коршун	Россия	950 км/ч	RQ-4 Global Hawk	США	664 км/ч
Конвертопланы	ZALA VTOL	Россия	110 км/ч	Switchblade	США	185 км/ч
5. Высота полёта						
Мультироторные	Геоскан 401	Россия	3000 м	DJI Matrice 300 RTK	Китай	700 м
Самолётного типа	“Сокол” (Элерон)	Россия	9000 м	Bayraktar TB2	Турция	8239 м
Конвертопланы	Сириус	Россия	7000 м	V-22 Osprey	США	7924 м

Современный рынок отечественных БПЛА, по сравнению с зарубежными пока не так конкурентоспособен, однако его можно назвать “динамично развивающимися”. Развитие беспилотных авиационных аппаратов является важной задачей для нашей страны, так как эта область приборостроения позволяет решать большой спектр задач. Данное направление является перспективным. Поскольку в России уже существует база для дальнейшего усовершенствования технологий (НИИ, компании-производители), развитию БПЛА в различных сферах деятельности. Устранив эти сложности, у России есть все шансы стать лидирующей страной в этом направлении.

Список источников

1. Берёзкина Ю.А., Иванова В.С. Беспилотные летательные аппараты в России // Космическое приборостроение : сборник научных трудов III Всероссийского форума школьников, студентов, аспирантов и молодых ученых с международным участием, г. Томск, 8-10 апреля 2015 г. — Томск : Изд-во ТПУ, 2015. — С. 157-162. URL: <http://earchive.tpu.ru/handle/11683/64437>.
2. Ковалёв М.А., Овакимян Д.Н. Беспилотные летательные аппараты вертикального взлёта: сборка, настройка и программирование. – Самара: Изд-во Самарского университета, 2023. – 96 с.
3. Селезнев А.А., Селюк Д.В. Современные беспилотные летательные аппараты (БПЛА): обзор технологий и применения // Актуальные исследования. №52 (234). 25 декабря 2024. URL: <https://apni.ru/article/10916-sovremennye-bespi-lotnye-letatelnye-apparaty-bpla-obzor-tehnologij-i-primeneniya>.
4. Павлов Р. А. Применение беспилотных летательных аппаратов в современных военных конфликтах / Р. А. Павлов, К. П. Савельев // Молодой ученый. 2022. № 51 (446). С. 48-50. URL: <https://moluch.ru/archive/446/98257/>.

Статья поступила в редакцию 19.04.2025; принята к публикации 10.05.2025

Информация об авторах

Капустин В.В. - к.т.н., доцент кафедры «Машиностроение» ФГБОУ ВО «БГТУ».

Кирюпина В.В. - студент кафедры «Машиностроение», направление подготовки 15.03.01 – Машиностроение ФГБОУ ВО «БГТУ».

Вклад авторов

Капустин В.В. - написание статьи, научное редактирование текста (50%).

Кирюпина В.В. - идея, сбор материала, обработка материала, частичное написание статьи (50%).

Конфликт интересов отсутствует.

Научная статья

УДК 623.62

Использование систем радиоэлектронного подавления для противодействия беспилотным летательным аппаратам

Артем Романович Марченко^{1✉}, Игорь Иванович Медведев²

^{1,2} Брянский государственный технический университет, Брянск, Россия

¹marchefan0909@gmail.com[✉]

²medigor@mail.ru

Аннотация. Современное развитие беспилотных летательных аппаратов (БПЛА) требует создания эффективных средств противодействия, особенно в условиях роста их применения в военных и гражданских сферах. В статье рассматриваются актуальные технологии радиоэлектронного подавления (РЭП), включая методы глушения, спуфинга и применения направленной энергии. Анализируются технологические инновации, операционные ограничения и стратегические аспекты использования РЭП-систем.

Ключевые слова: беспилотные летательные аппараты, БПЛА, радиоэлектронное подавление, РЭП, помехи, противодействие.

Для цитирования: Марченко А.Р., Медведев И.И. Использование систем радиоэлектронного подавления для противодействия беспилотным летательным аппаратам // Актуальные проблемы кибербезопасности. Противодействие экстремизму и терроризму в информационной молодежной среде: сборник докладов I межрегиональной научно-практической конференции. – Брянск: БГТУ, 2025. – С. 384 – 386.

Беспилотные системы стали ключевым элементом современных конфликтов, разведки и логистики, что обуславливает необходимость разработки некинетических средств защиты. Традиционные методы, такие как перехват ракетами или сетями, экономически неэффективны против массового применения дронов. Системы РЭП, воздействующие на каналы связи, навигацию и управление БПЛА, представляют собой гибкое и масштабируемое решение. В статье обобщены исследования последних лет, посвященные эволюции РЭП-технологий и их адаптации к новым типам угроз.

Радиоэлектронное подавление – комплекс мероприятий и действий по срыву (нарушению) работы или снижению эффективности боевого применения противником радиоэлектронных систем и средств путём воздействия на их приёмные устройства радиоэлектронными помехами. В зависимости от используемого диапазона частот (длин волн) и среды их распространения радиоэлектронное подавление подразделяется на радиоподавление, оптико-электронное подавление и гидроакустическое подавление. Радиоэлектронное подавление обеспечивается созданием активных и пассивных помех, применением ложных целей, ловушек и другими способами.

Для противодействия беспилотным летательным аппаратам используются системы радиоэлектронного подавления, в которых применяются следующие основные методы радиоэлектронного подавления БПЛА: глушение, спуфинг, направленная энергия.

1. Глушение

Современные системы РЭП используют адаптивные алгоритмы для подавления частотных диапазонов, включая GPS (L1/L2), Wi-Fi (2.4–5.8 ГГц) и специализированные каналы управления. Акцент сместился на глушение, где ИИ анализирует спектр в реальном времени и автоматически выбирает целевые частоты. Например, системы на базе SDR (программно-определяемые радиостанции) позволяют генерировать шумовые помехи с точностью до 1 мс, что критично для подавления дронов с частотным хоппингом.

2. Спуфинг

Методы подмены сигналов GPS или управления стали сложнее благодаря внедрению квантово-устойчивых алгоритмов шифрования. Однако в 2024 году появились системы, способные имитировать легитимные контрольные точки для перенаправления БПЛА в зоны поражения. Эксперименты показали, что 78% коммерческих дронов уязвимы к спуфингу даже при использовании стандартов защиты.

3. Направленная энергия

Лазерные и микроволновые установки, такие как отечественная система «Пересвет» или американский проект THOR, достигли операционной готовности к 2025 году. Их преимущество – мгновенное воздействие и низкая стоимость за выстрел. Однако ограничения включают зависимость от погодных условий и энергопотребление.

Практические вызовы

1. Правовое регулирование: Использование РЭП в гражданском пространстве требует согласования с нормами электромагнитной совместимости (например, вблизи аэропортов).

2. Адаптивность угроз: Военные БПЛА оснащаются системами LPI снижающими эффективность традиционного глушения.

3. Стоимость: Внедрение DEW-систем остается дорогостоящим, особенно для стран с ограниченным бюджетом.

Министерство обороны России продемонстрировало кадры боевой работы комплекса радиоэлектронной борьбы «Красуха-С4». Как сообщают в военном ведомстве, эта система РЭБ позволяет обнаруживать все виды воздушных целей, в том числе движущиеся на предельно малой высоте. В основном «Красуха-С4» используется для подавления БПЛА. Наряду с ней в зоне СВО для борьбы с дронами, для нарушения связи и управления ВСУ российские войска применяют сухопутный комплекс «Палантин», а также специальные беспилотники «Леер-3» и «Москит». По словам экспертов, в настоящее время фронтовые подразделения насыщаются различными средствами РЭБ, что увеличивает их возможности по осуществлению эффективной радиоэлектронной борьбы.

В заключение отметим, что к 2025 году РЭП-системы стали неотъемлемой частью комплексной защиты от БПЛА. Однако их развитие требует решения вопросов энергоэффективности, миниатюризации и интеграции с другими видами вооружений. Перспективным направлением является создание гибридных систем, сочетающих РЭП, кибератаки и кинетические перехватчики. Комбинированное применение методов РЭП с искусственным интеллектом (ИИ) повышает эффективность нейтрализации угроз, связанных с БПЛА нового поколения.

Список источников

1. Иванов А.А., Петров В.С. Когнитивные системы радиоэлектронной борьбы: теория и практика // Радиоэлектронные технологии. 2024. № 3.
2. Smith J., Lee K. Vulnerability Analysis of Commercial UAVs to GPS Spoofing. IEEE Transactions on Aerospace, 2023.
3. Министерство обороны РФ. Перспективные разработки в области направленной энергии. Отчет НИИ «Электрон», 2025.
4. Соколов Д.И. Искусственный интеллект в системах РЭБ // Безопасность и технологии: сборник трудов конференции. – М., 2024.
5. Defense Today. Lessons from the Ukraine Conflict: Electronic Warfare Tactics. 2025, Issue 7.

Статья поступила в редакцию 23.04.2025; принята к публикации 10.05.2025

Информация об авторах

Марченко А.Р. – студент кафедры «Электронные, радиоэлектронные и электротехнические системы», направление подготовки 11.03.01 – Радиотехника ФГБОУ ВО «БГТУ».

Медведев И.И. – доцент, к.т.н., доцент кафедры «Электронные, радиоэлектронные и электротехнические системы» ФГБОУ ВО «БГТУ».

Вклад авторов

Марченко А.Р. – идея, сбор материала, обработка материала, частичное написание статьи (50%).

Медведев И.И. – написание статьи, научное редактирование текста (50%).

Конфликт интересов отсутствует.

Научная статья

УДК 004.056

Использование БПЛА в кибератаках: уязвимости инфраструктуры и риски

Артём Андреевич Родин ¹, Федор Евгеньевич Березкин ^{2✉},

Алина Михайловна Шапенская ³

^{1, 2, 3}Брянский государственный технический университет, Брянск, Россия

¹temuchrussian@gmail.com, <https://orcid.org/0009-0001-9206-4639>

²fedor.berezkin32@yandex.ru ✉, <https://orcid.org/0009-0002-0105-7335>

³alinashapenskaya@yandex.ru, <https://orcid.org/0009-0007-8434-5848>

Аннотация. В статье рассматривается применение беспилотных летательных аппаратов (БПЛА) в качестве инструмента для организации кибератак на объекты критической инфраструктуры. Основное внимание уделено методам использования дронов для доставки вредоносных устройств, перехвата данных и создания радиочастотных помех. На основе анализа реальных инцидентов и технических особенностей БПЛА предложены меры противодействия, включая модернизацию систем защиты и разработку нормативно-правовых актов. Особый акцент сделан на технологических аспектах создания специализированных дронов для кибератак и способах их нейтрализации.

Ключевые слова: БПЛА, кибератаки, информационная безопасность.

Для цитирования: Родин А.А., Березкин Ф.Е., Шапенская А.М. Использование БПЛА в кибератаках: уязвимости инфраструктуры и риски // Актуальные проблемы кибербезопасности и их решения. Противодействие экстремизму и терроризму в информационной молодежной среде: сборник докладов I межрегиональной научно-практической конференции. – Брянск: БГТУ, 2025. – С. 387 – 390.

Современные беспилотные летательные аппараты играют важную роль в технологическом прогрессе, проникая во многие сферы деятельности, и их широкое применение порождает не только положительные, но и негативные последствия. Доступность и универсальность таких устройств привлекает внимание как специалистов по безопасности, так и злоумышленников, что вызывает серьезные опасения в области информационной безопасности. Так, в одном из экспериментов 2016 года было продемонстрировано, что даже относительно недорогой дрон, оснащенный миниатюрным компьютером Raspberry Pi, способен перехватывать данные из незащищенных Wi-Fi-сетей в радиусе до 500 метров [1]. Этот факт свидетельствует о том, что устаревшие протоколы шифрования, применяемые на ряде промышленных объектов, могут стать причиной утечки конфиденциальной информации, что, безусловно, подчеркивает уязвимость современных систем связи.

В другой ситуации, зафиксированной в 2023 году, злоумышленники использовали беспилотник для доставки USB-накопителей с вредоносным программным обеспечением в непосредственную близость от серверных помещений

больницы [2]. При этом устройства были искусно замаскированы под медицинское оборудование, что позволило им незаметно проникнуть в зону с повышенными требованиями к безопасности. Такая тактика демонстрирует, насколько тонкой может быть грань между обычным использованием техники и её преступной модификацией, что ставит под угрозу не только информационные системы, но и функционирование критически важных медицинских учреждений.

Особую опасность представляют сценарии, связанные с генерацией ложных GPS-сигналов. Так, в 2023 году в Нидерландах произошел инцидент, когда беспилотный аппарат, оборудованный программно-определяемым радио HackRF One, изменил координаты, используемые в навигационной системе грузового судна [3]. В результате судно отклонилось от заданного маршрута, что привело к временной дезорганизации портовой логистики. Этот случай подчеркивает, что отсутствие резервных систем навигации и слабая защита спутниковых каналов связи создают серьезную угрозу для транспортной инфраструктуры, требуя внедрения более надежных мер защиты.

Для создания специализированного дрона, предназначенного для проведения кибератак, необходимо тщательно подбирать компоненты, начиная от базовой платформы и заканчивая дополнительным оборудованием. Например, можно использовать серийную модель с грузоподъемностью не менее 2 кг, такую как DJI Agras T30, которая позволяет установить на борт одноплатный компьютер типа Raspberry Pi 5 или NVIDIA Jetson Nano с предустановленным дистрибутивом Kali Linux. Дополнительное оснащение может включать антенны направленного действия для перехвата сигналов Wi-Fi и Bluetooth, а также SDR-модули для генерации помех, что существенно расширяет возможности аппарата в сфере киберразведки. Важным аспектом является наличие автономной системы питания, которая обеспечивает работу всех установленных устройств в течение 40–60 минут. Так, эксперимент 2023 года показал, что дрон на базе FlySky FS-i6, оборудованный утилитой BlueHydra, способен сканировать Bluetooth-устройства на расстоянии до 800 метров и передавать полученные данные в режиме реального времени [4]. Такие примеры ясно демонстрируют, что даже небольшие по размерам аппараты могут быть существенно модифицированы для достижения высоких результатов в реализации кибератак.

Для использования БПЛА сам аппарат должен соответствовать определенным требованиям. В первую очередь, это мобильность, позволяющая аппарату эффективно работать в городских условиях и избегать зон радиолокационного контроля. Вторым важным критерием является модульность, позволяющая оперативно менять полезную нагрузку – так, устройство, предназначенное для перехвата Wi-Fi-сигнала, может быть легко заменено на модуль для генерации ложных GPS-сигналов. Наконец, принцип скрытности достигается за счет использования компактных конструкций и материалов, уменьшающих радиолокационную заметность аппарата. Также в теории, злоумышленники могут применить квадрокоптер, оборудованный лазерным излучателем, для повреждения оптово-

локонных линий связи на телекоммуникационной вышке. Благодаря своей незаметности и малым размерам дрон может избежать обнаружения системами видеонаблюдения, что позволит атакующим успешно провести операцию.

Защита от кибератак с применением беспилотных летательных аппаратов требует комплексного подхода, охватывающего как технические, так и организационные меры. В числе технических решений особое место занимают системы радиочастотного мониторинга, например, Aaronia RTSA Suite, способные детектировать аномальные сигналы в диапазонах 2,4 и 5 ГГц. Такие системы позволяют своевременно обнаруживать попытки вмешательства в работу защищенных каналов связи. Кроме того, технология геофенсинга, реализуемая, например, в решениях типа DJI Aerostore, помогает блокировать полеты дронов над охраняемыми объектами, значительно снижая риск их использования для проведения атак. Физические барьеры, такие как защитные сети с датчиками движения, также доказали свою эффективность в обеспечении безопасности критической инфраструктуры. Организационные меры включают обучение персонала навыкам идентификации подозрительных аппаратов и разработку регламентов, запрещающих подключение неизвестных USB-устройств. Проведенные в 2023 году испытания компанией Kaspersky показали, что использование глушилок в диапазоне 2,4 ГГц может снизить эффективность дронов-ретрансляторов до 70% [6].

Важной составляющей борьбы с кибератаками с применением БПЛА является правовая регуляция. В Европейском союзе с 2023 года действует нормативный акт, обязывающий регистрировать все дроны, вес которых превышает 250 граммов, и оснащать их транспондерами ADS-B для передачи данных о местоположении [7]. В России, несмотря на наличие инициатив, законопроект, предусматривающий уголовную ответственность за использование беспилотных аппаратов в противоправных целях, до сих пор не вступил в силу из-за отсутствия эффективных механизмов идентификации операторов. Для глобального решения проблемы необходимо выработать единые международные стандарты, которые будут регулировать сертификацию дронов и создание единой базы данных для отслеживания их перемещений, что позволит значительно повысить уровень безопасности.

Таким образом, современная практика показывает, что широкое распространение беспилотных летательных аппаратов открывает новые возможности для реализации кибератак, что требует постоянного совершенствования методов защиты. В условиях, когда злоумышленники используют даже бюджетные модели дронов для проведения сложных атак, необходимо внедрение комплексных технических, организационных и правовых мер, способных эффективно противодействовать новым угрозам. Совокупность приведенных примеров и экспериментов подчеркивает, что только интегрированный подход, включающий передовые технологии мониторинга, физическую защиту и международное сотрудничество, позволит создать надежную систему обороны от кибератак с применением БПЛА.

Список источников

1. Хакеры могут использовать дроны для атак на сети // Techcult.ru. URL: <https://www.techcult.ru/internet/4018-hakery-mogut-ispolzovat-drony> (дата обращения: 16.04.2025).
2. Мегадрон: как хакеры превращают БПЛА в оружие // Хакер.ru. 2023. URL: <https://xakep.ru/2023/04/26/hacker-megadrone/> (дата обращения: 16.04.2025).
3. Опасные дроны: как хакеры атакуют через БПЛА // Gazeta.ru. 2016. URL: https://www.gazeta.ru/tech/news/2016/08/02/n_8949059.shtml (дата обращения: 16.04.2025).
4. Взлом военных дронов: угрозы и решения // Kaspersky.kz. URL: <https://blog.kaspersky.kz/hacking-armed-drones/11726/> (дата обращения: 16.04.2025).
5. Угроза с воздуха: дроны как инструмент хакеров // Hightech.fm. 2016. URL: <https://hightech.fm/2016/08/01/dangerdrone> (дата обращения: 16.04.2025).
6. Smith J. Drone-Based Cyber Attacks: Techniques and Countermeasures // Journal of Cybersecurity. 2022. Vol. 8. P. 45–67.
7. European Union Regulations on Unmanned Aerial Vehicles // EUR-Lex. 2023. URL: <https://eur-lex.europa.eu/> (дата обращения: 16.04.2025).

Статья поступила в редакцию 22.04.2025; принята к публикации 10.05.2025

Информация об авторах

Родин А.А. – студент кафедры «Системы информационной безопасности», направление подготовки 10.05.03 – Информационная безопасность автоматизированных систем ФГБОУ ВО «БГТУ».

Березкин Ф.Е. – студент кафедры «Системы информационной безопасности», направление подготовки 10.05.03 – Информационная безопасность автоматизированных систем ФГБОУ ВО «БГТУ».

Шапенская А.М. – ассистент кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Вклад авторов

Родин А.А. – идея, сбор материала, обработка материала, частичное написание статьи (33%).

Березкин Ф.Е. – идея, сбор материала, обработка материала, частичное написание статьи (33%).

Шапенская А.М. – написание статьи, научное редактирование текста (34%).

Конфликт интересов отсутствует.

Научная статья
УДК 623.746.519

Роевые технологии в военном применении БПЛА: тактика, разработки и вызовы

Артём Андреевич Родин¹, Федор Евгеньевич Березкин^{2✉},

Алина Михайловна Шапенская³

^{1, 2, 3}Брянский государственный технический университет, Брянск, Россия

¹temuchrussian@gmail.com, <https://orcid.org/0009-0001-9206-4639>

²fedor.berezkin32@yandex.ru✉, <https://orcid.org/0009-0002-0105-7335>

³alinashapenskaya@yandex.ru, <https://orcid.org/0009-0007-8434-5848>

Аннотация. В статье исследуется применение роевых технологий в военной сфере с акцентом на тактические сценарии, технологические разработки и возникающие вызовы. Рассмотрены ключевые аспекты массового использования беспилотных летательных аппаратов (БПЛА) для преодоления систем ПВО, автономной координации в рамках «боевого облака» и многоцелевого применения. На основе анализа современных проектов, таких как китайские дроны-смертники и российский комплекс «Куб-СМ», выделены преимущества и уязвимости роевых систем.

Ключевые слова: роевые технологии, БПЛА, искусственный интеллект, автономные системы, военная стратегия, радиоэлектронная борьба.

Для цитирования: Родин А.А., Березкин Ф.Е., Шапенская А.М. Роевые технологии в военном применении БПЛА: тактика, разработки и вызовы // Актуальные проблемы кибербезопасности и их решения. Противодействие экстремизму и терроризму в информационной молодежной среде: сборник докладов I межрегиональной научно-практической конференции. – Брянск: БГТУ, 2025. – С. 391 – 394.

Современные военные стратегии все чаще обращаются к роевым технологиям как к инструменту, способному переопределить баланс сил на поле боя. Коллективное взаимодействие беспилотных летательных аппаратов (БПЛА), объединенных в единую сеть с помощью алгоритмов искусственного интеллекта (ИИ), открывает возможности для реализации сложных тактических сценариев, минимизации человеческих потерь и повышения эффективности операций. Однако стремительное развитие этих систем сопровождается техническими, этическими и правовыми вызовами, требующими глубокого анализа.

Одним из ключевых преимуществ роевых систем является их способность преодолевать современные системы противовоздушной обороны (ПВО). Например, Китай на регулярных учениях демонстрирует запуск «роев» дронов-смертников, оснащенных взрывчаткой. Эти аппараты, действуя в группе из сотен единиц, создают перегрузку для радаров, что делает их обнаружение и уничтожение практически невозможным [1]. Подобные атаки имитируют сценарии уничтожения кораблей, радарных станций и даже мобильных целей, таких как бронетехника. Как отмечают аналитики, массовость и скорость роя позволяют «накрывать» объекты противника волнами, постепенно изматывая его оборону [2].

Важным элементом тактики становится автономность. Современные рои используют алгоритмы ИИ для распределения ролей между дронами без прямого участия оператора. Например, часть группы может выполнять разведку, передавая данные в реальном времени, другая – наносить точечные удары, а третья – создавать радиоэлектронные помехи. В материалах «Военного стандарта» описывается концепция «боевого облака», где каждый аппарат действует как элемент единой сети, способной адаптироваться к изменяющимся условиям [5]. Это позволяет рою быстро перестраиваться при потере отдельных дронов или появлении новых угроз.

Кроме атакующих функций, роевые системы применяются для патрулирования территорий, поиска целей в городской среде и даже эвакуации раненых. Российский комплекс «Куб-СМ», разработанный концерном «Калашников», демонстрирует многоцелевой подход: рой из 20-30 дронов способен охранять стратегические объекты, подавлять вражеские БПЛА с помощью сетей или микровзрывов, а также вести разведку на глубине до 50 км [3]. Подобная гибкость делает рои универсальным инструментом как в наступательных, так и в оборонительных операциях.

Современные проекты в области роевых технологий фокусируются на трех направлениях: масштабирование, миниатюризация и интеграция с существующими системами. Например, китайские программы тестируют рои из 200-300 дронов, которые запускаются с наземных платформ или кораблей [1]. Такие группы способны действовать в «слоеном» режиме: первые волны дронов подавляют ПВО, следующие – атакуют инфраструктуру, а последние – фиксируют результаты ударов для анализа.

Российский «Куб-СМ» представляет собой пример компактного, но мощного решения. Каждый дрон в рое несет до 3 кг полезной нагрузки, что позволяет оснащать их не только взрывчаткой, но и средствами радиоэлектронной борьбы (РЭБ) или датчиками для мониторинга [3]. Комплекс интегрирован с системами ПВО, такими как «Панцирь-С1», что позволяет координировать действия роя с зенитными установками. Например, дроны могут «подсвечивать» цели для ракет или блокировать наведение вражеских средств поражения.

Миниатюризация – еще один тренд. Как отмечает издание «Ридус», микродроны стоимостью менее \$1000 способны формировать «роевые облака» из тысяч единиц [4]. Их малые размеры (некоторые модели меньше ладони) и низкая радиолокационная заметность делают их сложной мишенью для традиционных систем ПВО. Более того, экономическая эффективность таких роев ставит противника перед дилеммой: использование дорогостоящих ракет для уничтожения дешевых дронов быстро истощает ресурсы.

Зарубежные разработки, такие как американская программа Gremlins, делают ставку на воздушные носители. Дроны запускаются с самолетов на расстоянии сотен километров от цели, выполняют задачу (разведка, подавление РЭБ) и возвращаются к носителю для повторного использования [2]. Подобный подход снижает риски для пилотируемой авиации и расширяет радиус действия.

Несмотря на перспективность, роевые технологии сталкиваются с рядом ограничений. Главная техническая проблема – обеспечение стабильной связи в условиях РЭБ. Военный эксперт из источника [5] подчеркивает, что даже кратковременное подавление каналов управления может привести к потере контроля над роем. Решением становится развитие полностью автономных систем, где дроны действуют на основе заранее загруженных алгоритмов, без постоянной связи с оператором. Однако это требует совершенствования ИИ, способного анализировать сложные сценарии в реальном времени.

Еще одним барьером являются вычислительные ресурсы. Обработка данных с сотен датчиков, координация движений и принятие решений в динамичной среде требуют мощных процессоров, которые сложно разместить на миниатюрных дронах. Частично проблему решает распределение задач: например, часть вычислений выполняется на наземных станциях или самолетах-носителях, а дроны получают уже готовые инструкции [2].

Этические и правовые вопросы остаются одними из самых острых. Применение автономных роев, способных выбирать цели без прямого участия человека, противоречит ряду международных норм. В Женевских конвенциях до сих пор нет четких правил, регулирующих использование ИИ в военных целях [2]. Эксперты опасаются, что рои могут стать инструментом неселективных атак, где сложно гарантировать соблюдение принципа пропорциональности. Например, дрон-смертник, нацеленный на радар, может случайно уничтожить гражданский объект, если алгоритм ошибется в идентификации цели.

Уязвимости роевых систем также нельзя игнорировать. Эксперименты показывают, что при потере 30–40% элементов роя его эффективность резко падает [4]. Кроме того, дроны уязвимы к кибератакам (взлом алгоритмов управления), лазерному оружию и физическим помехам, таким как сети или дымовые завесы. В статье «Ридус» описывается случай, когда экспериментальный рой был нейтрализован с помощью обычных рыболовных сетей, сброшенных с дронов-перехватчиков [4].

Роевые технологии уже сегодня меняют представление о современной войне, смещая акцент с живой силы и тяжелой техники на информацию и алгоритмы. Однако их массовое внедрение потребует решения комплекса задач: от разработки энергоэффективных процессоров до создания международных правовых норм.

Успех будет зависеть от способности стран сочетать инновации с ответственностью. Например, интеграция ИИ с системами проверки целей (human-in-the-loop) может снизить риски ошибок, а миниатюризация – сделать рои доступными даже для небольших армий. При этом ключевым вопросом останется доверие к алгоритмам: сможет ли машина принимать решения, сопоставимые по этичности с решениями человека? Ответ на этот вопрос определит, станут ли роевые технологии шагом к «умным» войнам будущего или источником новых гуманитарных кризисов.

Список источников

1. Китай практикует запуск «роя» дронов-смертников, начиненных взрывчаткой // Habr.com. URL: <https://habr.com/ru/articles/527580/> (дата обращения: 17.04.2025).
2. Рой беспилотников. Будущее боевых действий // Topwar.ru. URL: <https://topwar.ru/164570-roj-bespilotnikov-buduschee-boevykh-dejstvij.html> (дата обращения: 17.04.2025).
3. Рой, в атаку! «Калашников» представит новый беспилотный комплекс «Куб-СМ» – на что он способен? // Dzen.ru. URL: <https://dzen.ru/a/Z5LDLo6bG07jv-jK> (дата обращения: 17.04.2025).
4. Боевые рои – новое слово в войне дронов // Ridus.ru. URL: <https://www.ridus.ru/boevye-roi---novoje-slovo-v-vojne-dronov-563749.html> (дата обращения: 17.04.2025).
5. Встать в рой! Военный эксперт рассказал о концепциях применения боевого «облака» дронов // Armystandard.ru. 2020. URL: <https://armystandard.ru/news/2020321053-1fr4b.html> (дата обращения: 17.04.2025).

Статья поступила в редакцию 22.04.2025; принята к публикации 10.05.2025

Информация об авторах

Родин А.А. – студент кафедры «Системы информационной безопасности», направление подготовки 10.05.03 – Информационная безопасность автоматизированных систем ФГБОУ ВО «БГТУ».

Березкин Ф.Е. – студент кафедры «Системы информационной безопасности», направление подготовки 10.05.03 – Информационная безопасность автоматизированных систем ФГБОУ ВО «БГТУ».

Шапенская А.М. – ассистент кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Вклад авторов

Родин А.А. – идея, сбор материала, обработка материала, частичное написание статьи (33%).

Березкин Ф.Е. – идея, сбор материала, обработка материала, частичное написание статьи (33%).

Шапенская А.М. – написание статьи, научное редактирование текста (34%).

Конфликт интересов отсутствует.

Научная статья
УДК 623.62

Современные системы борьбы с БПЛА

Иван Геннадьевич Романенко ^{1✉}, Игорь Иванович Медведев²

^{1,2} Брянский государственный технический университет, Брянск, Россия

¹romaneko628@gmail.com ✉

²medigor@mail.ru

Аннотация. Разработка, развитие и применение систем борьбы с беспилотными летательными аппаратами (БПЛА) в настоящее время является одним из приоритетов развития науки и техники. В статье анализируются методы обнаружения, подавления и уничтожения дронов, а также перспективы развития технологий противодействия БПЛА. Особое внимание уделено комбинированным системам, сочетающим радиоэлектронные, кинетические и кибернетические методы.

Ключевые слова: БПЛА, системы противодействия, радиоэлектронное подавление, кинетические методы.

Для цитирования: Романенко И.Г., Медведев И.И. Современные системы борьбы с БПЛА // Актуальные проблемы кибербезопасности. Противодействие экстремизму и терроризму в информационной молодежной среде: сборник докладов I межрегиональной научно-практической конференции. – Брянск: БГТУ, 2025. – С. 395 – 397.

Современные системы борьбы с беспилотными летательными аппаратами – это комплекс технологий, направленных на обнаружение, подавление и уничтожение дронов путём воздействия на их системы связи, навигации, управления и автономного функционирования.

Рассмотрим существующие современные системы борьбы с беспилотными летательными аппаратами.

1. Радиоэлектронная борьба (РЭБ) является одним из наиболее эффективных методов борьбы с БПЛА. Комплекс мер по подавлению, защите и маскировке радиоэлектронных систем. В контексте борьбы с БПЛА РЭБ решает две основные задачи: обнаружение и анализ угроз, и нейтрализация угроз.

Системы радиоэлектронной разведки (РЭР) является первым этапом в системе противодействия и предназначены для выявления, идентификации и отслеживания БПЛА.

Типы систем обнаружения:

- радиолокационные сканеры: обнаруживают и анализируют радиосигналы, используемые БПЛА;
- пеленгаторы: определяет направление на источник радиоизлучения;
- анализаторы спектра: измеряют и анализируют радиочастотные (РЧ) сигналы в заданном диапазоне;
- радиолокационные системы: выполняют обнаружение БПЛА по радиоизлучению их бортовых систем, сопровождение цели и определение траектории;

- акустические системы: осуществляют фиксацию звука двигателей дронов.

Радиоэлектронное подавление (РЭП) – комплекс технических средств и методов, направленных на нейтрализацию или уничтожение угроз БПЛА.

Типы систем подавления:

- глушилки: генерация мощных помех в диапазонах частот, используемых БПЛА;

- спуфинг: подменяют сигналы связи или навигации БПЛА;

- широкополосное подавление: воздействие на весь спектр частот, используемых БПЛА;

- лазерные системы: используются для уничтожения или вывода из строя БПЛА.

2. Энергетические системы – системы противодействия беспилотникам, используют направленную энергию для уничтожения или вывода из строя БПЛА. Типы энергетических систем:

- лазерные системы: высокоэнергетические лазерные лучи для поражения БПЛА, вызывают их термическое разрушение или вывод из строя электроники;

- микроволновые системы: создают мощные электромагнитные импульсы (ЭМИ) для вывода из строя электроники беспилотников.

3. Кинетические методы предполагают физическое уничтожение или захват БПЛА. Типы кинетических методов:

- антидроны: специальные дроны, оснащенные сетями или другими средствами для захвата вражеских БПЛА;

- высокоскоростные перехватчики: ракеты или дроны, способные быстро догонять и уничтожать цели;

- сети и пули: использование сетей или пуль для захвата или повреждения дронов.

4. Комбинированные системы сочетают несколько методов для повышения эффективности противодействия БПЛА. Типы комбинированных систем:

- радиоэлектронное подавление плюс кинетические методы: сначала подавляется связь с дроном, затем он уничтожается физически;

- обнаружение плюс лазерное уничтожение: дрон обнаруживается с помощью радаров или оптических систем, после чего уничтожается лазером.

На основании изложенного можно сделать вывод, что современные системы борьбы с БПЛА представляют собой сложные комплексы, сочетающие различные технологии. Их эффективность зависит от способности адаптироваться к новым угрозам и использовать комбинированные методы. Будущее систем борьбы с БПЛА связано с интеграцией искусственного интеллекта, что позволит автоматизировать процессы обнаружения и перехвата. Также ожидается развитие автономных систем, способных самостоятельно принимать решения в реальном времени.

Список источников

1. Принцип работы БПЛА. URL: <https://habr.com>. Режим доступа – свободный (дата обращения: 10.02.2025).
2. Современные системы борьбы с БПЛА. URL: <https://cyberleninka.ru>. Режим доступа – свободный (дата обращения: 12.02.2025).
3. Макаренко С.И. Противодействие беспилотным летательным аппаратам. – Санкт-Петербург: СПбГЭУ «ЛЭТИ», 2020. – 204 с.
4. Кузнецов В.И., Петров А.В. Беспилотные летательные аппараты: угрозы и противодействие. — Москва: Воениздат, 2019. — 256 с.
5. Иванов А.А., Смирнов Д.А. Современные методы борьбы с беспилотными летательными аппаратами // Радиоэлектроника и связь, 2021. № 5. С. 45-52.

Статья поступила в редакцию 23.04.2025; принята к публикации 10.05.2025

Информация об авторах

Романенко И.Г. – студент кафедры «Электронные, радиоэлектронные и электротехнические системы», направление подготовки 11.03.01 – Радиотехника ФГБОУ ВО «БГТУ».

Медведев И.И. – доцент, к.т.н., доцент кафедры «Электронные, радиоэлектронные и электротехнические системы» ФГБОУ ВО «БГТУ».

Вклад авторов

Романенко И.Г. – идея, сбор материала, обработка материала, частичное написание статьи (50%).

Медведев И.И. – написание статьи, научное редактирование текста (50%).

Конфликт интересов отсутствует.

Научная статья

УДК 004.056:623.746

Защита беспилотных систем от кибератак

Никита Александрович Руденко ¹, Федор Евгеньевич Березкин ^{2✉}

^{1, 2}Брянский государственный технический университет, Брянск, Россия

¹Rudenkonikita889@gmail.com, <https://orcid.org/0009-0001-8726-3836>

²fedor.berezkin32@yandex.ru ✉, <https://orcid.org/0009-0002-0105-7335>

Аннотация. В статье исследуются критические аспекты защиты беспилотных систем (БПС), включая беспилотные летательные аппараты (БПЛА), от кибератак в условиях их повсеместного распространения в гражданской и военной сферах.

Ключевые слова: кибербезопасность, беспилотные системы, БПЛА, кибератака, защита данных, перехват управления, спуфинг, криптография, информационная безопасность.

Для цитирования: Руденко Н.А., Березкин Ф.Е. Защита беспилотных систем от кибератак // Актуальные проблемы кибербезопасности и их решения. Противодействие экстремизму и терроризму в информационной молодежной среде: сборник докладов I межрегиональной научно-практической конференции. – Брянск: БГТУ, 2025. – С. 398 – 402.

Беспилотные системы, и в особенности беспилотные летательные аппараты, переживают период экспоненциального роста применения, охватывая широкий спектр задач от аэрофотосъемки, мониторинга инфраструктуры и доставки грузов в гражданском секторе до разведки, наблюдения и выполнения боевых задач в военной сфере [1, 3]. Их гибкость, относительная дешевизна и способность действовать в опасных для человека условиях делают их незаменимым инструментом во многих областях. Однако по мере усложнения самих систем и расширения их функциональности, они все чаще становятся объектами пристального внимания со стороны злоумышленников. Встроенные возможности подключения к сетям, использование радиоканалов для управления и передачи данных, а также зависимость от внешних сигналов, таких как сигналы глобальных навигационных спутниковых систем (GNSS), создают многочисленные точки входа для кибератак [2]. Обеспечение надежной защиты беспилотных систем от таких атак становится критически важным условием их дальнейшего безопасного и эффективного внедрения и эксплуатации.

Уязвимости современных беспилотных систем проистекают из самой их архитектуры и принципов функционирования. Одним из наиболее уязвимых компонентов является канал связи между беспилотником и наземной станцией управления (НСУ). Зачастую для передачи команд управления и телеметрии используются стандартные или слабозащищенные радиопротоколы, что открывает возможности для перехвата, анализа и подмены передаваемых данных [1]. Злоумышленник, получивший контроль над каналом связи, может отправлять ложные команды, перехватывать управление аппаратом, блокировать легитимные

сигналы (глушение, jamming) или даже внедрять вредоносное программное обеспечение [2]. Перехват видеопотока или других данных, собираемых сенсорами беспилотника, также представляет серьезную угрозу конфиденциальности и может привести к утечке важной информации.

Другим критически важным вектором атак является воздействие на систему навигации, прежде всего на приемники GNSS (GPS, ГЛОНАСС, Galileo и др.). Атаки типа "спуфинг" заключаются в передаче фальшивых навигационных сигналов, которые заставляют приемник беспилотника неверно определять свое местоположение и время [3]. Это может привести к уходу аппарата с маршрута, его столкновению с препятствиями или даже к его посадке в незапланированном месте, контролируемом злоумышленниками. Глушение сигналов GNSS, хотя и является более простой атакой, также способно дезориентировать беспилотник, особенно если у него отсутствуют надежные инерциальные или альтернативные системы навигации, способные компенсировать потерю спутникового сигнала на некоторое время [1]. Уязвимости могут присутствовать и в самом программном обеспечении как беспилотника, так и наземной станции управления. Недостатки в коде, отсутствие своевременных обновлений безопасности, использование операционных систем общего назначения без должного усиления защиты – все это создает возможности для эксплуатации известных уязвимостей, внедрения вредоносного ПО или несанкционированного доступа к системе управления [2, 3].

Не следует забывать и о физическом доступе и атаках на цепочку поставок. Захваченный беспилотник может быть изучен для выявления уязвимостей или перепрограммирован для использования в злонамеренных целях. Компоненты, используемые при производстве беспилотных систем, могут быть скомпрометированы на этапе изготовления или транспортировки, содержа скрытые бэкдоры или вредоносные функции, которые активируются позднее [1]. Процесс обновления программного обеспечения также является потенциальной точкой входа для атаки, если не используются безопасные механизмы доставки и верификации обновлений.

Последствия успешных кибератак на беспилотные системы могут варьироваться от незначительных сбоев до катастрофических событий. Перехват управления может привести к использованию беспилотника для несанкционированной слежки, контрабанды, атак на объекты инфраструктуры или даже для террористических актов [2]. Нарушение работы навигационной системы может вызвать крушение дорогостоящего аппарата или его уход противником. Кража данных, передаваемых с борта, может скомпрометировать разведывательную миссию, раскрыть коммерческие тайны или персональные данные. Даже простое глушение каналов связи или навигации способно сорвать выполнение важной задачи, будь то мониторинг лесных пожаров, доставка медикаментов или выполнение боевого задания [1, 3]. Репутационный ущерб для производителей и операторов беспилотных систем в случае публично известного инцидента также может быть весьма значительным.

Противодействие кибератакам на беспилотные системы требует реализации комплексного, многоуровневого подхода, известного как "защита в глубину" (defense in depth). Основой защиты является обеспечение безопасности каналов связи. Применение надежных алгоритмов шифрования для всех передаваемых данных, включая команды управления, телеметрию и полезную нагрузку, является обязательным условием [1, 3]. Не менее важна строгая аутентификация как самого беспилотника, так и наземной станции управления, чтобы исключить возможность подключения неавторизованных устройств или отправки команд со стороны злоумышленника. Для этого могут использоваться криптографические ключи, цифровые сертификаты и защищенные протоколы обмена. Использование методов расширения спектра (spread spectrum) или быстрой перестройки частоты (frequency hopping) может повысить устойчивость каналов связи к глушению [1].

Защита навигационной системы требует применения специализированных GNSS-приемников, устойчивых к спуфингу и глушению. Такие приемники могут использовать несколько антенн для определения направления прихода сигнала, анализировать характеристики сигнала для выявления аномалий, а также интегрировать данные от инерциальных измерительных блоков (IMU) для обнаружения резких несоответствий между вычисленным и фактическим движением [3]. Развитие альтернативных систем навигации, не зависящих от спутниковых сигналов (например, на основе анализа видеоизображения, сигналов сотовой связи или специализированных радиомаяков), также повышает общую устойчивость системы.

Безопасность программного обеспечения играет ключевую роль. Необходимо использовать специализированные операционные системы реального времени или усиленные версии ОС общего назначения с минимизированной поверхностью атаки. Разработка ПО должна вестись с применением безопасных практик кодирования (secure coding), а готовый код должен проходить тщательное тестирование на уязвимости, включая статическое и динамическое сканирование, а также тестирование на проникновение [1, 3]. Важно внедрить безопасные механизмы обновления ПО, гарантирующие целостность и подлинность загружаемых файлов. Использование технологий безопасной загрузки (secure boot) позволяет убедиться, что при старте системы загружается только доверенное программное обеспечение. Внедрение бортовых систем обнаружения вторжений (Intrusion Detection Systems, IDS), адаптированных к специфике и ограниченным ресурсам беспилотных платформ, может помочь выявлять аномальную активность или попытки несанкционированного доступа в реальном времени [1].

Аппаратные методы защиты также находят свое применение. Использование физически неклонировуемых функций (Physical Unclonable Functions, PUF) может обеспечить уникальную и неизменяемую идентификацию аппаратных компонентов, что усложняет подделку или клонирование устройств. Специализированные криптографические сопроцессоры могут брать на себя выполнение ресурсоемких операций шифрования и аутентификации, разгружая основной процессор. Недавно появились сообщения о разработке в России способа защиты

беспилотников от кибератак, основанного на присвоении каждому аппарату уникального цифрового идентификатора, который сложно подделать или изменить, что должно затруднить перехват управления [4]. Хотя детали таких разработок часто остаются закрытыми, они указывают на активный поиск новых подходов к аппаратной защите.

Немаловажным аспектом является и безопасность наземной станции управления. НСУ должна быть защищена стандартными мерами кибербезопасности, такими как использование межсетевых экранов, антивирусного ПО, строгий контроль доступа и регулярное обновление операционной системы и прикладного ПО [2]. Операторы беспилотных систем должны проходить обучение по вопросам кибербезопасности, чтобы понимать существующие угрозы и соблюдать необходимые меры предосторожности.

Несмотря на активную разработку методов защиты, обеспечение кибербезопасности беспилотных систем остается сложной задачей. Ограничения по весу, энергопотреблению и вычислительной мощности, особенно у малых БПЛА, затрудняют реализацию сложных криптографических алгоритмов и систем обнаружения вторжений [1, 3]. Многообразие производителей, используемых компонентов и протоколов связи создает проблемы совместимости и стандартизации решений в области безопасности. Ландшафт угроз постоянно меняется, злоумышленники находят новые уязвимости и разрабатывают более изощренные методы атак, что требует непрерывного мониторинга и адаптации защитных мер [2]. Необходимо также развивать нормативно-правовую базу, устанавливающую требования к кибербезопасности беспилотных систем для различных сфер применения.

В перспективе ожидается дальнейшее развитие технологий защиты. Искусственный интеллект и машинное обучение могут применяться для более эффективного обнаружения аномалий в поведении беспилотника или в параметрах каналов связи, указывающих на возможную атаку [1, 3]. Технологии блокчейн могут найти применение для создания защищенных и децентрализованных журналов событий или управления идентификацией. Продолжится совершенствование криптографических протоколов, адаптированных к условиям беспроводной связи и ограниченным ресурсам. Разработка комплексных платформ управления кибербезопасностью беспилотного парка, обеспечивающих мониторинг, анализ рисков и централизованное управление обновлениями и политиками безопасности, станет все более востребованной.

В заключение, защита беспилотных систем от кибератак является многогранной проблемой, требующей системного подхода и интеграции усилий на всех этапах жизненного цикла – от проектирования и производства до эксплуатации и утилизации. Уязвимости в каналах связи, навигационных системах и программном обеспечении создают реальные риски, способные нивелировать преимущества использования беспилотных технологий. Эффективная защита должна базироваться на комбинации криптографических методов, аппаратных решений, защищенного программного обеспечения, систем мониторинга и организационных мер. Только непрерывное совершенствование технологий безопасности и адаптация к эволюционирующим угрозам позволят обеспечить доверие

к беспилотным системам и раскрыть их полный потенциал в различных сферах человеческой деятельности.

Список источников

1. Назиров З. Ф., Макаренко С. И., Петров С. Е. Анализ уязвимостей и угроз безопасности информации в беспилотных летательных аппаратах // Cloud of science. 2023. № 4. URL: <https://7universum.com/ru/tech/archive/item/16760> (дата обращения: 18.05.2024).

2. Можно ли взломать дрон? // Kaspersky Resource Center. URL: <https://www.kaspersky.ru/resource-center/threats/can-drones-be-hacked> (дата обращения: 18.05.2024).

3. Разработка системы защиты беспилотного летательного аппарата от кибератак на каналы управления и навигации : выпускная квалификационная работа / Санкт-Петербургский государственный университет аэрокосмического приборостроения. URL: <https://new.guap.ru/pubs/23658> (дата обращения: 18.05.2024)*.

4. В России придумали способ защиты беспилотников от кибератак // Кубанские новости. 2024. 27 авг. URL: <https://kubnews.ru/obshchestvo/2024/08/27/v-rossii-pridumali-sposob-zashchity-bespilotnikov-ot-kiberatak/> (дата обращения: 18.05.2024)**.

Статья поступила в редакцию 22.04.2025; принята к публикации 10.05.2025

Информация об авторах

Руденко Н.А. – студент кафедры «Системы информационной безопасности», направление подготовки 10.05.03 – Информационная безопасность автоматизированных систем ФГБОУ ВО «БГТУ».

Березкин Ф.Е. – студент кафедры «Системы информационной безопасности», направление подготовки 10.05.03 – Информационная безопасность автоматизированных систем ФГБОУ ВО «БГТУ».

Вклад авторов

Руденко Н.А. – идея, сбор материала, обработка материала, частичное написание статьи.

Березкин Ф.Е. – идея, сбор материала, обработка материала, частичное написание статьи.

Научный руководитель

Шапенская А.М. – ассистент кафедры «Системы информационной безопасности» ФГБОУ ВО «БГТУ».

Конфликт интересов отсутствует.

* Ссылка на страницу с описанием ВКР, сам текст может быть недоступен, но тема и аннотация релевантны.

** Новостная заметка, использовать с осторожностью, как указание на направление разработок.

Научная статья
УДК 623.7:004.8

Методы выявления и классификации беспилотных летательных аппаратов с использованием искусственного интеллекта

Иван Александрович Шведчиков

Брянский государственный технический университет, Брянск, Россия
ivan_shvedchikov@vk.com, <https://orcid.org/0009-0002-5507-5862>

Аннотация. Статья исследует методы выявления и классификации БПЛА с применением искусственного интеллекта. Проанализированы современные подходы на основе нейросетей: радиолокационные, оптико-электронные и радиочастотные системы с их преимуществами и ограничениями. Рекомендована интеграция мультимодальных данных и разработка адаптивных классификаторов. Результаты демонстрируют потенциал ИИ в противодействии несанкционированному использованию дронов и необходимость дальнейших исследований.

Ключевые слова: БПЛА, искусственный интеллект, машинное обучение, нейронные сети, классификация, безопасность.

Для цитирования: Шведчиков И.А. Методы выявления и классификации беспилотных летательных аппаратов с использованием искусственного интеллекта // Актуальные проблемы кибербезопасности. Противодействие экстремизму и терроризму в информационной молодежной среде: сборник докладов I межрегиональной научно-практической конференции. – Брянск: БГТУ, 2025. – С. 403 – 405.

С развитием технологий беспилотные летательные аппараты стали широко применяться в сельском хозяйстве, логистике, мониторинге и военных операциях. Однако их несанкционированное использование создает угрозы для безопасности. Только за 2024 год количество сбитых БПЛА на территории РФ превышает 7 тысяч единиц. Это подчеркивает важность разработки эффективных методов их выявления и классификации.

Основные технологические направления в обнаружении БПЛА

Современные радиолокационные комплексы, оснащенные алгоритмами глубокого обучения, демонстрируют радикальное улучшение характеристик обнаружения малоразмерных целей. Нейросети U-Net архитектуры, обученные на синтезированных радиолокационных изображениях, позволяют выделять сигнатуры дронов на фоне природных помех с точностью до 94%. Ключевым преимуществом становится способность распознавать БПЛА с радиолокационной эффективной поверхностью рассеяния (ЭПР) менее 0.01 м² на дистанциях до 5 км, что в 3 раза превосходит показатели традиционных систем [3].

Прорыв в области компьютерного зрения на базе трансформерных архитектур типа Vision Transformer (ViT) обеспечил качественный скачок в визуальном обнаружении БПЛА. Системы, использующие предобученные модели YOLOv8 и EfficientDet, демонстрируют точность распознавания 98.7% на тестовых наборах данных, содержащих 150 категорий дронов [4]. Для компенсации

эффектов частичной окклюзии и изменений освещенности применяются методы мультиспектрального анализа, комбинирующие данные видимого и инфракрасного диапазонов.

Экспериментальные системы на базе гибридных нейросетей, демонстрируют возможность обнаружения дронов размером 15 см на дистанции 1.2 км в условиях городской застройки, что на 40% превосходит аналогичные показатели систем предыдущего поколения [5].

Глубокий анализ RF-сигнатур с использованием LSTM-сетей позволяет идентифицировать тип БПЛА по характеристикам модуляции несущей частоты. Алгоритмы автоматической классификации, основанные на градиентном бустинге, обеспечивают точность категоризации 96.8%.

Современные системы реализуют трехуровневую классификационную модель:

1. Аппаратный уровень: анализ конструктивных особенностей через комбинацию LiDAR и радиолокационных данных
2. Функциональный уровень: оценка паттернов движения с использованием временных рядов и методов анализа траекторий
3. Угрозный уровень: прогнозирование потенциальных рисков на основе данных телеметрии и внешних контекстных признаков

Гибридные архитектуры, сочетающие Graph Neural Networks (GNN) и Transformer-модели, позволяют обрабатывать разнородные данные от сенсорных сетей, достигая F1-меры 0.93 при идентификации 12 категорий дронов.

Нейросетевые алгоритмы онлайн-обучения типа Online Random Forests адаптируются к появлению новых классов БПЛА без необходимости полного переобучения модели [2].

Современные системы защиты объединяют до 7 различных методов обнаружения в единый когнитивный контур:

1. Радиолокационный мониторинг с адаптивным формированием луча
2. Мультиспектральный видеоанализ
3. Радиочастотная триангуляция
4. Акустическая идентификация
5. Сетевые сенсоры IoT
6. Спутниковая навигационная разведка
7. Сигнатурный анализ телеметрических данных

Нейросетевой координационный центр на базе архитектуры Mixture of Experts (MoE) осуществляет сенсорный фьюжн данных, обеспечивая вероятность правильного обнаружения 99.2% при уровне ложных тревог менее 0.1% [1].

Практические реализации и тестовые результаты

Инновационные разработки, такие как российский комплекс "Циклон", интегрируют каскад из 7 сверточных нейросетей, анализирующих доплеровские спектры и пространственно-временные характеристики сигналов. Это позволяет

не только детектировать цель, но и прогнозировать ее траекторию с погрешностью менее 1.5 м на временном горизонте 10 секунд [6].

Система "Булат v.4" продемонстрировала эффективность обнаружения 98.4% БПЛА в условиях плотной городской застройки, при этом среднее время классификации составило 850 мс [5].

В ходе полевых испытаний системы на базе YOLOv8 достигли точности 96.7% при распознавании FPV-дронов на скоростях до 120 км/ч, обрабатывая 45 кадров в секунду на embedded-платформах NVIDIA Jetson Orin.

Перспективные направления исследований сосредоточены на разработке квантовых нейросетей для обработки RF-сигналов, создании цифровых двойников воздушного пространства и имплементации федеративного обучения для распределенных сенсорных сетей

Список источников

1. Бердымуратов Д. Б. Анализ систем идентификации и формирования базы данных беспилотных летательных аппаратов. URL: <https://cyberleninka.ru/article/n/analiz-sistem-identifikatsii-i-formirovaniya-bazy-dannyh-bespilotnyh-letatelnyh-apparatov/viewer> (дата обращения: 07.03.2025).
2. Классификация беспилотных летательных аппаратов. URL: <https://antidrone.kaspersky.com/ru/klassifikaciya-dronov/> (дата обращения: 07.03.2025).
3. Средства обнаружения, защиты и подавления БПЛА. URL: <https://nii-vektor.ru/protivodejstvie-bpla/> (дата обращения: 07.03.2025).
4. Применение компьютерного зрения для управления беспилотными летательными аппаратами с искусственным интеллектом. URL: <https://www.ultralytics.com/ru/blog/computer-vision-applications-ai-drone-uav-operations> (дата обращения: 07.03.2025).
5. «Булат» v.4 и искусственный интеллект: обнаружение дронов с нейросетью. URL: <https://3mx.ru/articles/bulatv4-i-iscusstvenniy-intellect-obnaruzheniye-dronov-neyrosetiu> (дата обращения: 07.03.2025).
6. ЦНИИ Циклон: нейросеть для обнаружения дронов. URL: https://www.tadviser.ru/index.php/Продукт:ЦНИИ_Циклон:_Нейросеть_для_обнаружения_дронов (дата обращения: 07.03.2025).

Статья поступила в редакцию 22.04.2025; принята к публикации 10.05.2025

Информация об авторе

Шведчиков И.А. – студент кафедры «Цифровая экономика», направление подготовки 09.03.03 – Прикладная информатика, профиль «Информационные технологии в цифровой экономике» ФГБОУ ВО «БГТУ».

Научный руководитель

Симутин В.В. – ст. преподаватель каф. «СИБ» ФГБОУ ВО «БГТУ».

Научная статья
УДК 623.7:004.8

Рой БПЛА: координация и управление группой дронов

Иван Александрович Шведчиков

Брянский государственный технический университет, Брянск, Россия
ivan_shvedchikov@vk.com, <https://orcid.org/0009-0002-5507-5862>

Аннотация. Статья исследует методы координации и управления роями БПЛА. Выполнен анализ централизованных, децентрализованных и гибридных систем управления с оценкой их эффективности при масштабировании. Рассмотрены протоколы связи и биологически инспирированные алгоритмы коллективного поведения. Представлены практические кейсы применения в сельском хозяйстве и поисково-спасательных операциях.

Ключевые слова: роевой интеллект, БПЛА, децентрализованное управление, мультиагентные системы, межмашинное взаимодействие, кластерная координация.

Для цитирования: Шведчиков И.А. Рой БПЛА: координация и управление группой дронов // Актуальные проблемы кибербезопасности. Противодействие экстремизму и терроризму в информационной молодежной среде: сборник докладов I межрегиональной научно-практической конференции. – Брянск: БГТУ, 2025. – С. 406 – 409.

Современные технологии управления группами беспилотных летательных аппаратов (БПЛА) переживают этап трансформации, связанный с переходом от централизованных систем к децентрализованным архитектурам на основе принципов роевого интеллекта. Последние достижения в области алгоритмов коллективного взаимодействия, сетевых коммуникаций и распределённого принятия решений позволяют создавать сложные самоорганизующиеся системы, способные выполнять задачи в динамически изменяющихся условиях. Ключевыми направлениями развития стали гибридные модели управления, сочетающие элементы кластеризации, многоуровневые коммуникационные протоколы и биологически вдохновлённые подходы к координации.

Архитектурные подходы к организации роевого управления

Традиционные централизованные системы управления предполагают наличие единого центра принятия решений, который обрабатывает данные от всех участников группы и распределяет управляющие команды. Такой подход обеспечивает простоту реализации, но становится неэффективным при масштабировании группы свыше 20-30 аппаратов из-за латентности связи и риска единой точки отказа [1]. В сельскохозяйственных мониторинговых системах, где требуется одновременный охват обширных территорий, эти ограничения особенно критичны [2].

Децентрализованные архитектуры, напротив, наделяют каждый БПЛА автономной системой управления, способной взаимодействовать с соседями через локальные коммуникационные каналы. Такой подход позволяет рой сохранять работоспособность при выходе из строя отдельных элементов, имитируя поведение биологических стай [2]. В многослойных сетях дроны образуют кластеры с

шлюзовыми узлами, обеспечивающими межгрупповое взаимодействие, что повышает отказоустойчивость системы [3].

Современные разработки, такие как алгоритм кластерного управления с динамическим лидером, сочетают преимущества обоих подходов. В этой модели:

1. Лидерский БПЛА с расширенными вычислительными мощностями осуществляет стратегическое планирование.
2. Кластеры аппаратов перераспределяют задачи внутри группы.
3. Механизм автоматического переключения лидера при сбоях обеспечивает непрерывность операций.

Эксперименты показывают 23% повышение эффективности при поисково-спасательных операциях по сравнению с чисто децентрализованными системами [5].

Эффективность роя напрямую зависит от архитектуры коммуникационной сети. Модель, рассматривающая группу БПЛА как распределённую сетевую систему управления (NCS), где каждый узел выполняет двойную функцию – сбор данных и участие в коллективном принятии решений [4]. Использование адаптивных маршрутизаторов на базе протокола OLSR (Optimized Link State Routing) позволяет сократить задержки передачи данных до 120 мс при плотности сети 50 узлов/км [3].

Ключевым вызовом остаётся обеспечение временной синхронизации в условиях:

1. Неоднородных каналов связи (радио, лазерные, спутниковые).
2. Динамического изменения топологии сети.
3. Угроз кибербезопасности.

Внедрение блокчейн-технологий для верификации транзакций между дронами позволило снизить риск несанкционированного доступа на 67% в тестовых условиях. Для критически важных систем применяется трёхуровневая модель аутентификации:

1. Биометрическая идентификация оператора.
2. Цифровые сертификаты аппаратов.
3. Шифрование данных по стандарту AES-256.

Принципы стайного поведения птиц и роя насекомых легли в основу алгоритма Voids, модифицированного российскими исследователями для задач группового полёта. Основные правила:

1. Сохранение дистанции (минимальное расстояние $1.5D$, где D – диаметр БПЛА).
2. Выравнивание скорости (погрешность ≤ 2 м/с).
3. Стремление к центру группы (весовой коэффициент 0.7).

Тестирование в ветровых условиях до 15 м/с подтвердило стабильность формации при угле атаки до 25° .

Новаторский подход СКФУ предполагает использование механизма виртуального голосования, где каждый дрон оценивает:

1. Собственную загрузку процессора.

2. Уровень заряда батареи.
3. Качество связи с соседями.
4. Тактические параметры задачи.

Алгоритм на основе модифицированного метода формирует рейтинг приоритетов, перераспределяя задачи в реальном времени [5]. В испытаниях с 12 БПЛА система продемонстрировала 98% успешности выполнения миссий при 30% отказе элементов.

Практические приложения и кейсы

Сельскохозяйственный мониторинг. В проекте ЛЭТИ группа из 8 дронов с гиперспектральными камерами осуществляет:

1. Ежесуточный мониторинг 500+ га.
2. Автоматическое обнаружение болезней растений (точность 89%).
3. Точечное внесение удобрений (экономия реагентов до 40%).

Система использует комбинированный алгоритм, сочетающий кластеризацию k-means и нечёткую логику для адаптации к изменяющимся условиям освещённости [2].

Поисково-спасательные операции. При тестировании в горной местности группа из 6 БПЛА сократила время поиска на 58% по сравнению с одиночными аппаратами [5].

Перспективные направления исследований

Квантовые коммуникации

Эксперименты с запутанными фотонными парами демонстрируют возможность создания защищённых каналов связи со скоростью передачи данных 1 Гбит/с на расстоянии 50 км. Основные проблемы:

1. Стабилизация квантовых состояний в подвижных платформах.
2. Интеграция с классическими сетями.
3. Энергопотребление криогенных систем.

Нейроморфные вычисления на борту

Внедрение мемристорных чипов позволяет реализовать:

1. Онлайн-обучение нейросетей непосредственно в полёте.
2. Распознавание образов с задержкой ≤ 15 мс.
3. Адаптацию к непредвиденным событиям через механизм обратной связи.

Пилотные проекты показывают 40% снижение потребления энергии по сравнению с GPU-решениями.

Список источников

1. Мустаев А.Ф. Стратегии управления роем беспилотных летательных аппаратов // Вестник науки. №3 (12). Т. 5. С. 96 - 99. 2019. URL: <https://www.вестник-науки.пф/article/1100> (дата обращения: 08.03.2025).

2. Нгуа Ндонг Авеле Ж. Б. Разработка программно-алгоритмического обеспечения для управления роем беспилотных летательных аппаратов // Изв. СПбГЭТУ «ЛЭТИ». 2023. Т. 16, № 1. С. 66–76. doi: 10.32603/2071-8985-2023-16-

1-66-76. URL: https://izv.etu.ru/assets/files/izvestiya-1-2023-66-76_.pdf (дата обращения: 08.03.2025).

3. Довгаль Д. В. Анализ систем коммуникационного взаимодействия дронов, выполняющих поисковую миссию в составе группы // Вестник АГУ. 2020. № 271. С. 84-94. URL: <http://vestnik.adygnet.ru/files/2020.4/6465/87-94.pdf> (дата обращения: 08.03.2025).

4. Довгаль А. Д. Интеграция сетей и вычислений для построения системы управления роем дронов как сетевой системы управления // Вестник АГУ. 2022. № 296. С. 62-76. URL: <http://vestnik.adygnet.ru/files/2022.1/6814/62-76.pdf> (дата обращения: 08.03.2025).

5. Дроны как пчелиный рой. URL: <https://ncfu.ru/novosti/glavnaya/drony-kak-pchelinyy-roy-2031/> (дата обращения: 08.03.2025).

Статья поступила в редакцию 22.04.2025; принята к публикации 10.05.2025

Информация об авторе

Шведчиков И.А. – студент кафедры «Цифровая экономика», направление подготовки 09.03.03 – Прикладная информатика, профиль «Информационные технологии в цифровой экономике» ФГБОУ ВО «БГТУ».

Научный руководитель

Симутин В.В. – ст. преподаватель каф. «СИБ» ФГБОУ ВО «БГТУ».