

ПЕРМСКИЙ
ГОСУДАРСТВЕННЫЙ
НАЦИОНАЛЬНЫЙ
ИССЛЕДОВАТЕЛЬСКИЙ
УНИВЕРСИТЕТ

АКТУАЛЬНЫЕ ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Сборник статей

Выпуск 1



МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное
образовательное учреждение высшего образования
ПЕРМСКИЙ ГОСУДАРСТВЕННЫЙ
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ

АКТУАЛЬНЫЕ ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Сборник статей

Выпуск 1



Пермь 2026

УДК 004
ББК 32.81
А437

Актуальные проблемы информационной безопасности
А437 [Электронный ресурс] : сборник статей / Пермский государственный национальный исследовательский университет. – Электронные данные. – Пермь, 2026. – Вып. 1. – 1,56 Мб ; 118 с. – Режим доступа: <http://psu.ru/files/docs/science/books/sborniki/aktualnye-problemy-informacionnoj-bezopasnosti-2026.pdf> – Заглавие с экрана.

ISBN 978-5-7944-4354-7

Сборник содержит статьи, посвященные различным проблемам информационной безопасности, являющимся наиболее актуальными в настоящее время в Российской Федерации. Данный выпуск сборника отражает результаты исследований по вопросам информационной безопасности, проводимых на различных предприятиях и в организациях Пермского края.

Материалы сборника предназначены для специалистов в области информационной безопасности.

**УДК 004
ББК 32.81**

*Издается по решению ученого совета
института компьютерных наук и технологий
Пермского государственного национального исследовательского университета*

Редакторы:

Е. А. Рабчевский (ответственный редактор),
Н. И. Григоров, Е. Ю. Никитина, А. Н. Рабчевский, А. В. Черников

Рецензенты: канд. техн. наук, доцент кафедры экономики ПГГПУ
А. Г. Кузнецов
д-р техн. наук, профессор **О. Г. Пенский**

ISBN 978-5-7944-4354-7

© ПГНИУ, 2026

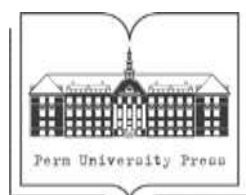
MINISTRY OF SCIENCE AND HIGHER EDUCATION
OF THE RUSSIAN FEDERATION

Federal State Autonomous
Educational Institution of Higher Education
PERM STATE UNIVERSITY

ACTUAL PROBLEMS OF INFORMATION SECURITY

Collection of Research Articles

Issue 1



Perm 2026

UDC 004
BBK 32.81

Actual problems of information security [Electronic resource] : collection of articles / Perm State University. – Electronic data. – Perm, 2026. – Issue 1. – 1,56 Mb ; 118 p. – Access mode: <http://psu.ru/files/docs/science/books/sborniki/aktualnye-problemy-informacionnoj-bezopasnosti-2026.pdf>. – Title from the screen.

ISBN 978-5-7944-4354-7

The collection contains articles on various information security issues that are currently the most relevant in the Russian Federation. This issue of the collection reflects the results of information security research conducted at various enterprises and organizations in the Perm Region. The materials of the collection are intended for specialists in the field of information security.

UDC 004
BBK 32.81

*Published by the decision of the Scientific Council
of the Institute of Computer Science and Technology of the Perm State University*

Editors:

E. A. Rabtchevsky (responsible editor),
N. I. Grigorov, E. Yu. Nikitina, A. N. Rabtchevsky, A. V. Tchernikov

Reviewers: Associate Professor of the Department of Economics of PSHPU,
Candidate of Technical Sciences **A. G. Kuznetsov**,
Doctor of Technical Sciences, Professor **O. G. Pensky**

ISBN 978-5-7944-4354-7

© PSU, 2026

ОГЛАВЛЕНИЕ

А.А. Абдульманов, Я.Р. Мустакимова	
Рекомендации по применению иммунных операционных систем.....	6
В.В. Савчук, М.Д. Белецкий, А.В. Черников	
Пентест, как ключевой инструмент обеспечения информационной безопасности.....	12
С.В. Брызгалов, П.В. Жданов, В.Д. Котегова, М.А. Крыжановский, Е.Д. Лядов, К.Л. Поторочина, Е.Ю. Никитина	
Разработка социальной сети "Найди друга"	22
Д.П. Гурьянов, А.Н. Рабчевский	
Самообучающийся словарь на основе больших языковых моделей.....	27
П.В. Жданов, А.Н. Рабчевский	
Имитационное моделирование процесса распространения информации в социальных сетях.....	31
Я.Р. Мустакимова, А.Н. Рабчевский	
Исследование статистики информационных атак.....	37
В.М. Авдониная, И.Н. Дорофеев, А.Д. Косберг, А.П. Кузнецов, О.П. Маринкина, Т.С. Посохина, Е.Ю. Никитина	
Разработка веб-приложения для сопровождения иностранных студентов.....	45
А.Н. Рабчевский	
Перспективы развития методов информационного противоборства.....	55
И.С. Сыпачев, Е.Ю. Никитина	
Технические методы противодействия социальной инженерии.....	60
А.Н. Трухин, А.В. Черников	
Защита информации от несанкционированного доступа на физическом уровне.....	66
А.Р. Усманов	
Медиаресурсы движения "Антифа" в антироссийской повестке.....	76
А.А. Федорочев, А.В. Черников	
Методы защиты биометрической информации человека.....	82
И.Н. Хиривимский, А.П. Шкарапута	
Современные методы стеганоанализа и защита от стеганографических атак.....	96
Е.К. Шкуренок, Е.Ю. Никитина	
Защита от финансового мошенничества.....	105
Е.О. Шолков, А.Н. Рабчевский	
Технические методы защиты интеллектуальной собственности.....	113

РЕКОМЕНДАЦИИ ПО ПРИМЕНЕНИЮ ИММУННЫХ ОПЕРАЦИОННЫХ СИСТЕМ

А.А. Абдульманов, Я.Р. Мустакимова

Пермский государственный национальный исследовательский университет

Аннотация. В данной статье рассматривается концепция иммунной операционной системы как перспективного средства защиты информации. Проведен сравнительный анализ существующих реализаций иммунных операционных систем, а также сравнение иммунных и традиционных(неиммунных) операционных систем. На основе проведенного анализа даны практические рекомендации по применению иммунных операционных систем.

Ключевые слова: *кибериммунитет, иммунные операционные системы, средства защиты информации, информационная безопасность.*

Актуальность подхода

На сегодняшний день информационные технологии получили широкое распространение в промышленности, государственных учреждениях и среди населения. Помимо того, что сфера защиты информации развивается, большинство угроз остаётся актуальными и по сей день, так как классические подходы к защите от них устаревают. В следствие чего увеличиваются:

- Количество атак на компьютеры АСУ в промышленных системах: по данным Kaspersky ICS CERT, 40,6% компьютеров АСУ, задействованных в промышленных системах, были атакованы в 2022 году. [1]
- Популярность и размеры ботнетов: по данным StormWall, в 2023 году ботнеты, представляющие собой сеть устройств, находящихся под управлением злоумышленников, включали в себя более 50 миллиардов скомпрометированных устройств. [2]
- Число атак на персональные компьютеры: по данным Kaspersky Security Network, в первом квартале 2023 зарегистрировано более 865 миллионов атак с интернет-ресурсов. К наиболее часто преследуемым целям при атаках на персональные компьютеры относятся кража денежных средств с банковских счётов, вымогательство и установка программ для добычи криптовалюты.
- Новых модификаций вирусов: по данным Kaspersky Security Network, в первом квартале 2023 года было обнаружено 9 новых семейств шифровальщиков и 3089 новых модификаций этого типа. [3]
- Число атак на медицинские учреждения: по данным MTC RED, в первом полугодии 2024 года количество критических атак на медицинские учреждения увеличилось на 32%. [4]
- Число атак на транспортные системы: по данным StormWall, в третьем квартале 2023 года количество зарегистрированных DDoS-атак в транспортной отрасли выросло на 136% по сравнению с аналогичным периодом 2022 года. [5]

В свою очередь, иммунные операционные системы предлагают иной подход в обеспечении борьбы с информационными угрозами, основанный на принципах самосовершенствования системы защиты, жёсткой изоляции процессов и степени доверенности компонентов. Иммунные операционные системы характеризуются способностью к превентивному блокированию большинства атак без дополнительной настройки, тогда как неиммунные аналоги требуют внедрения внешних средств защиты. [6] Указанное преимущество обуславливает перспективность развития данного подхода.

Определение иммунной операционной системы

Понятие «иммунная операционная система» не является общепринятым и впервые было предложено Евгением Касперским при описании концепции KasperskyOS. В основе принципа иммунности лежит сочетание двух свойств: автоматическое обнаружение угрозы и блокировка её распространения. Эти свойства реализованы по аналогии с механизмами биологической иммунной системы. [7]

Исходя из этого, иммунная операционная система – это операционная система со встроенными механизмами автономной защиты, работающими по аналогии с биологическим иммунитетом.

Сравнение текущих реализаций иммунитета операционных систем

На сегодняшний день существует не так много реализаций иммунитета операционных систем. Самыми репрезентативными примерами являются такие операционные системы как KasperskyOS, Qubes OS и IBM Digital Immune System. Данные системы демонстрируют принципиальные различия в методах обеспечения защиты от информационных угроз.

Таблица 1

Сравнительная таблица реализаций иммунитета операционных систем

Характеристика	KaspeskyOS	Qubes OS	IBM Digital Immune System
Средства обеспечения безопасности	Микроядерная архитектура, изоляция компонентов, встроенный монитор безопасности, гибкая настройка политик безопасности	Изоляция с помощью виртуализации, изоляция системных компонентов и доступа к физическим устройствам от пользовательских программ	Аналитика и машинное обучение, мониторинг, адаптация
Средства борьбы с угрозами	Мониторинг и контроль взаимодействий компонентов	Изоляция заражённого контейнера	Обновление центральной базы данных и распространение обновлений
Сфера применения	Логические контроллеры, интернет вещей, автомобили, сетевое оборудование, встраиваемая электроника, доверенные рабочие станции	Персональные компьютеры	ЭВМ, входящие в состав корпоративных информационных систем

KasperskyOS

KasperskyOS – микроядерная операционная система, основой которой служит микроядро с расширенными функциями безопасности, разработанное специалистами «Лаборатории Касперского». Контроль всех междоменных взаимодействий осуществляется службой Kaspersky Security System, что позволяет формально доказать выполнение политик безопасности. ОС сертифицирована ФСТЭК и применяется в логических контроллерах, IoT-шлюзах, транспортных системах и на объектах критической инфраструктуры. [8]

Qubes OS

Qubes OS — это бесплатная операционная система с открытым исходным кодом. Она использует гипервизор для создания изолированных виртуальных окружений, каждое из которых получает собственные права доступа и цветовую метку доверия. Такой подход оправдывает себя на персональных рабочих станциях, где требуется разделить служебную и личную информацию без затрат на покупку дополнительного оборудования. [9]

IBM Digital Immune System

В отличие от перечисленных выше реализаций, IBM Digital Immune System — не операционная система, а сам механизм иммунитета, который может быть встроен в любую систему. Он объединяет телеметрию, машинное обучение и автоматическое создание сигнатур. Данный механизм развивается как сервис корпоративного класса, нацеленный на обнаружение и блокировку аномалий в режиме реального времени, а также на оперативное обновление защитных политик. [10]

Сравнение иммунных и неиммунных операционных систем

Иммунные операционные системы обладают рядом преимуществ и недостатков по сравнению с традиционными, неиммунными системами.

К преимуществам иммунных операционных систем относятся:

- Минимизация рисков: подавляющее большинство типов атак на иммунную операционную систему неэффективно и не может повлиять на выполнение ею критических функций. Данный подход обеспечивает надежность и прогнозируемость работы информационных систем.
- Автономная защита: иммунные операционные системы обладают способностью самостоятельно обнаруживать и реагировать на угрозы без необходимости внешнего вмешательства или дополнительных средств защиты, что снижает зависимость от обновлений и внешних систем безопасности.
- Использование иммунной операционной системы позволяет сократить расходы на разработку и поддержку защищенных решений: поскольку операционная система самостоятельно обеспечивает требуемый уровень безопасности, отпадает необходимость в реализации дополнительных защитных механизмов на уровне прикладных программ. [1]

Однако иммунные операционные системы также обладают и недостатками:

- Высокая ресурсоёмкость: механизмы адаптивной защиты, такие как машинное обучение, постоянный анализ поведения и виртуализация, требуют

значительных вычислительных ресурсов, что может сильно снижать производительность системы в целом.

- Сложность настройки и управления: иммунные операционные системы требуют специализированных знаний для эффективного администрирования, что может осложнить их использование неподготовленными пользователями.

- Ложные срабатывания: автономные системы защиты могут ошибочно идентифицировать безопасные процессы как угрозы, что может приводить к сбоям в работе программ.

- Совместимость: архитектура безопасности иммунных операционных систем накладывает особые требования к разработке программного обеспечения, при создании приложений необходимо учитывать специфику работы защитных механизмов системы.

Таким образом, иммунные операционные системы не могут полностью заменить традиционные операционные системы, однако их архитектурная ориентированность на обеспечение информационной безопасности обуславливает более высокую эффективность в части защиты данных по сравнению с неиммунными аналогами.

Рекомендации по применению

Совокупность рассмотренных преимуществ иммунных операционных систем перед традиционными позволяет прогнозировать их повсеместное распространение в долгосрочной перспективе. Вместе с тем, принципиальные архитектурные отличия иммунных операционных систем обуславливают необходимость разработки специальных рекомендаций по их применению. В рамках настоящего исследования предлагается следующий подход:

1. Выбор иммунной операционной системы

Тип операционной системы (по классификации ФСТЭК) должен быть подобран в соответствии со сценарием её использования. Тип «А» – для систем общего назначения, тип «Б» – для систем, предназначенных для решения заранее определённых задач, тип «В» – для систем, предназначенных для обеспечения реагирования на события в рамках заданных временных ограничений при заданном уровне функциональности.

Класс защиты ОС должен отвечать требованиям защищённости обрабатываемой информации. 1, 2 и 3 класс – для систем, обрабатывающих информацию, содержащую государственную тайну; 4 класс – для информационных систем 1 класса защищённости, автоматизированных систем управления производственными и технологическими процессами 1 класса защищённости, информационных систем персональных данных при необходимости обеспечения 1 уровня защищённости персональных данных, информационных систем общего пользования 2 класса; 5 класс – для государственных информационных системах 2 класса защищённости, автоматизированных систем управления производственными и технологическими процессами 2 класса защищённости, информационных систем персональных данных при необходимости обеспечения 2 уровня защищённости персональных данных; 6 класс – для государственных информационных систем 3 и 4 классов защищённости, автоматизированных си-

стем управления производственными и технологическими процессами 3 класса защищенности, информационных систем персональных данных при необходимости обеспечения 3 и 4 уровней защищенности персональных данных. [11]

При выборе операционной системы необходимо отдавать предпочтение отечественным решениям. Это позволяет обеспечить технологическую независимость и защиту от санкционных рисков, гарантирует соответствие требованиям законодательства, а также имеется возможность получить локализованную поддержку.

2. Настройка

Необходимо настроить механизмы защиты, являющиеся отличительной особенностью иммунных операционных систем. Например, необходимо определить политики безопасности, которые жестко регламентируют все информационные потоки между изолированными процессами. Также следует активировать защиту с использованием аппаратной виртуализации для изоляции критических процессов. Конкретный состав активируемых механизмов защиты зависит от того, какая именно операционная система была выбрана.

3. Эксплуатация

Необходимо отдавать предпочтение программному обеспечению, учитывающему особенности иммунной операционной системы и отвечающему требованиям защищенности обрабатываемой информации.

Заключение

В данной статье была рассмотрена концепция иммунной операционной системы как перспективного средства защиты информации. Был проведен сравнительный анализ существующих реализаций таких систем, а также их сравнение с неиммунными операционными системами. Также были сформулированы практические рекомендации, которые помогут эффективно использовать иммунные операционные системы с учетом их особенностей. Можно сделать вывод, что применение таких систем открывает новые возможности для обеспечения безопасности и устойчивости информационной инфраструктуры в условиях современных угроз.

Список литературы

1. Kaspersky Cyber Immunity [Электронный ресурс] URL: <https://os.kaspersky.ru/uncategorized/1kaspersky-cyber-immunity/> (дата обращения: 15.04.2025)
2. StormWall: за 2023 год численность ботнетов для DDoS-атак выросла на 300%. CISOCUB [Электронный ресурс] URL: <https://cisoclub.ru/stormwall-za-2023-god-chislennost-botnetov-dlja-ddos-atak-vyrosla-na-300> (дата обращения: 15.04.2025)
3. Kaspersky. Статистика по вредоносным программам для ПК, первый квартал 2023 г. Securelist [Электронный ресурс] URL: <https://securelist.ru/it-threat-evolution-q1-2023-pc-statistics/107526> (дата обращения: 15.04.2025)
4. Количество кибератак на российские медучреждения увеличилось на 32% Computerra [Электронный ресурс] URL:

<https://www.computerra.ru/299858/kolichestvo-kiberatak-na-rossijskie-meduchrezhdeniya-uvelichilos-na-32> (дата обращения: 15.04.2025)

5. Отчет о DDoS-атаках за третий квартал 2023 г. StormWall [Электронный ресурс] URL: <https://stormwall.pro/otchet-o-ddos-atakah-2023-tretij-kvartal> (дата обращения: 15.04.2025)

6. Общие вопросы о KasperskyOS [Электронный ресурс] URL: <https://os.kaspersky.ru/faq-general/> (дата обращения: 22.03.2025)

7. Лукьян А. В. «Концепция иммунитета в информационной безопасности». Материалы конференции «Цифровая подстанция» [Электронный ресурс] URL: <https://digitalsubstation.com/wp-content/uploads/2019/06/2.-Lukiyan-Immunity-Concept-RU.pdf> (дата обращения: 22.03.2025)

8. KasperskyOS: кибериммунный подход [Электронный ресурс] URL: <https://os.kaspersky.ru/media/KasperskyOS-Cyber-Immune-Approach-Ru.pdf> (дата обращения: 22.03.2025)

9. Introduction to Qubes OS [Электронный ресурс] URL: <https://www.qubes-os.org/intro/> (дата обращения: 22.03.2025).

10. Digital Immune System. Croyten. [Электронный ресурс] URL: <https://croyten.com/digital-immune-system/> (дата обращения: 22.03.2025)

11. Федеральная служба по техническому и экспортному контролю. Информационное сообщение от 18 октября 2016 г. № 240/24/4893 «Об утверждении Требований безопасности информации к операционным системам». ФСТЭК России [Электронный ресурс] URL: <https://fstec.ru/dokumenty/vse-dokumenty/informatsionnye-i-analiticheskie-materialy/informatsionnoe-soobshchenie-fstek-rossii-ot-18-oktyabrya-2016-g-n-240-24-4893> (дата обращения 10.06.2025)

RECOMMENDATIONS FOR THE USE OF IMMUNE OPERATING SYSTEMS

A.A. Abdulmanov, Y.R. Mustakimova

Perm State University

Abstract. This article examines the concept of an immune operating system as a promising information security tool. A comparative analysis of existing immune operating system implementations is provided, as well as a comparison of immune and traditional (non-immune) operating systems. Based on this analysis, practical recommendations for the use of immune operating systems are provided.

Keywords: *cyberimmunity, immune operating system, information security tools, information security.*

ПЕНТЕСТ, КАК КЛЮЧЕВОЙ ИНСТРУМЕНТ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В.В. Савчук, М.Д. Белецкий, А.В. Черников

Пермский государственный национальный исследовательский университет

Аннотация. В статье рассматриваются современные подходы к тестированию на проникновение (пентестингу) как ключевому инструменту обеспечения информационной безопасности. Анализируются виды пентестинга, этапы проведения, используемые инструменты, нормативно-правовая база в России и виды атак злоумышленников. Особое внимание уделено актуальности пентестинга в условиях роста угроз информационной безопасности и предложениям по совершенствованию его регулирования.

Ключевые слова: *пентест, информационная безопасность, защита данных.*

В современном цифровом мире вопросы информационной безопасности становятся все более актуальными. С развитием технологий растет количество атак, направленных на получение несанкционированного доступа к данным, нарушения работы информационных систем и компрометацию конфиденциальной информации. Одним из ключевых инструментов обеспечения информационной безопасности является тестирование на проникновение (пентестинг), позволяющее выявлять уязвимости и оценивать степень защищенности IT-инфраструктуры.

Пентестинг (от англ. penetration testing, или "тестирование на проникновение") представляет собой метод оценки защищенности информационных систем, при котором специалисты моделируют действия злоумышленников. В ходе такой проверки уязвимостей, способных привести к нарушению работы системы или несанкционированному доступу к конфиденциальным данным.

Пентестер – это квалифицированный специалист по информационной безопасности, который проводит контролируемые атаки на IT-системы с целью обнаружения их слабых мест. В отличие от хакеров, пентестеры действуют легально, по договору с владельцем системы, и предоставляют детальные рекомендации по устранению найденных уязвимостей.

Проводя тестирование на проникновение, эксперты решают несколько ключевых задач:

Обнаружение уязвимостей – выявление потенциальных слабых мест в IT-инфраструктуре, которые могут быть использованы злоумышленниками.

Оценка угроз – анализ возможных векторов атак и определение степени риска для критических важных систем организации.

Тестирование защитных систем – проверка эффективности существующих механизмов безопасности при различных сценариях кибератак.

Разработка рекомендаций – подготовка конкретных предложений по устранению выявленных уязвимостей и усилению защиты.

Профилактика атак – снижение рисков успешных кибервзломов за счет устранения потенциальных точек проникновения.

Обеспечение безопасности – поддержание конфиденциальных данных, целостности системы и непрерывности бизнес-процессов [1].

Основные виды пентестинга

Тестирование белого ящика (White Box): тестировщик обладает полной информацией о системе, включая исходный код, конфигурации сети и архитектуры. Этот метод позволяет глубоко анализировать систему и выявлять скрытые уязвимости.

Тестирование черного ящика (Black Box): тестировщик не обладает предварительной информацией о системе и ведет себя как злоумышленник, который впервые столкнулся с системой. Это наиболее приближенный к реальным атакам сценарий.

Тестирование серого ящика (Gray Box): тестировщик имеет ограниченный доступ к информации о системе, например, учетные данные с ограниченными привилегиями. Такой подход позволяет сфокусироваться на выявлении уязвимостей, которые могут быть использованы внутренними нарушителями [2].

Правовые основы тестирования на проникновение в Российской Федерации

Проведение пентестинга должно соответствовать действующим нормативно-правовым актам, чтобы избежать нарушений законодательства. В России нормативно-правовая база в сфере пентестинга охватывает законы, регулирующие защиту информации, критическую информационную инфраструктуры и персональные данные.

Современное правовое поле в области пентестинга формируется тремя ключевыми законодательными актами:

Федеральный закон «Об информации, информационных технологиях и о защите информации» (№ 149-ФЗ): устанавливает фундаментальные принципы защиты информации. В контексте пентестинга особое значение имеют положения о:

- обязанностях организаций предотвращению несанкционированного доступа;
- правовые ограничения при проведении атак;
- ответственности за нарушение конфиденциальности данных [3].

Закон "О персональных данных" (№ 152-ФЗ): нормативный акт, требующий особой осторожности при тестировании системы, содержащих данные. Основные требования:

- обязательное согласование с оператором ПД;
- специальные меры защиты при работе с конфиденциальной информацией;

- повышенная ответственность за нарушения [4].

Закон "О безопасности КИИ" (№ 187-ФЗ): вводит особый режим тестирования для объектов критической инфраструктуры:

- обязательное лицензирование исполнителей;
- согласование методик с регуляторами;
- специальные требования к отчетности [5].

Детализация законодательных норм осуществляется через систему подзаконных актов:

Постановления Правительства: документ №127 определяет порядок категорирования объектов КИИ, устанавливая:

- критерии отнесения к критически важным объектам;
- периодичность обязательных проверок;
- требования к квалификации специалистов [6].

Нормативы ФСТЭК: ведомственные приказы (№17, 21) конкретизируют:

- методики тестирования для государственных систем;
- требования к защите автоматизированных систем управления;
- стандарты оформления результатов [7], [8].

Регламенты Банка России: для финансового сектора действуют особые правила (Положения №382-П, 683-П, 684-П), предусматривающие:

- обязательную регулярность проверок;
- тестирование всех компонентов банковских систем;
- специальные требования к защите транзакций [9], [10], [11].

Требования ФСБ: приказ №66 устанавливает особый порядок работы с криптографическими системами, включая:

- необходимость специальных лицензий;
- ограничения на методы тестирования;
- дополнительные требования к отчетности [12].

Основные инструменты тестирования на проникновение

Тестирование на проникновение невозможно без специализированных инструментов, которые позволяют автоматизировать процесс поиска уязвимостей и их эксплуатации. На сегодняшний день наиболее востребованными являются следующие инструменты:

• **Metasploit Framework** – одна из самых популярных платформ для тестирования на проникновения. Позволяет автоматизировать эксплуатацию уязвимостей, создать пользователей эксплойты и проводить анализ защищенности системы.

• **Nmap (Network Mapper)** – инструмент для тестирования сетей, который помогает выявлять активные узлы, открытые порты и запущенные сервисы.

• **Burp Suite** – комплексное средство для тестирования веб-приложений. Включает в себя прокси-сервер, сканер уязвимостей и другие инструменты для анализа трафика и атак на веб-сайты.

- **Wireshark** – мощный анализатор сетевого трафика, позволяющий изучать передаваемые данные и выявлять аномалии в работе сетевого взаимодействия.

- **John the Ripper** – инструмент для подбора паролей и анализа их стойкости. Используется для тестирования надежности учетных записей.

- **SQLmap** – автоматизированный инструмент для обнаружения и эксплуатации SQL-инъекций, который помогает находить уязвимости в базах данных.

- **Hydra** – утилита для брутфорс-атак на учетные записи, используемая для проверки стойкости паролей различных сервисов.

- **Nikto** – веб сканер, предназначенный для выявления уязвимостей в веб-серверах и их конфигурации [13-15].

Каждый из этих инструментов выполняет свою функцию и часто используются в едином комплексе, что позволяет получить наиболее полное представление о состоянии безопасности тестируемой системы.

Основные этапы проведения пентестинга

- **Планирование и определение объема тестирования.** На этом этапе уточняются цели тестирования, согласовываются правила и границы работы, а также определяется перечень систем и сервисов, которые будут подвергаться анализу.

- **Сбор информации.** Пентестеры ищут открытые порты, определяют используемые технологии и анализируют публично доступную информацию об организации или целевой системе.

- **Анализ уязвимостей.** На этом этапе пентестеры сканируют систему на предмет уязвимостей, которые могут быть использованы злоумышленниками.

- **Моделирование атак.** В зависимости от собранной информации пентестеры определяют наиболее вероятные сценарии атак, которые могли бы использовать злоумышленники.

- **Эксплуатация.** Когда обнаружены уязвимости, пентестеры проводят атаки на систему с целью получения несанкционированного доступа или перехвата данных.

- **Повышение привилегий.** Если удалось получить доступ к системе, следующим шагом является попытка повысить права учетной записи, чтобы расширить возможности атаки.

- **Закрепление доступа.** Тестировщики могут имитировать действия атакующих, которые стремятся сохранить контроль над системой для длительного использования.

- **Очистка следов.** Пентестеры оценивают, насколько легко злоумышленник мог бы скрыть свои действия, чтобы избежать обнаружения.

- **Постанализ и документация.** После завершения тестирования пентестеры составляют подробный отчет о своих действиях и результаты анализа уязвимостей. Отчет включает рекомендации по устранению обнаруженных проблем и повышению общего уровня безопасности [13,14,16].

Способы атак злоумышленников

Рассмотрим основные виды атак, используемые злоумышленниками.

1. Фишинговые атаки

Фишинг – это метод социальной инженерии, при котором злоумышленники отправляют поддельные электронные письма или сообщения с целью заставить жертву выдать конфиденциальную информацию (логины, пароли, данные банковских карт) [17].

Варианты фишинговых атак:

- **Spear Phishing** – нацеленная атака на конкретного человека или организацию.
- **Whaling Attack** – атака на топ-менеджеров и руководителей.
- **Smishing** – фишинговые атаки через SMS-сообщения.
- **Vishing** – голосовой фишинг (по телефону).

Способы защиты:

- Использование фильтров для обнаружения подозрительных писем (DMARC, SPF, DKIM).
- Обучение сотрудников распознаванию фишинга.
- Применение двухфакторной аутентификации (2FA).
- Мониторинг и анализ подозрительных ссылок и вложений.

2. Атаки с повышением привилегий (Privilege Escalation)

Злоумышленник использует уязвимости в системе для получения более высоких привилегий (например, от обычного пользователя до администратора) [17].

Способы защиты:

- Регулярное обновление ОС и ПО.
- Ограничение прав пользователей (минимально необходимые привилегии).
- Мониторинг подозрительной активности с помощью SIEM-систем.

3. Атака через уязвимости нулевого дня (Zero-Day Exploits)

Zero-day – уязвимость, которая неизвестна разработчику ПО и может быть использована злоумышленниками до выпуска исправлений [18].

Способы защиты:

- Быстрое внедрение патчей безопасности.
- Использование IDS/IPS-систем для выявления аномалий.
- Сегментация сети для минимизации ущерба.

4. Атаки на веб-приложения (SQL-инъекции, XSS, CSRF)

• **SQL-инъекции** – внедрение вредоносного SQL-кода для доступа к базам данных.

- **XSS (межсайтовый скриптинг)** – внедрение вредоносного JavaScript-кода.
- **CSRF (подделка межсайтовых запросов)** – атака, вынуждающая пользователя выполнить нежелательное действие [17].

Способы защиты:

- Использование параметризованных запросов для защиты от SQL-инъекций.
- Внедрение Content Security Policy (CSP) для предотвращения XSS.

- Применение защитных токенов (CSRF-токены) для предотвращения CSRF-атак.

5. Ransomware-атаки (шифровальщики)

Злоумышленники используют вредоносное ПО для шифрования данных и требуют деньги за их восстановление данных [18].

Способы защиты:

- Регулярное резервное копирование данных.
- Обнаружение аномального поведения с помощью EDR/XDR-систем.
- Обучение сотрудников правилам безопасности (не открывать подозрительные файлы).

6. Атаки на облачные сервисы

Неправильная конфигурация облачных хранилищ (AWS S3, Azure Blob). Кража учётных данных через фишинг или атаки «человек посередине» (MITM) [17].

Способы защиты:

- Многофакторная аутентификация.
- Шифрование данных в облаке.
- Мониторинг событий безопасности в облачных средах.

7. Атаки на цепочку поставок (Supply Chain-атаки)

Злоумышленники атакуют поставщиков ПО или оборудования, внедряя вредоносный код в программные обновления [18].

Способы защиты:

- Проверка цепочек поставок.
- Контроль целостности ПО с использованием цифровых подписей.
- Разграничение доверенных и не доверенных источников ПО.

Актуальность применения пентестинга

Актуальность пентестинга обусловлена рядом факторов, отражающих современные вызовы и угрозы в области информационной безопасности. Эти факторы, включая рост количества атак на информационные системы, ужесточение законодательства и необходимость защиты цифровых активов. Ниже рассмотрены основные причины, делающие пентестинг неотъемлемой частью стратегии информационной безопасности в условиях современных реалий.

- Эскалация угроз: современные злоумышленники используют ИИ и социальную инженерию для атак на новые технологические платформы (IoT, облака, 5G). Пнтестинг помогает опережать эти угрозы, минимизируя финансовые и репутационные риски.

- Защита критической инфраструктуры: в условиях участвовавшихся атак на энергетику и финансы пентестинг становится обязательным инструментом устойчивости ключевых объектов государственного значения.

- Комплаенс и регулирование: строгие требования законодательства к защите данных делают регулярный пентестинг необходимым условием соответствия отраслевым стандартам.

- Экономическая эффективность: проактивное выявление уязвимостей дешевле ликвидации последствий успешных информационных атак.
- Человеческий фактор: тестирование с элементами социальной инженерии выявляет слабые места в поведении персонала, повышая общий уровень грамотности в области информационной безопасности.
- Непрерывность защиты: регулярные проверки по аналогии с медосмотрами поддерживают «иммунитет» IT-систем в условиях постоянно эволюционирующих угроз.

Необходимые действия для минимизации угроз информационной безопасности с помощью средств пентестинга

Тестирование на проникновение является одной из наиболее эффективных методик выявления уязвимостей в IT-инфраструктуре. Однако, несмотря на свою важность, пентестинг сталкивается с множеством проблем и открытых вопросов. К их возможным путям решения можно отнести:

1. Обязательное регулярное проведение пентеста с использованием комбинации методов тестирования – одновременное использование ручных и автоматизированных инструментов, методов «белого», «чёрного» и «серого» ящиков, полноценные Purple Team упражнения с совместной работой Red и Blue Teams, чтобы более полно оценить защищённость системы, учитывая, как внутренние, так и внешние угрозы.

2. Постоянное совершенствование методов, инструментов и подходов к пентестингу. Создание стандартных пентест-стендов с Kali Linux, Metasploit, Burp Suite, Nessus. Внедрение AI-решений. Стремление разработать отечественный аналог Darktrace (продукт британской компании) для обнаружения аномалий на основе машинного обучения.

3. Анализ результатов и устранение уязвимостей – не просто выявление проблем, но разработка и применение стратегии по их устранению.

4. Повышение уровня подготовки специалистов – углублённое изучение сетевых технологий, криптографии, программирования и социальной инженерии для комплексной оценки угроз.

5. Интеграция пентестинга в DevSecOps-цикл. Внедрение тестирования на этапах разработки продукта.

6. Тестирование человеческого фактора – работа с персоналом, тренинги по социальной инженерии с отработкой реальных сценариев атак.

Но наиболее значимыми направлениями являются:

7. Создание специализированных регулирующих документов.

В России на сегодняшний день нет специализированного нормативного акта, напрямую регулирующего проведение тестирования на проникновение. Существующие законы (ФЗ-149, ФЗ-152, ФЗ-187) и подзаконные акты (приказы ФСТЭК, ФСБ) затрагивают лишь отдельные аспекты информационной безопасности, но не дают чётких правил для легального и безопасного пентестинга. Это создаёт правовую неопределённость:

- Отсутствие стандартов отчётности усложняет взаимодействие с регуляторами.

- Повышение рисков юридической ответственности за несанкционированный доступ даже при добросовестном тестировании.

- Размытые требования к уровню квалификации исполнителей, что иногда приводит к непрофессиональному тестированию и ложным выводам.

Принятие отдельного федерального стандарта или нормативного документа о пентестинге устранил правовые пробелы и создаст прозрачные условия для всех участников процесса. Это особенно важно в условиях роста информационных атак и ужесточения регулирования КИИ.

Целью документа должны стать задачи закрепления правовых основ пентестинга и определения:

- Кто имеет право проводить тестирование: лицензирование пентестеров и требования к квалификации.
- Установление единых методических требований к проведению пентестинга.
- Обязательное письменное соглашение с заказчиком, определяющее границы тестирования.
- Запрет на тестирование без разрешения (исключения – госзаказчики в рамках проверок КИИ).
- Ограничения на методы (например, запрет DDoS-атак без спецразрешения).
- Стандартизацию отчётности, включая обязательный перечень данных, формат документирования уязвимостей и сроки предоставления результатов.
- Обязательная передача результатов в ФСТЭК/ФСБ при обнаружении критических уязвимостей в КИИ.
- Интеграцию с отраслевыми стандартами (ФСТЭК, ЦБ РФ, КИИ) для избежания противоречий в регулировании.
- Обязательная регистрация в реестре Минцифры или ФСТЭК.

8. Создание системы сертификации для пентестеров и компаний, осуществляющих тестирование на проникновение.

Система сертификации призвана стандартизировать требования к квалификации специалистов и компаний и обеспечить высокий уровень качества услуг в области информационной безопасности. Сертификация будет носить обязательный характер для работы с государственными системами и критической информационной инфраструктурой, а также рекомендованный для коммерческого сектора. Предполагаемая система сертификации позволит:

- Упорядочить рынок услуг пентестинга, исключив недобросовестных исполнителей и снизив риски неквалифицированного тестирования.
- Повысить уровень информационной безопасности за счёт внедрения единых стандартов и лучших практик.
- Создать прозрачные условия работы для всех участников.
- Гарантировать высокий уровень квалификации специалистов через обязательную аттестацию и регулярное подтверждение компетенций.

- Стимулировать развитие отрасли за счёт повышения доверия бизнеса и государства к услугам сертифицированных пентестеров.

Заключение

В ходе исследования была обоснована важность пентестинга для обеспечения информационной безопасности информационных систем, а также были предложены дополнительные действия в области информационной безопасности для дальнейшего повышения эффективности пентестинга.

Список литературы

1. Онлайн-школа Skillfactory. Пентест. [Электронный ресурс]. URL: <https://blog.skillfactory.ru/glossary/pentest/> (дата обращения 02.04.2025).
2. Онлайн платформа Skillbox. Что такое пентесты и для чего они нужны. [Электронный ресурс]. URL: <https://skillbox.ru/media/code/chto-takoe-pentesty-i-dlya-chego-oni-nuzhny/> (дата обращения 02.04.2025).
3. Федеральный закон № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [Электронный ресурс]. URL: <http://pravo.gov.ru/proxy/ips/?docbody&nd=102108264> (дата обращения 15.04.2025).
4. Федеральный закон № 152-ФЗ от 27 июля 2006 года "О персональных данных" [Электронный ресурс]. URL: <http://pravo.gov.ru/proxy/ips/?docbody&nd=102108261> (дата обращения 15.04.2025).
5. Федеральный закон № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» [Электронный ресурс]. URL: http://pravo.gov.ru/proxy/ips/?docbody=&link_id=3&nd=102439340 (дата обращения 15.04.2025).
6. Постановление Правительства РФ от 8 февраля 2018 года № 127 "Об утверждении Правил категорирования объектов критической информационной инфраструктуры" [Электронный ресурс]. URL: <http://publication.pravo.gov.ru/Document/View/0001201802130006> (дата обращения 15.04.2025).
7. Приказ ФСТЭК № 17 от 11 февраля 2013 года [Электронный ресурс]. URL: <https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-11-fevralya-2013-g-n-17> (дата обращения 15.04.2025).
8. Приказ ФСТЭК № 21 от 18 февраля 2013 года [Электронный ресурс]. URL: <https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-18-fevralya-2013-g-n-21> (дата обращения 15.04.2025).
9. Положение Банка России № 382-П от 9 июня 2012 года "О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств" [Электронный ресурс]. URL: <https://www.garant.ru/products/ipo/prime/doc/70091962/> (дата обращения 15.04.2025).
10. Положение Банка России № 683-П от 17 апреля 2019 года "Об установлении обязательных для кредитных организаций требований к обеспечению

информационной безопасности" [Электронный ресурс]. URL: <https://base.garant.ru/72246408/> (дата обращения 15.04.2025).

11. Положение Банка России № 684-П от 17 апреля 2019 года "Об установлении обязательных для операторов платежных систем требований к обеспечению информационной безопасности" [Электронный ресурс]. URL: <https://www.garant.ru/products/ipo/prime/doc/72146094/> дата обращения 15.04.2025).

12. Приказ ФСБ № 66 от 9 февраля 2005 года "Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации" [Электронный ресурс]. URL: <https://base.garant.ru/187947/> дата обращения 15.04.2025).

13. Кибератаки на российские компании в 2024 году: аналитический отчет [Электронный ресурс] // rt-solar.ru – URL: <https://rt-solar.ru/analytics/reports/5320/> (дата обращения: 27.06.2025).

14. Инструменты для тестирования на проникновение [Электронный ресурс] // ITGLOBAL.COM. — URL: <https://itglobal.com/ru-ru/company/blog/instrumenty-dlya-testirovaniya-na-proniknovenie/> (дата обращения: 27.06.2025).

15. Инструменты для тестирования [Электронный ресурс] // Хабр. — URL: <https://habr.com/ru/articles/125317/> (дата обращения: 27.06.2025).

16. Дорожная карта по пентесту: как стать пентестером с нуля [Электронный ресурс] // Tproger. — URL: <https://tproger.ru/articles/dorozhnaja-karta-po-pentestu-kak-stat-pentesterom-s-nulja> (дата обращения: 27.06.2025).

17. Типы кибератак которыми пользуются злоумышленники [Электронный ресурс]. // c-sharpcorner.com – URL: <https://www.securitylab.ru/analytics/535598.php?clkid=e97bff62> (дата обращения: 27.06.2025)

18. Кибератаки: как нас взламывают и можно ли защититься [Электронный ресурс] // hi-tech.mail.ru - URL: <https://hi-tech.mail.ru/review/129076-kiberataka/#anchor175042322265242509> (дата обращения: 27.06.2025).

PENTESTING AS A KEY TOOL FOR INFORMATION SECURITY

V.V. Savchuk, M.D. Beletsky, A.V. Chernikov

Perm State University

Abstract. the article discusses modern approaches to penetration testing (pentesting) as a key tool for ensuring information security. It analyzes the types of pentesting, the stages of its implementation, the tools used, the regulatory framework in Russia, and the types of attacks by malicious actors. Special attention is given to the relevance of pentesting in the context of growing information security threats and proposals for improving its regulation.

Keywords: *pentesting, information security, data protection.*

РАЗРАБОТКА СОЦИАЛЬНОЙ СЕТИ «НАЙДИ ДРУГА»

*С.В. Брызгалов, П.В. Жданов, В.Д. Котегова, М.А. Крыжановский,
Е.Д. Лядов, К.Л. Поторочина, Е.Ю. Никитина*

Пермский государственный национальный исследовательский университет

Аннотация. В данной статье авторы рассмотрели проблемы, возникающие при адаптации студентов в университете. На основе анализа текущей ситуации был предложен инструмент для создания единого университетского сообщества. Особое внимание уделяется поиску единомышленников. В заключении делается вывод о важности такого инструмента.

Ключевые слова: *социальная сеть, социальные связи, учебное окружение, социальная адаптация студентов, университет.*

Исследования, проведенные Центром психолого-педагогической помощи ПГНИУ, утверждают, что одной из основных проблем, с которыми сталкиваются многие студенты в период своего обучения, является проблема адаптации к новой учебной среде. В этот период студенты переживают чувство неуверенности и изоляции. [1] Эти факторы затрудняют установление новых социальных связей и поиск групп с общими интересами в новом учебном окружении.

Несмотря на существующие возможности для знакомства внутри университета, такие как выбор элективных курсов и участие в различных клубах и организациях, студенты часто испытывают трудности в поиске новых друзей и знакомств из-за ограниченности по времени, неудобного расписания и страха знакомства с незнакомыми людьми.

Кроме того, следует отметить, что деструктивные воздействия могут осуществляться с помощью разных средств передачи информации, чаще всего которыми являются наиболее популярные на момент реализации воздействия социальные сети и мессенджеры.

Создание внутриуниверситетской социальной сети поможет снизить вероятность возникновения ситуаций, связанных с деструктивным влиянием.

Таким образом, возникает потребность в создании инструмента, который мог бы помочь студентам находить единомышленников и поддерживать социальные связи в университетской среде. Этот инструмент не только облегчит процесс адаптации, но и будет способствовать формированию дружественного и поддерживающего сообщества, что, в свою очередь, положительно скажется на успеваемости и общем комфорте студентов.

В ответ на указанные проблемы, была разработана социальная сеть «Найди друга», которая предлагает инновационный подход к поддержке социальной адаптации студентов. Эта платформа ставит перед собой несколько ключевых целей:

1. Улучшение образовательного процесса: «Найди друга» предоставляет студентам возможность обсуждать учебные вопросы, получать помощь от других студентов и поддерживать взаимную академическую мотивацию.
2. Формирование дружественного сообщества: Платформа предоставляет удобные инструменты для поиска единомышленников и организации совместных досуговых и образовательных мероприятий.
3. Активное участие в университетской жизни: Студенты могут использовать «Найди друга» для поиска информации о мероприятиях, клубах и инициативах, а также для организации своих собственных мероприятий и проектов.

Чтобы достичь поставленных целей, социальная сеть «Найди друга» была наделена функциональными возможностями, которые свойственны любой социальной сети:

1. создание персональных профилей;
2. поиск других пользователей по интересам;
3. просмотр новостей;
4. комментирование и обмен мнениями;
5. обмен сообщениями;
6. возможность выражать свою реакцию относительно просматриваемого контента.

Также были реализованы специальные функции, необходимые для социальной адаптации студентов:

1. Создание событий: сеть «Найди друга» предоставляет возможность пользователям создавать события и уведомлять других участников о возможности принять в них участие. Эти события могут включать в себя разнообразные уникальные активности и мероприятия, которые проходят в рамках университета и могут быть интересны другим пользователям. Например, это могут быть встречи для обсуждения актуальных тем, вечеринки, спортивные соревнования, культурные мероприятия и другие интересные активности.
2. Создание вопросов и обсуждений: Студенты могут использовать функцию создания вопросов и обсуждений для того, чтобы обменяться мнениями и идеями с другими участниками сообщества. Эта функция предоставляет возможность пользователям задавать вопросы по различным темам, например, касающимся учебного процесса, академических заданий, интересов и хобби. Студенты могут обсуждать важные темы, делиться своим опытом и знаниями, а также получать поддержку и советы от своих коллег. Это способствует укреплению связей между студентами и созданию благоприятной атмосферы в университетском сообществе.

Таким образом, социальная сеть «Найди друга» становится не только инструментом для улучшения социальной адаптации студентов, но и важным элементом развития университетского сообщества, способствующим формированию новых знакомств и укреплению связей между его участниками.

На основе анализа существующих социальных сетей было выявлено, что первостепенную роль в реализации играет модель пользователя социальной сети. Была предложена модель, в основе которой лежат первичный и вторичный идентификаторы, в качестве которых выступили логин и почта, последняя в последующих версиях должна замениться на внутриуниверситетский идентификатор. Так же в модели пользователя есть пароль для дальнейшей аутентификации и авторизации в социальной сети. Пароли, ради сохранности данных, записываются в виде хэша. Так же в модель пользователя были добавлены дополнительные поля – имя, фамилия, факультет, курс и интересы.

При реализации раздела «Новости» было принято решение о том, что без исключения все пользователи сети могут их создавать, комментировать и ставить реакции на уже опубликованные записи.

Также было принято решение о создании отдельного раздела «Вопросы», чтобы не загромождать разделы «Новости» и «События» вопросами от пользователей, а оставить указанные разделы именно для того, для чего они предназначены.

Сеть «Найди друга» разработана на основе фреймворка Django, представляющего собой мощный инструмент для создания веб-приложений на языке программирования Python. Django — это фреймворк, который предоставляет разработчикам набор готовых инструментов и функций для упрощения процесса создания сайтов и приложений, работающих в веб-браузере. Он обеспечивает высокую производительность, удобство использования и расширяемость, что делает его идеальным выбором для разработки приложения, ориентированного на социальную адаптацию студентов.

В архитектуре Django применяется модульная система приложений, в которой каждое приложение состоит из нескольких модулей, отвечающих за определенный функционал. Такой подход позволяет разбивать приложение на независимые компоненты - модули, каждый из которых выполняет определенную функцию и имеет свою логику и интерфейс взаимодействия с другими модулями.

Вышеупомянутая многомодульная архитектура обладает следующими преимуществами:

1. Удобная разработка в команде: модульная архитектура позволяет разработчикам работать над модулями независимо друг от друга, что значительно упрощает командную работу и увеличивает эффективность процесса разработки.
2. Возможность повторного использования кода: программный код, написанный для одного модуля, может быть легко использован в другом, что сокращает время разработки и повышает его качество.
3. Усовершенствованная отладка и тестирование: возможность отдельного тестирования и отладки модулей облегчает процесс разработки, позволяя выявлять и устранять ошибки на ранних этапах, что в конечном итоге способствует повышению качества и надежности приложения.

4. Лучшая масштабируемость: модульная архитектура делает приложение более гибким и масштабируемым, облегчая добавление новых функций и модулей в процессе его дальнейшей разработки.

Архитектура Django соответствует структуре MVT, обеспечивая четкое разделение ответственностей между компонентами приложения, облегчая его разработку, поддержку и масштабирование. [2]

«М» аббревиатуры MVT означает model (модели) — это объекты Python, которые используют приложения Django для доступа к данным и управления ими. Модели определяют внутреннюю структуру хранимых данных. Создание моделей не зависит от того, какая база данных используется. Более того, можно использовать любую базу данных (в социальной сети «Найди друга» используется SQL Lite). Модель избавляет разработчиков приложений от необходимости «прямого» обращения к базе данных - достаточно описать структуру модели на языке программирования, и Django берет на себя работу по взаимодействию с базой данных.

«V» аббревиатуры MVT означает views — это функция Python, которая принимает веб-запрос и выдает веб-ответ. Ответом в представлениях Django в нашем приложении могут быть:

- HTML веб-страницы
- перенаправления
- страницы ошибок
- изображения

«Т» аббревиатуры MVT означает templates - эта часть архитектуры приложения содержит статическое содержимое проекта Django, такое как Html, CSS и Javascript, наряду с изображениями, используемыми в проекте.

Заключение

Социальная сеть «Найди друга» — это инструмент, который способствует формированию поддерживающего и дружественного университетского сообщества, отражая идею единства и взаимопомощи. Прделанная работа по разработке этого приложения имеет глубокий смысл и важное значение для студентов. Главная цель разработанной сети — это помочь студентам расширить свой круг общения, найти новых друзей и единомышленников, которые будут поддерживать их в учебе и повседневной жизни.

Создание такой социальной сети открывает перед студентами новые возможности для социальной адаптации и взаимодействия - она будет облегчать процесс знакомства, помогать вести активное участие в университетской жизни. Благодаря разнообразным функциям и модулям приложения, студенты могут не только находить друзей, но и организовывать совместные мероприятия, обсуждать учебные вопросы, задавать вопросы и делиться опытом.

Список литературы

1. Любякин А.А., Оконечникова Л. В ИССЛЕДОВАНИЕ ОДИНОЧЕСТВА У СТУДЕНТОВ // ПЕДАГОГИЧЕСКОЕ ОБРАЗОВАНИЕ В РОССИИ. 2016 № 2. - 2016. - №2. - С. 149-156. DOI: 10.26170/po16-02-22 EDN: VTLDVT
2. Григорьев Е.А. СРАВНЕНИЕ ФУНКЦИОНАЛЬНЫХ ВОЗМОЖНОСТЕЙ И СТРУКТУРЫ ФРЕЙМВОРКОВ DJANGO И ASP.NET MVC, РЕАЛИЗУЮЩИХ ПАТТЕРН ПРОГРАММИРОВАНИЯ MVC // Форум молодых ученых. 2018. №6-1 (22). URL: <https://cyberleninka.ru/article/n/sravnenie-funktsionalnyh-vozmozhnostey-i-struktury-freymvorkov-django-i-asp-net-mvc-realizuyuschih-pattern-programmirovaniya-mvc> (дата обращения: 10.04.2024).

DEVELOPMENT OF THE SOCIAL NETWORK «FIND A FRIEND»

S.V. Bryzgalov, P.V. Zhdanov, V.D. Kotegova, M.A. Kryzhanovsky, E.D. Lyadov, K.L. Potorochina, E.Yu. Nikitina

Perm State University

Abstract. In this article, the authors examined the problems that arise during the adaptation of students at the university. Based on the analysis of the current situation, a tool was proposed for creating a unified university community. Special attention is paid to finding like-minded people. In conclusion, it is concluded that such a tool is important.

Keywords: *social network, social connections, learning environment, social adaptation of students, university.*

САМООБУЧАЮЩИЙСЯ СЛОВАРЬ НА ОСНОВЕ БОЛЬШИХ ЯЗЫКОВЫХ МОДЕЛЕЙ

Д.П. Гурьянов, А.Н. Рабчевский

Пермский государственный национальный исследовательский университет

Аннотация. В статье рассматривается разработка самообучающегося терминологического словаря на основе больших языковых моделей (LLM). Описаны ограничения классических методов извлечения ключевых слов при работе с неструктурированными текстами социальных сетей и специализированной лексикой. Описана архитектура веб-приложения, объединяющая модули автоматического сбора данных из открытых источников (Google, ВКонтакте, YouTube, Telegram) и модули анализа текста с использованием моделей Gemini 3 Flash, Claude Haiku 4.5, GPT-4.1 и Llama-2-13B. Показано, что применение LLM обеспечивает высокую точность извлечения терминов и именованных сущностей, поддержку многоязычного контента и гибкую настройку без переобучения. Рассмотрены перспективные направления применения инструмента.

Ключевые слова: *большие языковые модели, LLM, самообучающийся словарь, извлечение ключевых слов, именованные сущности, обработка естественного языка, NLP, информационная безопасность, мониторинг киберугроз, веб-приложение.*

Введение

В условиях стремительного развития цифровых технологий обеспечение информационной безопасности становится одной из приоритетных задач как для государственных структур, так и для частного бизнеса. Эффективный мониторинг киберугроз требует непрерывного анализа огромных массивов текстовых данных: публикаций в социальных сетях, новостных статей, форумов, технических блогов и т.д. Ключевым инструментом такого анализа служат терминологические словари – структурированные базы данных, содержащие актуальную специализированную лексику.

Проблема классических подходов

Классические подходы к формированию терминологических баз данных предполагают ручную работу экспертов: специалисты отбирают термины, формулируют определения и актуализируют коллекции – такой процесс трудоемок, медленен и плохо масштабируется в условиях информационного взрыва. Традиционные методы извлечения ключевых слов – статистические (TF-IDF [1]), графовые (TextRank [2], RaKUn [3]) и иные алгоритмические подходы демонстрируют посредственную эффективность при работе с узкоспециализированными текстами и неформальной лексикой социальных сетей.

Отдельную сложность представляют многоязычные тексты, жаргон различных сообществ и гибридные конструкции (например, транслитерированные

термины). Ни один из существующих алгоритмических методов не обеспечивает достаточной точности и полноты при их обработке без значительной ручной доработки. Это и определяет необходимость перехода к качественно иному подходу – использованию больших языковых моделей.

Решение на основе больших языковых моделей

Самообучающийся словарь представляет собой веб-приложение, которое автоматически собирает тексты из интернета, извлекает из них ключевые слова и сущности с помощью ряда больших языковых моделей, а затем сохраняет полученные данные в структурированный словарь формата JSON. Пользователь в любой момент может просматривать, редактировать и дополнять содержание словаря при помощи веб-интерфейса.

Архитектура системы включает несколько функциональных модулей: модули сбора данных обеспечивают интеграцию с поисковой системой Google, социальной сетью ВКонтакте, мессенджером Telegram и видеоплатформой YouTube. По заданным ключевым словам, или ссылкам система автоматически извлекает тексты публикаций, постов и комментариев, после чего собранный корпус данных передается в модули языковых моделей, где происходит анализ: выделение терминов, именованных сущностей (т.е. организаций, персон, технологий, географических объектов и т.д.) и других лексических единиц, относящихся к заданной тематике.

Непосредственно для анализа текстов в систему интегрированы 4 языковые модели: Gemini 3 Flash (Google) [4], Claude Haiku 4.5 (Anthropic) [5], GPT-4.1 (OpenAI) [6]. Каждая из них обладает собственными характеристиками: объемом контекстного окна, скоростью работы и доступностью. Возможность выбора модели позволяет адаптировать систему под конкретные задачи и ресурсные ограничения.

В результате одними из ключевых преимуществ самообучающегося словаря стали высокая точность извлечения терминов даже из неструктурированных и зашумленных текстов социальных сетей, способность работать с многоязычным контекстом и жаргонными выражениями, возможность настройки поведения модели через специализированные системные промпты без переобучения.

Практическое применение

Область применения самообучающегося словаря не ограничивается информационной безопасностью. Любая предметная область, в которой терминология быстро эволюционирует, может извлечь выгоду из подобного инструмента. Среди наиболее перспективных направлений хочется выделить несколько.

Аналитика киберугроз: автоматическое отслеживание новых типов атак, уязвимостей, названий вредоносного ПО и хакерских групп, упоминаемых в открытых источниках. Медиа-аналитика и маркетинговые исследования: мониторинг трендов, брендов и личностей в социальных сетях в режиме реального времени.

Перспективы развития

Разработанный MVP-продукт является основанием для создания более мощной платформы. Среди приоритетных направлений развития – расширение списка источников (Яндекс, X, MAX), интеграция дополнительных локальных open-source моделей с широкими контекстными окнами, предоставление пользователю возможности кастомизировать промпты и параметры обработки.

Особое внимание хочется уделить перспективе интеграции локальных языковых моделей. В отличие от облачных решений, локальные модели, как правило, не подвержены ограничениям цензурирования и не зависят от сторонних API, что критически важно при работе с чувствительными данными в сфере безопасности.

Список литературы

1. Papagiannopoulou E., Tsoumakas G. A Review of Keyphrase Extraction [Электронный ресурс] URL: <https://arxiv.org/abs/1905.05044> (дата обращения: 27.02.2026)
2. Shrivastava I. Exploring Different Keyword Extractors – Graph Based Approaches [Электронный ресурс] URL: <https://medium.com/gumgum-tech/exploring-different-keyword-extractors-graph-based-approaches-c46ec6c12c34> (дата обращения: 27.02.2026)
3. Škrlj B., Repar A., Pollak S. RaKUn: Rank-based Keyword extraction via Unsupervised learning and Meta vertex aggregation [Электронный ресурс] URL: <https://arxiv.org/abs/1907.06458> (дата обращения: 27.02.2026)
4. Google DeepMind Models. Gemini 3 Flash [Электронный ресурс] URL: <https://deepmind.google/models/gemini/flash/> (дата обращения: 27.02.2026)
5. Anthropic Claude. Claude Haiku 4.5 [Электронный ресурс] URL: <https://www.anthropic.com/claude/haiku> (дата обращения: 27.02.2026)
6. OpenAI Developers Models. GPT-4.1 [Электронный ресурс] URL: <https://developers.openai.com/api/docs/models/gpt-4.1> (дата обращения: 27.02.2026)

SELF-LEARNING DICTIONARY BASED ON LARGE LANGUAGE MODELS

D.P. Guryanov, A.N. Rabchevsky

Perm State University

Abstract. This article examines the development of a self-learning terminological dictionary based on large language models (LLMs). The limitations of classical keyword extraction methods when applied to unstructured social media texts and specialized vocabulary are discussed. A web application architecture is proposed that combines modules for automated data collection from open sources (Google, VKontakte, YouTube, Telegram) with text analysis modules powered by Gemini 3 Flash, Claude Haiku 4.5, GPT-4.1, and Llama-2-13B. It is demonstrated that the use of LLMs provides high accuracy in extracting terms and named entities, supports multilingual content, and enables flexible configuration without model retraining. Promising application areas are outlined.

Keywords: *large language models, LLMs, self-learning dictionary, keyword extraction, named entity recognition, natural language processing, NLP, information security, cyber threat monitoring, web application.*

ИМИТАЦИОННОЕ МОДЕЛИРОВАНИЕ ПРОЦЕССА РАСПРОСТРАНЕНИЯ ИНФОРМАЦИИ В СОЦИАЛЬНЫХ СЕТЯХ

П.В. Жданов, А.Н. Рабчевский

Пермский государственный национальный исследовательский университет

Аннотация. В статье рассматривается разработка и валидация детерминированной модели имитационного моделирования процесса распространения информации в социальной сети «ВКонтакте» в контексте информационных атак. Проведён анализ существующих моделей, выявлены их ограничения. Предложены две модели распространения информации, основанные на индивидуальных параметрах пользователей: уровне влияния и уровне внушаемости. Разработана программа, обеспечивающая моделирование на реальных данных. Проведена валидация модели на основе информационного повода «Дворец Путина». Показано, что модель, основанная на общем уровне влияния пользователя, демонстрирует более высокую степень соответствия реальному процессу распространения информации.

Ключевые слова: *имитационное моделирование, информационная атака, уровень влияния, распространение информации, потенциал влияния, социальная сеть, пользователь.*

Введение

Согласно Федеральному закону от 27.07.2006 N 149-ФЗ “Об информации, информационных технологиях и о защите информации”, распространение информации определяется как действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц [1]. В социальных сетях данный процесс приобретает массовый и ускоренный характер, что делает его ключевым элементом как легитимных информационных кампаний, так и деструктивных информационных атак.

Информационные атаки рассматриваются как спланированное, целенаправленное, массированное информационное воздействие на адресата, результатом которого будет формирование запрограммированного общественного мнения и поведения [2]. Одним из способов понимания особенностей информационных атак и борьбы с ними является имитационное моделирование процесса распространения информации в социальных сетях – это метод исследования, при котором изучаемая система заменяется моделью, с достаточной точностью описывающей реальную систему, с которой проводятся эксперименты с целью получения информации об этой системе [3].

Актуальность работы обусловлена совокупностью взаимосвязанных факторов. Во-первых, в настоящее время противостояние между государствами и негосударственными акторами всё чаще перемещается из физического пространства в информационное [4]. Во-вторых, информационные операции зна-

чительно учащаются и увеличиваются в масштабе. За последние два с половиной года было совершено девять крупных информационных операций против Российской Федерации [5]. В-третьих, было доказано, что в социальных сообществах есть два типа структур: большая и слабо-связная сеть пользователей, а также её ядро – более маленькая и сильно-связная подсеть [6]. Считается, что информация, попав к любому пользователю из ядра сети – сразу быстро распространится на всё ядро, а затем попадёт и в периферию. Также ядро пользователей является постоянным числом в каждой сети пользователей [7]. Таким образом, знание структуры и состава ядра сети позволяет перейти от пассивного наблюдения к активному превентивному противодействию информационным атакам. Для решения задачи выявления и анализа ядер необходима разработка инструментов имитационного моделирования процесса распространения информации.

Анализ существующих моделей для имитационного моделирования

Наиболее часто используемым подходом в имитационном моделировании является использование эпидемиологических моделей, в частности модели SI и SIR. В них пользователь сети в любой момент времени может находиться только в одном из нескольких заданных состояний – восприимчивый, зараженный, а также выздоровевший в случае SIR модели (невозможность заразиться снова). Передача “вируса” осуществляется с заданной вероятностью. Такие модели просты в исполнении и модель SIR хорошо отражает динамику распространения информации, что подтверждено исследованием Болотина В.А. о прогнозировании роста числа подписчиков сообществ [8], а также эта модель была использована в статье [9] для описания процесса распространения информации в “Twitter”, но эти модели обладают недостатком — вероятностным подходом, кроме того, в ней не учитываются индивидуальные параметры пользователей.

Также используется модель Далея-Кендалла, то есть модель слухов, которая учитывает отношение пользователей к распространяемой информации [10], однако её практическая реализация требует данных о субъективных характеристиках пользователей, которые невозможно получить при анализе информационных атак.

Системы моделирования, такие как AnyLogic, позволяют работать со случайными графами или агентными моделями, однако не обеспечивают: точного задания реальной социальной сети, учёта индивидуальных параметров пользователей и масштабирования под десятки тысяч пользователей в бесплатных версиях.

Таким образом, существующие решения либо имеют в своей основе вероятностный подход, либо не ориентированы на работу с реальными сетевыми данными.

Разработка модели распространения информации

В результате анализа существующих подходов к моделированию процесса распространения информации в социальных сетях были выделены основные требования к разрабатываемой модели: наличие дискретных состояний пользо-

вателей (сохранение логики SIR-модели); учёт индивидуальных характеристик узлов и их связей; детерминированность результата при фиксированных входных данных; интерпретируемость вклада каждого узла.

В разработанной модели каждый пользователь может находиться в одном из трёх состояний: не обладающий информацией, распространяющий информацию, завершивший распространение (после попытки передачи информации). Передача информации реализуется по пороговому принципу, то есть при превышении произведения характеристик пользователей над заданным порогом. Такой подход обеспечивает детерминированность процесса моделирования.

В первой модели характеристикой источника служит потенциальный уровень влияния (ПУВ), то есть произведение количества друзей пользователя и числа публикаций по теме информационного повода. Характеристикой приемника служит внушаемость пользователя, то есть линейная комбинация числа отметок «Мне нравится» и комментариев, оставленных пользователем в профиле источника. Их произведение сравнивается с пороговым значением.

При этом, согласно статье [11], реализация потенциала влияния пользователя не зависит напрямую от самого значения ПУВ, от количества друзей или количества постов, так как каждый пользователь по-разному реализует свой потенциал. Поэтому была разработана вторая модель, в которой используется не потенциальный, а общий уровень влияния, основанный на суммарной реакции пользователей.

Программная реализация и валидация имитационного моделирования

Для разработки программы, реализующей имитационное моделирование, разработанная модель была взята как основа алгоритма.

Программа состоит из нескольких модулей, первый модуль собирает данные об участниках информационной атаки используя API “ВКонтакте” для получения информации о реакциях на публикации и списки друзей пользователей. Исходными данными для моделирования распространения информации в сети пользователей являются данные об их связях, их уровни влияния (потенциальные или общие) и уровни внушаемости, а также список начальных источников информации.

Далее, в модуле имитационного моделирования, каждый источник информации передает её дальше всем узлам-соседям (друзьям) при условии того, что комбинация уровня влияния узла и уровня внушаемости узла-соседа выше заданного порогового значения.

Валидация разработанной модели проведена на основе предоставленных материалов по информационному поводу «Дворец Путина». Сравнение результатов моделирования данного информационного повода с реальными данными показало, что модель с общим уровнем влияния воспроизводит процесс распространения информации наиболее точно, отклоняясь к середине процесса моделирования от реальных данных не более чем на 2 процента, при минимальном отклонении в 0.3% от количества реальных участников информационной атаки. С точки зрения качественного анализа, список пользователей, полученный при моделировании, на 97% совпадает со списком реальных участников информа-

ционного повода. Можно сделать вывод, что модель действительно правильно отражает динамику данного процесса и может использоваться для прогнозирования информационных атак в данной социальной сети.

Заключение

Нами была разработана детерминированная модель имитационного моделирования распространения информации в социальной сети «ВКонтакте», ориентированная на анализ информационных атак. Актуальность выбранной темы обусловлена ростом масштабов и интенсивности информационного противостояния, а также необходимостью перехода от реактивных мер противодействия деструктивному информационному воздействию к проактивным и превентивным подходам, основанным на анализе структуры социальных сетей и поведения их участников. В отличие от существующих вероятностных моделей, предложенный подход учитывает индивидуальные параметры пользователей и структуру реальной социальной сети, обеспечивая воспроизводимость и интерпретируемость результатов.

Эмпирическая валидация показала, что модель, основанная на общем уровне влияния пользователя, более адекватно отражает реальные механизмы распространения информации по сравнению с моделью потенциального влияния.

Практическая значимость исследования заключается в возможности использования разработанного инструмента для выявления наиболее опасных узлов сети, оценки потенциального охвата информационных атак и поддержки принятия решений в сфере информационной безопасности. Перспективы дальнейших исследований связаны с расширением набора индивидуальных параметров пользователей и адаптацией модели к межплатформенному распространению информации.

Список литературы

1. Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 24.06.2025) "Об информации, информационных технологиях и о защите информации" (с изм. и доп., вступ. в силу с 01.09.2025) // СПС «КонсультантПлюс».
2. Коцюбинская Любовь Вячеславовна Информационная атака: понятие и онтологические свойства // Политическая лингвистика. 2017. №6. URL: <https://cyberleninka.ru/article/n/informatsionnaya-ataka-ponyatie-i-ontologicheskie-svoystva> (дата обращения: 27.11.2025).
3. Имитационное моделирование // Википедия URL: https://ru.wikipedia.org/wiki/%D0%98%D0%BC%D0%B8%D1%82%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%BE%D0%B5_%D0%BC%D0%BE%D0%B4%D0%B5%D0%BB%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5 (дата обращения: 17.11.2025).
4. Моделирование противодействия деструктивному влиянию в социальных сетях / В. А. Минаев, М. П. Сычев, Л. С. Куликов, Е. В. Вайц // Моделирование, оптимизация и информационные технологии. – 2019. – Т. 7, № 1(24). – С. 511-520. – DOI 10.26102/2310-6018/2019.24.1.004. – EDN VHMNPA.

5. Информационная война, связанная со вторжением России на Украину // Википедия URL:
https://ru.wikipedia.org/wiki/%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%B2%D0%BE%D0%B9%D0%BD%D0%B0,_%D1%81%D0%B2%D1%8F%D0%B7%D0%B0%D0%BD%D0%BD%D0%B0%D1%8F_%D1%81%D0%BE_%D0%B2%D1%82%D0%BE%D1%80%D0%B6%D0%B5%D0%BD%D0%B8%D0%B5%D0%BC_%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D0%B8_%D0%BD%D0%B0_%D0%A3%D0%BA%D1%80%D0%B0%D0%B8%D0%BD%D1%83 (дата обращения: 22.11.2025).
6. Dover Y., Kelman G. Centralized nucleation in online networks leads to high social inequality. *Appl Netw Sci* 3, 43 (2018). DOI: 10.1007/s41109-018-0102-3 EDN: OGIRXE
7. X. Palla G., Barabási A.-L., Vicsek T. Quantifying social group evolution // *Nature*. 2007. Vol. 446. P. 664–667.
8. Разработка модели распространения новостей в социальных сетях на основе SIR- модели эпидемии // Высшая школа экономики URL:
<https://www.hse.ru/edu/vkr/219505170> (дата обращения: 19.11.2025).
9. Fei Xiong, Yun Liu, Zhen-jiang Zhang, Jiang Zhu, Ying Zhang An information diffusion model based on retweeting mechanism for online social media // *Physics Letters A*. - 2012. - №376, Issues 30–31. - С. 2103-2108.
10. Горковенко Д. К. Обзор моделей распространения информации в социальных сетях / Д. К. Горковенко. — Текст: непосредственный // Молодой ученый. — 2017. — № 8 (142). — С. 23-28. — URL:
<https://moluch.ru/archive/142/39946>. EDN: XXKAUN
11. Жданов П.В., Мустакимова Я.Р., Рабчевский А.Н. ИССЛЕДОВАНИЕ РЕАЛИЗАЦИИ ПОТЕНЦИАЛА НАИБОЛЕЕ ВЛИЯТЕЛЬНЫХ ПОЛЬЗОВАТЕЛЕЙ // АКТУАЛЬНЫЕ ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. - Пермь: Пермский государственный национальный исследовательский университет, 2024. - С. 10-18.

SIMULATION OF THE PROCESS OF INFORMATION DISTRIBUTION IN SOCIAL NETWORKS

P.V. Zhdanov, A.N. Rabchevsky

Perm State University

Abstract. The article discusses the development and validation of a deterministic model of imitation modeling of the process of disseminating information on the VKontakte social network in the context of information attacks. Analysis of existing models was carried out, their limitations were identified. Two models of information dissemination are proposed, based on individual user parameters: the level of influence and the level of suggestibility. A program has been developed that provides modeling on real data. The model was validated on the basis of the information occasion "Putin's Palace." It is shown that the model based on the general level of user influence demonstrates a higher degree of compliance with the real process of information dissemination.

Keywords: *simulation, information attack, influence level, information dissemination, influence potential, social network, user.*

ИССЛЕДОВАНИЕ СТАТИСТИКИ ИНФОРМАЦИОННЫХ АТАК

Я.Р. Мустакимова, А.Н. Рабчевский

Пермский государственный национальный исследовательский университет

Аннотация. В статье описана методика раннего обнаружения информационных атак в социальных сетях. В отличие от существующих подходов, которые фиксируют угрозу с запозданием, предложенный метод позволяет выявлять информационные атаки на начальных стадиях на основе трех критериев: одновременной публикации четких и нечетких дубликатов текстов, присутствия ботов и наличия независимых каналов вброса информации. По результатам анализа шести информационных поводов установлены пороговые значения, которые могут быть использованы для автоматического детектирования атаки.

Ключевые слова: *информационная атака, раннее обнаружение информационных атак, социальные сети, боты, дубликаты сообщений, независимые каналы вброса.*

Введение

В современном мире всё чаще говорят об информационных атаках, и это не случайно. Сегодня, чтобы победить противника, не обязательно применять оружие — достаточно получить информационное преимущество. В условиях тотальной цифровизации и проникновения сетевых технологий во все сферы общественной жизни информационные атаки приобретают способность поражать критически важные инфраструктуры, включая энергосистемы, финансовые институты и органы государственного управления. Но самое опасное направление таких атак — это воздействие на сознание людей. Когда человек теряет способность критически мыслить и отличать достоверные сведения от ложных, он становится уязвимым для любых идеологических внушений. В конечном счете это ведет к разрушению механизмов общественной самоорганизации, что делает государство беззащитным перед внешним управлением. Поэтому особую значимость на сегодняшний день приобретает как изучение феномена информационных атак, так и разработка эффективных систем их обнаружения и нейтрализации.

Под информационной атакой понимается спланированное, массированное информационное воздействие на объекты с целью формирования общественного мнения и поведения в соответствии с задачами организаторов атаки. Объектами воздействия информационных атак являются как общество в целом (гражданское население, его социальные группы), так и его государственные, экономические и социальные институты [1]. Информационные атаки являются частью информационных операций, которые в свою очередь являются частью информационной войны. Основное отличие между этими понятиями состоит в их масштабе. Информационная война — это широкомасштабное и долгосроч-

ное стратегическое противоборство государств, она может длиться годами. Информационная операция — тактическая кампания в рамках такой войны, направленная на достижение конкретной цели. А информационная атака — это единичное, точечное воздействие.

Система автоматического выявления информационных атак

Для проведения информационных атак сегодня всё больше используются социальные сети. Благодаря огромному охвату аудитории социальные сети становятся идеальным каналом для быстрого распространения информации между людьми. Алгоритмы платформ устроены так, что любой эмоционально заряженный контент распространяется вирусно, даже если он ложный. Кроме того, в социальных сетях легко создавать фейковые аккаунты и сети ботов, которые могут имитировать массовую поддержку или возмущение. Таргетированная реклама позволяет нацеливаться на конкретные группы людей с наиболее уязвимыми точками восприятия. А из-за того, что модерационные службы часто не успевают за вирусным распространением контента, ложная информация успевает прочно осесть в сознании людей еще до появления каких-либо опровержений.

На сегодняшний день сложилось два основных подхода к выявлению информационных атак. Первый основан на подсчете сообщений: если их количество за определенное время превышает норму, фиксируется атака. Второй подход сравнивает реальный график публикаций с типовым шаблоном [2]. Общая проблема этих методов заключается в том, что они работают с опозданием, так как требуют накопления данных. К моменту, когда будет зафиксировано превышение пороговых значений, деструктивный контент уже успеют посмотреть миллионы пользователей. Это заставляет защищающуюся сторону всегда находиться в роли догоняющего, тратя ресурсы не на предотвращение, а на ликвидацию уже нанесенного ущерба. Мы же предлагаем методику раннего выявления информационных атак. Ведь если обнаруживать информационные атаки на ранних стадиях, у государства появится возможность реагировать на репутационные угрозы и волны дезинформации в тот момент, когда они только начинают распространяться. Это позволит принимать меры еще до того, как ложные сведения успеют охватить широкую аудиторию и закрепиться в общественном сознании.

Наша система нацелена на выявление информационных атак в социальных сетях, а именно в социальной сети ВКонтакте. В нашей системе мы будем определять информационные атаки по следующим признакам: наличие ботов, наличие независимых каналов вброса информации и использование четких и нечетких дубликатов текста. Мы считаем, что именно эти признаки позволят нам выявить информационные атаки на ранних стадиях, т.е. в первые часы. Потому что если не связанные между собой пользователи начнут почти одновременно публиковать схожие посты, то это может говорить о проведении информационной атаки. А если большинство этих пользователей окажутся еще и ботами, то тут можно говорить о какой-то специально заранее спланированной деятельности. К тому же эти признаки можно отследить уже на начальной ста-

дии, когда атака только начинается. Рассмотрим каждый из перечисленных признаков подробнее:

1) Использование ботов. Бот – это специально созданный аккаунт, замаскированный под обычного пользователя. Бот действует полностью автономно: он либо запускается в ответ на определенные события в режиме реального времени, либо активируется по заранее установленному расписанию для выполнения заданных операций. Для выявления ботов мы используем нейронные сети. В социальной сети ВКонтакте есть два вида профилей пользователей – открытые и закрытые. У открытых профилей доступно больше данных для анализа, чем у закрытых. В связи с этим были созданы две разные нейросетевые модели – для поиска ботов среди открытых профилей и для поиска ботов среди закрытых профилей. Обе нейронные сети представляют собой многослойный персептрон с одним скрытым слоем и одним выходным нейроном, который дает нам число от 0 до 1, которое обозначает вероятность того, что данный аккаунт – бот.

2) Распространение четких и нечетких дубликатов сообщений. Четкий дубликат – это точная копия исходного текста, а нечеткий дубликат – исходный текст с некоторыми изменениями. Для получения нечеткого дубликата можно поменять слова местами, заменить некоторые слова на синонимы, добавить дополнительные предлоги или союзы. При этом исходный смысл текста останется неизменным. Для поиска четких и нечетких дубликатов используется кластеризация текстов. Сначала проводится векторизация с помощью SentenceTransformer('distiluse-base-multilingual-cased-v1') [3] – это процесс преобразования текстовых предложений в числовые векторы с использованием специальной модели. А затем с помощью DBSCAN [4] проводится кластеризация.

3) Использование независимых каналов вброса информации. Под независимыми каналами понимаются каналы, между которыми нет связей. Отсутствие связей между авторами постов указывает на целенаправленный, организованный вброс целевого контента. Потому что вряд ли не связанные между собой люди будут одновременно публиковать одинаковые сообщения. Для поиска связей между пользователями используется VK API [5], а конкретно метод friends.get, который позволяет получить список друзей по ID пользователя.

Ключевая задача при создании системы — определение пороговых значений, на основании которых будет приниматься решение о факте проведения информационной атаки. Необходимо перейти от эмпирических, экспертных оценок к статистически обоснованным критериям. Для этого необходимо проанализировать уже прошедшие информационные атаки, выделить количественные характеристики исследуемых признаков (наличие ботов, связей, дубликатов) и на их основе определить пороговые значения, превышение которых будет указывать на атаку.

Анализ информационных атак

Для анализа были выбраны следующие инфоповоды: Жыве Беларусь, Арест Ивана Голунова, Дворец Путина, Арест Алексея Навального* (Внесен в

перечень террористов и экстремистов Росфинмониторинга), Частичная мобилизация, Арест Сергея Фургала. Эти инфоповоды связаны с различными протестными акциями. Для анализа были выбраны именно они, потому что эти события вызвали широкий общественный резонанс. Они оказали комплексное влияние на различные сферы общественно-политической жизни, в том числе на общественное мнение и настроение, на институты власти и госуправление, на международные отношения.

По этим инфоповодам с помощью поисковой системы SEUS были собраны коллекции материалов. Поисковая система SEUS – это программный комплекс для поиска, мониторинга и анализа информации в открытом пространстве социальных сетей и мессенджеров [6]. Для каждого события сначала формировался словарь характерных ключевых слов, а затем с помощью поисковой системы собирались посты, опубликованные за интересующий нас промежуток времени. В таблице 1 во втором столбце указано количество постов, которое было собрано по каждому инфоповоду. Далее была проведена кластеризация текстов и были получены группы четких и нечетких дубликатов. При кластеризации часть постов была отнесена к шуму. То есть часть постов сильно отличалась по содержанию от всех остальных, и алгоритм кластеризации не смог отнести эти посты в какую-либо группу и отправил в шум как уникальные выбросы. В таблице 1 приведены минимальные и максимальные значения числа постов в группах. Характерно, что большинство групп оказались малочисленными, тогда как группы с большим объемом постов представлены, как правило, в единственном экземпляре.

Таблица 1

Характеристики инфоповодов

Инфоповод	Кол-во постов в коллекции	Кол-во постов в группах	Кол-во групп	Макс. кол-во постов в группе	Мин. кол-во постов в группе
Живе Беларусь	13031	7315	213	4108	5
Арест Голунова	34503	24019	567	15525	4
Дворец Путина	58644	39158	1106	20085	4
Арест Навального*	88442	58583	1699	35672	3
Частичная мобилизация	68597	43716	1860	16151	4
Арест Фургала	24666	17839	353	12747	5

В результате кластеризации выделились два типа групп: содержащие четкие дубликаты и содержащие нечеткие. Нечеткие дубликаты образуются преимущественно за счет добавления смайликов, изменения заголовков, переста-

новки или удаления слов; использования синонимов не зафиксировано. Доля групп с четкими дубликатами составляет от 13% до 18%, следовательно, основная масса групп относится к категории нечетких дубликатов.

После сортировки всех групп по временной шкале были сформированы информационные треки. Для анализа динамики мы определили моменты их запуска. На рисунке 1 видно, что треки запускаются в различное время.

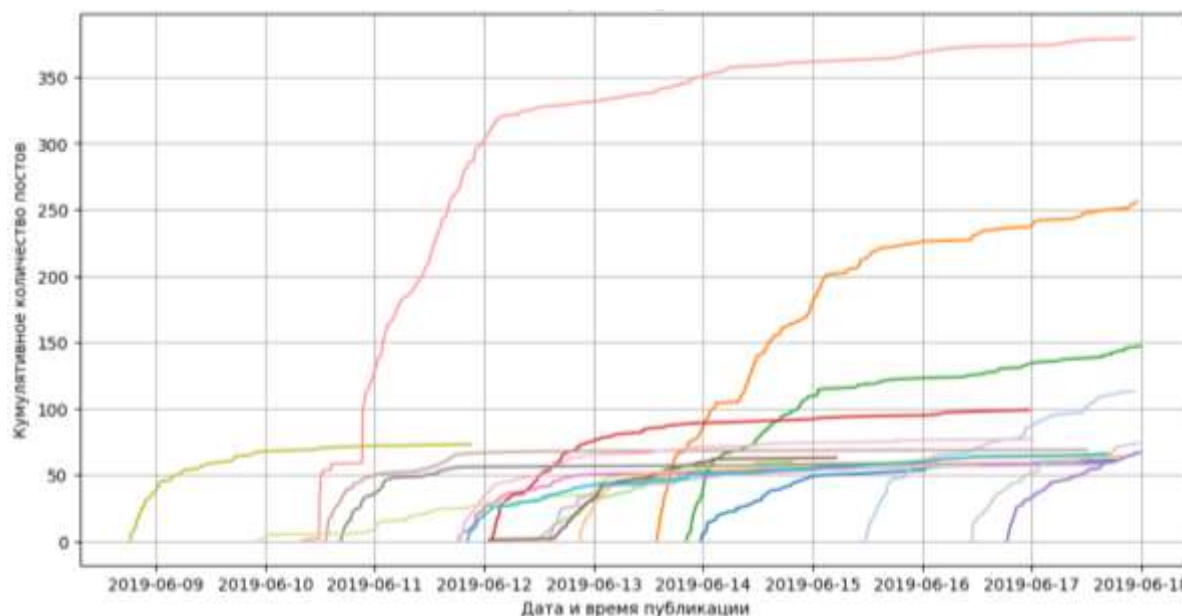


Рис.1. Информационные треки по инфоповоду «Арест Ивана Голунова»

Далее был построен график часового распределения количества запусков треков. Он представлен на рисунке 2. Каждая волна на графике соответствует одному дню: днем количество запускаемых треков увеличивается, ночью – спадает. Ключевая закономерность заключается в том, что амплитуда волн возрастает день ото дня, что свидетельствует о ежедневном увеличении количества новых треков вплоть до пикового значения, после которого следует спад.

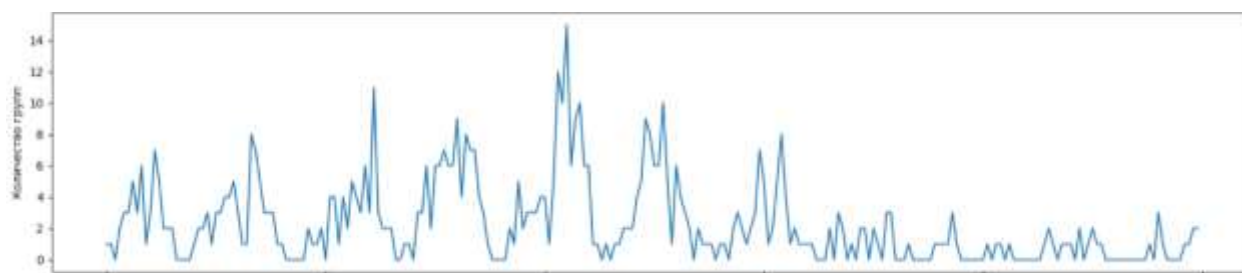


Рис.2. График часового распределения информационных треков по инфоповоду «Арест Ивана Голунова»

Также мы измерили время от начала информационной атаки до её кульминации, что соответствует фазе активного развития информационной атаки. В итоге получилось, что информационная атака развивается несколько дней. Средняя продолжительность фазы развития информационной атаки по исследованным инфоповодам составила 8 дней. Это означает, что есть достаточно

времени для обнаружения информационной атаки и применения соответствующих защитных механизмов.

На рисунке 1 видно, что графики информационных треков различаются по форме. Среди всех графиков можно выделить повторяющиеся шаблоны, которые представлены на рисунке 3. Плавный характер графика без резких скачков свидетельствует о естественном распространении информации. А наличие резкого скачка указывает на одновременную публикацию большого количества однотипных постов, что характерно для информационного вброса.

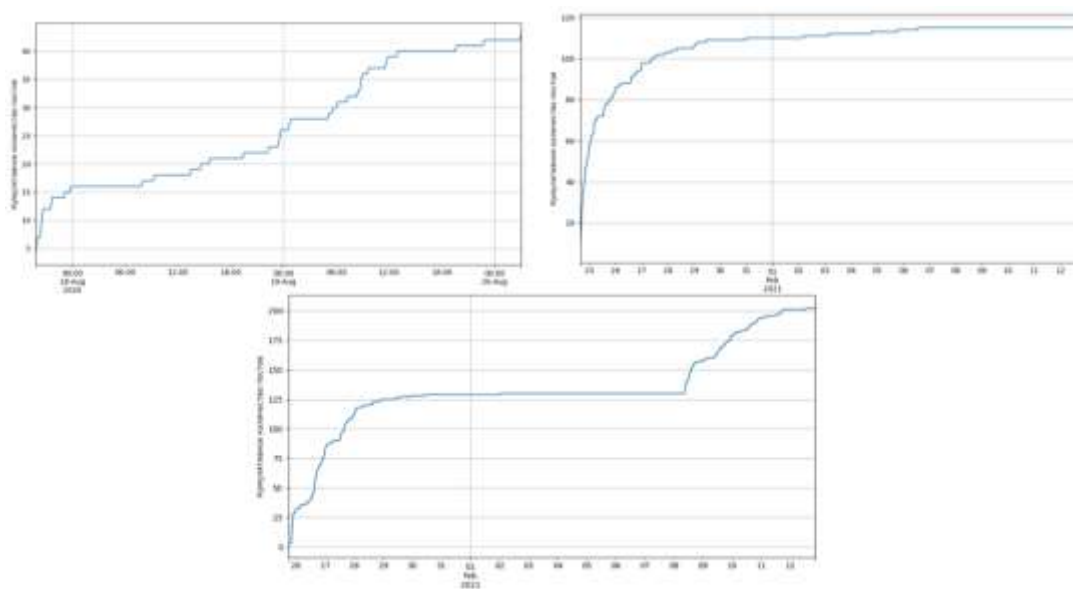


Рис. 3. Типовые шаблоны информационных треков

Также был проведен анализ групп на предмет наличия связей между пользователями, которые публиковали схожий контент. Выяснилось, что в среднем лишь 15% групп демонстрируют такие связи, тогда как остальные 85% их не имеют. Кроме того, мы проверили, являются ли пользователи ботами. Оказалось, что боты присутствуют в 61% групп.

Заключение

В ходе проведенных статистических исследований было обработано шесть инфоповодов, и были выявлены пороговые значения, на основании которых в автоматическом режиме можно принимать решение о факте проведения информационной атаки. Были получены следующие значения: средний объем вброса сообщений (скачок активности) – 5,06 (≈ 5), среднее количество связей в группах со связями – 2, а среднее присутствие ботов в группах с ботами – 3,58 (≈ 4). Эти количественные критерии позволяют перейти от эвристических оценок к более объективным статистически обоснованным методам выявления информационных атак.

Список литературы

1. Коцюбинская Л.В. Информационная атака: понятие и онтологические свойства // Политическая лингвистика. 2017. №6. С. 106-111. EDN: YMJXMA
2. Потемкин А.В. Распознавание информационных операций средств массовой информации сети Интернет // Интернет-журнал «Науковедение». 2015. Т. 7. № 3. С. 1-11. DOI: 10.15862/139TVN315 EDN: UMFXXB
3. Sentence transformers. Distiluse-base-multilingual-cased-v. [Электронный ресурс] URL: <https://huggingface.co/sentence-transformers/distiluse-basemultilingual-cased-v1> (дата обращения: 02.03.2026)
4. DBSCAN. [Электронный ресурс] URL: <https://scikit-learn.org/stable/modules/generated/sklearn.cluster.DBSCAN.html> (дата обращения: 02.03.2026)
5. API ВКонтакте. [Электронный ресурс] URL: <https://dev.vk.com/ru/method> (дата обращения: 02.03.2026)
6. SEUS – поисковая система информации в социальных сетях. Официальная страница сайта компании разработчика ООО «СЕУСЛАБ». [Электронный ресурс] URL: <https://seuslab.ru/seus> (дата обращения 02.03.2026)

RESEARCH OF INFORMATION ATTACK STATISTICS

Y.R. Mustakimova, A.N. Rabchevsky

Perm State University

Abstract. The article describes a technique for early detection of information attacks on social networks. Unlike existing approaches that detect the threat late, the proposed method allows to identify information attacks at the initial stages based on three criteria: the publication of clear and fuzzy duplicate texts, the presence of bots and the presence of independent information distribution channels. Based on the results of the analysis of six information events, thresholds were established that can be used for automatic attack diagnostics.

Keywords: *information attack, early detection of information attacks, social networks, bots, duplicate messages, independent distribution channels.*

РАЗРАБОТКА ВЕБ-ПРИЛОЖЕНИЯ ДЛЯ СОПРОВОЖДЕНИЯ ИНОСТРАННЫХ СТУДЕНТОВ

*В.М. Авдони́на, И.Н. Дорофеев, А.Д. Косберг, А.П. Кузнецов,
О.П. Маринкина, Т.С. Посохина, Е.Ю. Никитина*

Пермский государственный национальный исследовательский университет

Аннотация. Описывается универсальный информационный ресурс, реализованный как веб-приложение со справочной информацией, предназначенный для иностранных студентов. Информация, размещенная в этом ресурсе, поможет студентам в решении типовых проблем, а также в ориентации по студенческому городку ПГНИУ и городу Перми. Приложение создано с использованием инструментов Flutter и имеет клиент-серверную архитектуру.

Ключевые слова: *веб-приложение, гибридное приложение, иностранные студенты, виджет.*

Глобальные информационные сети невозможно полностью контролировать. Публикуемая в глобальной информационной сети информация может быть недостоверной или неподтвержденной. При этом ложная информация или форма её изложения может негативно воздействовать на человека и, в некоторых случаях, стимулировать человека к совершению деструктивных поступков.

Возможно снизить негативное влияние информации из глобальной информационной сети с помощью создания локальных информационных ресурсов.

Целью настоящей работы являлось создание локального информационного ресурса для иностранных студентов. Ресурс должен содержать всю необходимую информацию для комфортного обучения иностранных студентов в ПГНИУ. Необходим качественный выбор контента ресурса, включающий все необходимые сведения о правилах проживании и обучении в университете, возможностях для саморазвития и успешного усвоения новых знаний. Контент должен быть достоверным, актуальным, востребованным иностранными студентами. Приложение должно быть разработано в соответствии с законом РФ «О средствах массовой информации», и будет содержать данные, не входящие в список запрещенных в Российской Федерации.

На текущий момент существуют аналоги разрабатываемого приложения, созданные в различных вузах Российской Федерации для своих иностранных студентов. Краткие сведения о данных приложениях содержатся в таблице 1.

Приложения-аналоги

Название и тип ресурса	Описание
Мобильное приложение «Мой БашГУ»	Приложение является личным кабинетом иностранного студента, может быть использовано как чат (есть функция отправления вопросов), геоинформационная система (подключены карты), справочник по миграционному законодательству, источник новостей. Приложение разрабатывалось на платформе Android Studio. [10, 15]
Мобильное приложение «PreTPU»	Приложение является личным кабинетом иностранного студента, может быть использовано как календарь, источник новостей, источник информации об университете, словарь (в том числе словарь академических терминов). Приложение разрабатывалось на платформе Android Studio. [12]
Веб-ресурс «Помощник иностранного студента»	Ресурс представлен как сайт, может быть использован для электронного документооборота (заказа справок, оформления документов), изучения законодательства, источник новостей. [9]
Мобильное приложение «HSE COMPANION»	Приложение предназначено для моделирования различных ситуаций, в которых может оказаться иностранный студент. Студент знакомится с ситуациями через приложение и проходит их как игру. Концепция приложения очень отличается от поставленной в настоящей работе цели, но идея адаптации в игровой форме интересна. [11]
Веб-ресурс «Иностран- ный студент»	Ресурс представлен как онлайн-платформа для взаимодействия студента со структурными подразделениями университета. Скорее всего, сейчас платформа не работает, так как последние новости по ней опубликованы в 2021 году. [7]
Веб-ресурса «Под- держка иностранных абитуриентов»	Ресурс представлен как сайт, может быть использован как источник новостей, источник информации об университетах РФ, справочная система по законодательству. Ресурс имеет приятный интерфейс, четкий и наглядный. [16]
Мобильное приложение «UrFU Guide»	Приложение помогает в ориентации в университете и общежитиях. В приложении предложен минимальный набор функций, также нет данных о ресурсе, на котором создавалось приложение [5]

Программы-аналоги созданы для конкретных университетов и предоставляют различный выбор функций и возможностей. На идеи программ-аналогов можно ориентироваться при создании нового информационного ресурса. Универсальной разработки, легко адаптируемой под задачи различных университетов, не существует в силу как разнообразия самих вузов, так и потребностей иностранных студентов, обучающихся в этих вузах. Большинство из программ-аналогов созданы как выпускные квалификационные работы, и их программные коды не опубликованы в открытых источниках.

Выбор информационных модулей для ресурса ПГНИУ сделан на основании данных, полученных в процессе анкетирования иностранных студентов, обучающихся в Пермском университете. Анкета была сформирована на английском языке, включает 12 вопросов, в том числе 3 вопроса открытой формы. Все вопросы посвящены проблемам, связанным с адаптацией к жизни и учебе в другой стране у студентов. Результаты анкетирования представлены в таблице 2.

Таблица 2

Данные о результатах анкетирования

Проблемные вопросы для иностранных студентов ПГНИУ	Количество студентов, для которых этот вопрос оказался проблемным
How can I get a SIM card and Wi-Fi connection?	12%
Where can I get medical care? How do I join a hospital?	12%
How can I get to my university and dormitory?	10%
How can I obtain a bank card?	10%
How can I find out the public transport routes and timetables?	10%
What is the dormitory, university, city code of conduct?	8%
Which social networks and messengers are popular and allowed in Russia?	8%
Where are the food shops located?	6%
Where are the hardware stores, clothing stores, stationery stores located?	6%
What laws are in force in Russia?	6%
How do I get legal aid?	6%
How to navigate the university and dormitory?	4%
Where can I get cash from my card or exchange currency?	4%

В перечень информационных материалов для иностранных студентов были включены следующие: ответы на популярные вопросы иностранных студентов, особенности оформления банковской карты, карта университета и города (с геоточками магазинов, общежитий, кафе, аптек), права человека, законы РФ (хорошее знание которых необходимо всем обучающимся, не имеющим гражданства РФ), контакты кураторов иностранных студентов и экстренных служб. [13]

Также были включены материалы, необходимость которых выявлена не в результате анкетирования, а в процессе общения с иностранными студентами: общепринятые правила поведения, культурные места для отдыха, особенности менталитета, праздники, правила обучения.

Перечисленные материалы представлены в создаваемом информационном ресурсе как информационные модули на экране приложения, при нажатии разворачивающиеся в самостоятельные экраны; модули доступны для чтения любым пользователям приложения.

Приложение разработано с учетом с учетом следующих требований:

- должно хорошо работать на любых устройствах: компьютерах, телефонах, планшетах;
- должно запускаться в любой операционной системе: iOS, Android, Windows, Linux;
- можно открыть в браузере или установить на устройство;
- возможность автоматической смены языка. Например, иностранный студент, телефон которого настроен на английский язык, увидит текст в приложении на английском языке.

Перечисленным требованиям соответствуют гибридные приложения (RIA-приложения). Гибридное приложение взаимодействует с нативным, характерным для конкретной операционной системы кодом через специальные фреймворки или контейнеры. Гибридное приложение не только является кросс-платформенным, но и учитывает характеристики устройства, на котором оно работает. При этом в процессе разработки приложения создается только один программный код. Код адаптируется для различных операционных систем через функции платформы разработки приложения. [1,4,6,8,14]

Различия между средствами разработки гибридных приложений приведены в таблице 3 [2,17,18].

Таблица 3

Сравнение средств разработки

Flutter	React Native	Xamarin
Наличие подробной документации		
Да, в том числе есть правила и примеры работы всех инструментов	Да, но документация ориентирована на программистов, хорошо владеющих языком JavaScript	Да, но в документации нет примеров работы функций фреймворка
Поддержка нативного кода старых версий ОС		
Встроенная функция	Возможна, но необходимо подключение дополнительных библиотек к коду	Возможно, но некоторые функции могут быть не доступны.
Безопасность		
Защита от значений NULL (sound null safety). Инструменты периодически тестируются разработчиками на наличие уязвимостей.	Используются небезопасные глубокие ссылки для связи с нативным кодом, на сайте разработчиков фреймворка опубликованы рекомендации по повышению безопасности приложения	Возможно отключение сторонних библиотек, используемых в работе приложения, после прекращения выпуска обновления библиотек.

В качестве программного средства шифрования выбраны инструменты Flutter: высокая производительность, безопасность, поддержка работы приложения для нескольких операционных систем различных версий, а также наличие подробной и удобной документации составляют преимущество инструментов Flutter перед фреймворками.

Веб-приложение построено по модели клиент-сервер (рис.1). Архитектура приложения обладает свойством масштабируемости: можно добавлять новые модули или редактировать информацию в существующих модулях без изменения структуры приложения. Любые изменения — появление нового сообщения, изменения в оформлении информации, дополнительные функции — становятся доступны всем пользователям после изменения информации на сервере. Обновление приложения или загрузки новых версий в этом случае не требуется. [3]

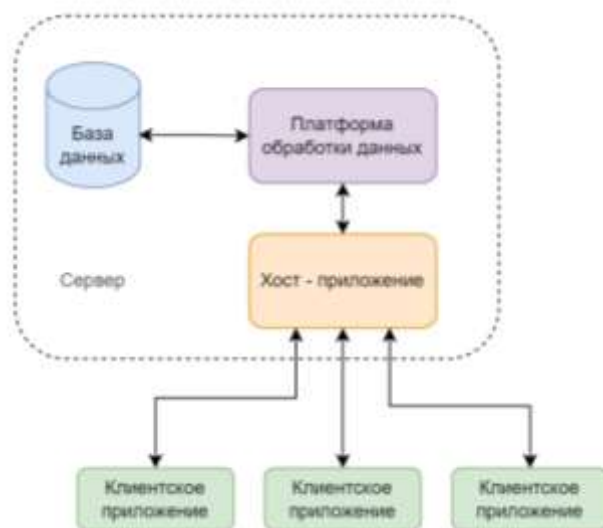


Рис. 1. Архитектура приложения

Работа клиентской части приложения построена по ролевой модели: алгоритм взаимодействия пользователя с приложением (в том числе, количество допустимых действий и функций) изменяется в зависимости от роли пользователя (клиента).

В системе существует три основных роли (рис.2):

- Обычный пользователь (например, иностранный студент): имеет права на чтение информации в приложения, смену языка, добавление геометок на карту города. Назовем перечисленные доступные обычному пользователю функции базовыми.
- Редактор (например, куратор иностранных студентов): имеет права на изменение (редактирование) содержания информационных модулей приложения: он может добавлять, удалять и изменять текстовые и графические материалы, геоточки, новости, события. Назовем перечисленные доступные редактору функции дополнительными.



Рис. 2. Схема взаимодействия пользователей с приложением.

- Администратор (например, системный администратор приложения): имеет полный доступ к приложению, в том числе к серверу и базе данных; может изменить (отредактировать) не только содержание существующих в приложении модулей (как Редактор), но и структуру приложения. Например, только администратор может добавлять или изменять функцию локализации приложения, в том числе подключать к приложению автоматический перевод на новый иностранный язык. Предполагается, что администратор будет поддерживать целостность приложения, доступность приложения обычным пользователям и редакторам. Дополнительно администратор сможет обновлять приложение и добавлять в его структуру новые инструменты.

В качестве базовых функций приложения выбраны следующие функции:

- Работа с картой города: просмотр информации об обозначенных на карте локациях, добавление собственных локаций на карту;
- Изменение языка приложения (выбор варианта из перечня поддерживаемых языков);
- Просмотр информационных модулей;
- Поиск информации через специальную строку поиска.

Для реализации базовых функций использованы библиотеки `Flutter_map`, `Latlong2`, `Page_view_dot_indicator`, `Flutter_localizations.dart`.

Графический интерфейс веб-приложения, написанного с использованием инструментов `flutter`, состоит из виджетов. Виджет является совокупностью графического элемента (в том числе его стилей – цвета, размера, формы) и функций, доступных при работе пользователя с этим элементом. Каждый информационный модуль приложения в программном коде представляет отдельный виджет. Внешний вид некоторых виджетов приведен на рис. 3-7).



Рис. 3. Выбор языка в настройках приложения

Рис. 4. Добавление новой геоточки на карту

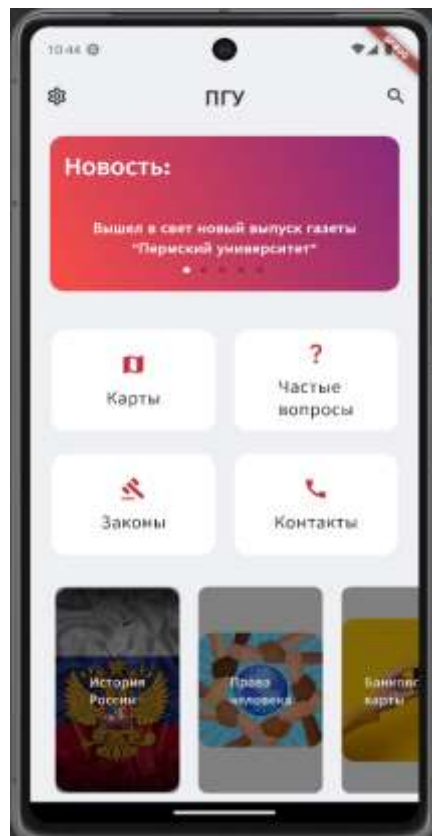


Рис. 5. Домашний экран



Рис. 6. Карты Openstreetmap

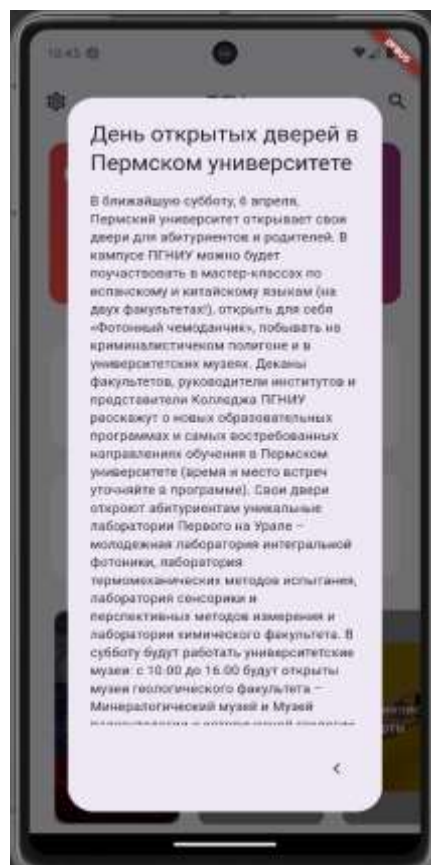


Рис. 7. Раздел новостей

В будущем можно будет легко изменить структуру приложения или просто добавить в него новые функции. Например, можно интегрировать в приложение интерактивные карты университетского городка и форум (форму обратной связи) для общения студентов с кураторами или контактными лицами университета. Взаимодействие с иностранными студентами через приложение (например, через модуль «Новости») улучшит культуру взаимодействия таких студентов с остальными обучающимися и сотрудниками университета. С помощью модулей «Новости» и «События» иностранные студенты будут узнавать о научных и образовательных мероприятиях, и как следствие, станут чаще участвовать в учебной и творческой жизни университета и города.

Список литературы

1. Виды мобильных приложений / Б. Х. Нгуен, Д. Ч. Нгуен, Н. Х. Нгуен [и др.] // Синергия Наук. – 2017. – № 7. – С. 246-253. – EDN: XRNGQJ.
2. Документация по Xamarin - Xamarin | Microsoft Learn URL: <https://learn.microsoft.com/ru-ru/xamarin/>
3. Дубаков А.А. Сетевое программирование: учебное пособие / А.А. Дубаков – СПб: НИУ ИТМО, 2013. – 248 с. EDN: XFXCLW
4. Заяц А. М. Введение в гибридные технологии разработки мобильных приложений: учебное пособие для спо / А. М. Заяц, Н. П. Васильев. — 2-е изд., стер. — Санкт-Петербург: Лань, 2022. — ISBN 978-5-8114-9555-9. — Текст: электронный // Лань: электронно-библиотечная система. — URL:

<https://e.lanbook.com/book/200459> (дата обращения: 11.04.2024). ISBN: 978-5-8114-9555-9

5. Иностранным студентам станет проще ориентироваться в вузе (urfu.ru) URL: <https://urfu.ru/ru/news/30995/> (дата обращения: 28.03.2024)

6. Колчанова Светлана Анатольевна СРАВНЕНИЕ ФРЕЙМВОРКОВ FLUTTER И REACT NATIVE, ИСПОЛЬЗУЕМЫХ В РАЗРАБОТКЕ ГИБРИДНЫХ ПРИЛОЖЕНИЙ // E-Scio. 2022. №4 (67). URL: <https://cyberleninka.ru/article/n/sravnenie-freymvorkov-flutter-i-react-native-ispolzuemyh-v-razrabotke-gibridnyh-prilozheniy> (дата обращения: 11.04.2024).

7. Новая система взаимодействия с иностранными студентами (mgimo.ru) URL: <https://mgimo.ru/about/news/main/intsup/> (дата обращения: 28.03.2024)

8. НОУ ИНТУИТ | Разработка гибридных приложений для мобильных устройств под Windows Phone. Лекция 1: Особенности разработки гибридных мобильных приложений (intuit.ru) URL: <https://intuit.ru/studies/courses/18046/1187/lecture/21572?ysclid=luvclx1ie8433130372> (дата обращения: 10.04.2024)

9. Помощник иностранного студента URL: <https://international-student-assistant.netlify.app/pages/about/about> (дата обращения: 28.03.2024)

10. Разработка мобильного приложения «Мой БашГУ» на базе операционной системы Android: текст для Дипломной работы - Allref.su URL: <https://allref.su/downloads/razrabotka-mobilnogo-prilozheniya-moj-bashgu-na-baze-operacionnoj-sistemy-android/?ysclid=luicw4z1s5910094592> (дата обращения: 28.03.2024)

11. Разработка мобильного приложения для интеграции и адаптации иностранных студентов в учебную и социальную жизнь НИУ ВШЭ – Выпускные квалификационные работы студентов НИУ ВШЭ – Национальный исследовательский университет «Высшая школа экономики» (hse.ru) URL: <https://www.hse.ru/edu/vkr/368892179?ysclid=lui7kpl1rf223675047> (дата обращения: 28.03.2024)

12. Разработка программного комплекса (клиентское мобильное приложение) PreTPU для иностранных студентов URL: <http://earchive.tpu.ru/handle/11683/67465> (дата обращения: 28.03.2024)

13. Социокультурная адаптация иностранных студентов в российских вузах: проблемы, решения, лучшие практики [Электронный ресурс] : сборник статей по материалам Всероссийской научно-практической конференции (8–9 декабря 2021 г.) / Пермский государственный национальный исследовательский университет. – Электронные данные. – Пермь, 2022. – 2,38 Мб ; 90 с. – Режим доступа:

<http://www.psu.ru/files/docs/science/books/sborniki/Sociokulturnayaadaptaciya-inostrannyh-studentov-v-rossijskih-vuzah.pdf>. – Заглавие с экрана.

14. Сравнительный анализ кроссплатформенных подходов к разработке мобильных приложений / М.С. Орлова, М.В. Слива // III Международная научно-практическая конференция «Современное программирование» - УДК 519.688 DOI: 10.36906/AP-2020/20 EDN: QNBQPT

15. Сулейманов Т. Р. Разработка мобильного приложения для иностранных студентов / Т. Р. Сулейманов, М. Л. Бердникова // Фундаментальная математика и ее приложения в естествознании: спутник Международной научной конференции "Уфимская осенняя математическая школа-2022" : Тезисы докладов XIII Международной школы-конференции студентов, аспирантов и молодых ученых, посвященной 50-летию образования математического и физического факультетов БашГУ, Уфа, 21–22 октября 2022 года / Отв. редактор Л.А. Габдрахманова. – Уфа: Башкирский государственный университет, 2022. – С. 25. – DOI 10.33184/fmpve2022-2022-10-19.21. – EDN COSLJX.

16. Электронный архив открытого доступа НИУ «БелГУ»: Проектирование и разработка информационного обеспечения интернет-ресурса для сопровождения иностранных абитуриентов (bsu.edu.ru) URL: <http://dspace.bsu.edu.ru/handle/123456789/38185> (дата обращения: 28.03.2024)

17. Docs | Flutter URL: <https://docs.flutter.dev/> (дата обращения: 09.03.2024)

18. React Native Learn once, write anywhere URL: <https://reactnative.dev/> (дата обращения: 09.03.2024)

DEVELOPMENT OF A WEB APPLICATION FOR ACCOMPANYING INTERNATIONAL STUDENTS

*V.M. Avdonina, I.N. Dorofeev, A.D. Kosberg, A.P. Kuznetsov, O.P. Marinkina,
T.S. Posokhina, E.Yu. Nikitina*
Perm State University

Abstract. It describes a universal information resource implemented as a web application with reference information intended for international students. The information posted in this resource will help students in solving typical problems, as well as in orientation around the PSU campus and the city of Perm. The application was created using Flutter tools and has a client-server architecture.

Keywords: *web application, hybrid application, international students, widget.*

ПЕРСПЕКТИВЫ РАЗВИТИЯ МЕТОДОВ ИНФОРМАЦИОННОГО ПРОТИВОБОРСТВА

А.Н. Рабчевский

Пермский государственный национальный исследовательский университет

Аннотация. В настоящей статье кратко рассмотрено текущее состояние дел в сфере информационного противоборства. Сделан прогноз об усилении информационного давления в контексте информационных войн. Показаны изменения информационной среды в социальных медиа и описаны новые технологии, используемые для манипуляции сознанием пользователей. Выявлены основные технологии, которым предстоит противодействовать в среднесрочной перспективе. Предложены направления научных и технологических исследований и новые программные продукты, необходимые для противодействия новым угрозам.

Ключевые слова: *дипфейк, социальная инженерия, манипуляция, информационное противодействие.*

Текущее состояние дел в информационной войне, развязанной странами коллективного Запада против нашей страны, характеризуется тем, что по всей западной границе России расположены центры информационных операций, деятельность которых направлена против нашей страны. На Украине развернуты ЦИПСО (центры информационно-психологических операций), призванные осуществлять информационно-психологические операции на территории России и стран СНГ. Общая численность войск ЦИПСО составляет не менее 600 человек. Для ведения подрывной информационно-пропагандистской работы в России и против России на Западе была создана сеть специальных структур, именуемых «центрами передового опыта» (Centers of Excellence) НАТО. В Латвии это Центр передового опыта (NATO StratCom Centre of Excellence). Его цель – совершенствование технологий воздействия на целевую аудиторию для формирования радикальной оппозиции. В Эстонии – NATO Cooperative Cyber Defence COE – (CCDCOE). Его задачи: техническое обеспечение информационных операций, укрепление потенциала, сотрудничества и обмена информацией между странами НАТО и партнерами в области киберзащиты. В Литве – Центр передового опыта НАТО по проблемам энергетической безопасности (NATO Energy Security COE). Его задача – идентификация потенциальных энергетических угроз и выработка рекомендаций для членов альянса по их эффективному преодолению. В Хельсинки – Центр по обобщению информации о гибридных угрозах. Его цель – борьба с якобы исходящими от России гибридными угрозами. «Польская Центральная группа психологических действий» (Polish Central PSIOPS Group – PSPG) – элитный блок вооруженных сил Польши, специализирующийся на проведении психологических операций. Достижение военно-

политических и пропагандистских целей здесь видится через осуществление информационно-психологического воздействия на войска и население противника.

Из представленных выше данных совершенно очевидно, что Россия находится под информационным огнем противника. Так по данным ФСБ в 2022 году было выявлено свыше 5000 хакерских атак на критическую инфраструктуру России. Количество информационно-психологических атак постоянно растет. Особенно ситуация обострилась с началом специальной военной операции на Украине.

Исходя из основных доктринальных документов [1, 2, 4–6], с точки зрения США, Россия воспринимается как автократия, выступающая с ревизионистских позиций, стремящаяся нарушить устоявшийся международный порядок, основанный на правилах, сложившийся после окончания второй мировой войны, а особенно после окончания холодной войны, как агрессор, вмешивающийся во внутренние дела США и других, в том числе европейских стран, стремящийся к разрушению связей в Евросоюзе, нарушению европейской безопасности и использующий свои природные ресурсы как оружие для осуществления давления на другие страны. Соответственно, США и их союзники должны объединить свои усилия для всемерного стратегического сдерживания России и противодействия любым мерам, способствующим дальнейшему развитию России. В декабре 2025 года была опубликована новая версия стратегии национальной безопасности, в которой указано, что одним из основных направлений стратегии является налаживание с Россией отношений сотрудничества. Возможно, это связано с осознанием в администрации президента США новых геополитических реалий, связанных с формированием многополярного мира. Казалось бы, стратегия полностью изменила курс и теперь можно расслабиться и оставить усилия по формированию рубежа информационной безопасности. Однако помимо стратегии национальной безопасности существуют и другие доктринальные документы, в которых в отношении к России ничего не изменилось. Кроме того, нужно понимать, что стратегия национальной безопасности принимается каждый год и не факт, что со сменой президента новая стратегия не вернется к прежнему конфронтационному варианту. Кроме того, не стоит забывать про принципы ведения войны от Сунь-Цзы, который говорил про войну, как искусство обмана.

Совершенно очевидно, что информационное давление на нашу страну будет усиливаться. И связано это с тем, что Россия не просто выстояла в противостоянии со всем западным миром в конфликте на Украине, а еще и поднялась в экономическом и военном плане и постоянно одерживает одну победу за другой на поле боя. Кроме того, наличие и современный уровень развития ядерной триады России не позволяет странам запада осуществить прямую военную агрессию. А поскольку Россия воспринимается на Западе как экзистенциаль-

ная угроза западной безопасности, то усилия стран Запада будут направлены на всяческое ослабление и разрушение России невоенными способами. И чем больше Россия будет подниматься, тем сильнее будет давление в информационной войне.

Стоит ли говорить, что без обеспечения мер информационного противодействия со стороны России, безопасности нашей страны грозит катастрофический ущерб. Для обеспечения эффективной защиты от информационных угроз необходимо проводить разработку современных средств противодействия деструктивному воздействию.

В статье 57 Стратегии национальной безопасности РФ изложены задачи, необходимые для достижения цели обеспечения информационной безопасности, среди которых основными являются следующие:

«2) развитие системы прогнозирования, выявления и предупреждения угроз информационной безопасности Российской Федерации, определения их источников, оперативной ликвидации последствий реализации таких угроз;

3) предотвращение деструктивного информационно-технического воздействия на российские информационные ресурсы, включая объекты критической информационной инфраструктуры Российской Федерации;

10) развитие сил и средств информационного противоборства;

12) совершенствование средств и методов обеспечения информационной безопасности на основе применения передовых технологий, включая технологии искусственного интеллекта и квантовые вычисления» [3].

В пунктах 2, 10 и 12 прямо говорится о том, что необходимо развивать силы и средства информационного противоборства, развивать системы прогнозирования, выявления и предупреждения угроз информационной безопасности на основе применения передовых технологий, включая технологии искусственного интеллекта и квантовые вычисления.

Что же происходит в области противодействия информационным атакам и что нас может ожидать в ближайшем будущем, какие угрозы мы должны уже сейчас предвидеть и развивать средства противодействия им?

В настоящее время мы находимся в стадии отказа от мессенджера Телеграмм, серверы которого находятся в США и вероятнее всего контролируются их спецслужбами, и постепенного перехода на суверенный российский мессенджер МАХ. Несомненно, такой переход приведет к усилению нашего цифрового суверенитета и ограничит возможность иностранных государств осуществлять деструктивное воздействие на российских пользователей социальных медиа. Казалось бы, это должно укрепить нашу информационную безопасность. В сочетании с ужесточением мер по ограничению бесконтрольной продажи СИМ-карт это должно затруднить создание армии деструктивных ботов в мессенджере МАХ. Но судя по тому, каких высот достигла социальная инженерия, методы которой используются западными спецслужбами для проведения мо-

шеннических операций против граждан нашей страны и для их вербовки для совершения террористических акций на территории России, не стоит ожидать, что эти ограничительные меры значительно затруднят внедрение деструктивных агентов в российские социальные медиа. А раз так, то и в этой сфере следует ожидать обострения информационного противостояния.

Итак, понятно, что давление будет нарастать, вторжение деструктивных агентов в социальные медиа будет продолжаться. Также следует иметь в виду, что переход на МАХ не означает, что все пользователи откажутся от использования Телеграмм. В некоторых случаях это диктуется привычкой, пренебрежением к правилам информационной безопасности и даже протестом против «насилованной» миграции на другие платформы. Тем более, что использование средств VPN позволяет работать в западных социальных медиа без ограничений. Таким образом, средства воздействия на российских граждан не исчезнут, а методы социальной инженерии будут становиться все более изощренными. И в этой ситуации крайне важно всемерно развивать методы противодействия. Однако, чтобы понять, как противодействовать, сначала нужно понять, чему нам предстоит противодействовать в среднесрочной перспективе.

Очевидно, что мы находимся в стадии бурного развития генеративных нейросетевых технологий. Сегодня сгенерировать изображение любого человека или подделать его голос технически сможет любой студент. Это значит, что нас ожидает гремучая смесь дипфейков и методов социальной инженерии. Из этого следует, что с каждым разом распознать подделку простому пользователю будет все труднее, а в сочетании с методами психологического воздействия с использованием приемов социальной инженерии, угроза информационной безопасности существенно возрастет.

Противодействие подобным угрозам должно предполагать онлайн анализ видео и аудио потоков на предмет выявления артефактов, характерных для подделки с одной стороны, и анализ аудиопотока на предмет выявления методов психологического воздействия на сознание и подсознание пользователей с другой. Для этого необходимо проведение научных и технологических исследований по методам выявления дипфейков, методам онлайн преобразования речь-в-текст, методам анализа текстов на предмет выявления психологических признаков манипуляции, характерных для социальной инженерии. Очевидно также, что нужны разработки программных модулей для установки на мобильные устройства пользователей и на серверное оборудование, которые могут на лету выявлять признаки дипфейков и попыток манипуляции и блокировать трафик или выдавать предупреждение об опасности.

Проведение исследований в данной области и внедрение подобных систем позволит существенно повысить уровень информационной безопасности граждан нашей страны, пользователей социальных медиа.

Список литературы

1. Commander's Handbook for Strategic Communication and Communication Strategy Version 3.0. US Joint Forces Command Joint Warfighting Center. 2010.
2. Commander's Handbook for Strategic Communication and Communication Strategy Version 3.0. // Joint Combat Operations Center, United States Joint Forces Command [Электронный ресурс]. URL: <https://www.yumpu.com/en/document/view/7925384/commanders-handbook-strategic-communication-communication-> (дата обращения: 27.01.2026).
3. О Стратегии национальной безопасности Российской Федерации. Указ Президента Российской Федерации от 02.07.2021 г. № 400 // <http://www.kremlin.ru/acts/bank/47046>.
4. NATIONAL SECURITY STRATEGY // 2022.
5. National Defense Strategy // U.S. Department of Defense. 2022.
6. NATIONAL CYBERSECURITY STRATEGY // 2023. С. 1–39.

PROSPECTS FOR THE DEVELOPMENT OF INFORMATION CONFRONTATION METHODS

A. N. Rabchevsky

Perm State University

Abstract. This article briefly discusses the current state of affairs in the field of information confrontation. A forecast was made about increasing information pressure in the context of information wars. Changes in the information environment in social media are shown and new technologies used to manipulate the consciousness of users are described. The main technologies to be counteracted in the medium term have been identified. Areas of scientific and technological research and new software products necessary to counter new threats are proposed.

Keywords: *deepfake, social engineering, manipulation, information counteraction.*

ТЕХНИЧЕСКИЕ МЕТОДЫ ПРОТИВОДЕЙСТВИЯ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ

И.С. Сыпачев, Е.Ю. Никитина

Пермский государственный национальный исследовательский университет

Аннотация. Сегодня информационные технологии плотно вошли в жизнь, делая её проще и удобнее. Однако для злоумышленников эти технологии открыли множество возможностей для получения разного рода информации, в том числе и той, доступ к которой они не имеют права получать. Самый популярный, на сегодняшний день, способ получения такой информации - это социальная инженерия. Она позволяет обходить, не взламывая, системы защиты информации. Человеческий фактор играет существенную роль в построении системы защиты информации. Рассматриваются технические методы противодействия социальной инженерии и предлагается несколько новых способов решения.

Ключевые слова: *социальная инженерия, информационные технологии, фишинг, информационная безопасность, методы противодействия.*

Социальная инженерия — это метод манипуляции людьми с целью получения их конфиденциальной информации, доступа к ресурсам или другим представляющим ценность объектам [1]. Киберпреступники прекрасно овладели искусством обмана: они знают, как убедить ничего не подозревающих пользователей поделиться своими данными, распространить вредоносную программу или открыть доступ к системам, не предназначенным для посторонних. Атаки происходят не только в интернете, но также при личном общении и других видах взаимодействия.

Социальные инженеры выстраивают мошеннические схемы, основываясь на своих знаниях о психологии человеческого поведения. Именно поэтому они легко манипулируют сознанием и действиями пользователей. Разобравшись с мотивами поведения своей жертвы, преступники могут эффективно применять методы психологического манипулирования.

Помимо методов социальной инженерии злоумышленники нередко рассчитывают на недостаток знаний у пользователя. Технологии развиваются так быстро, что о некоторых типах угроз, например, о заражении путем скрытой загрузки, многие рядовые пользователи даже не слышали.

Как правило, специалисты по социальной инженерии преследуют одну из двух целей.

- Диверсия: причинение вреда или неудобств в результате повреждения данных.
- Кража: получение ценной информации, доступа к ресурсам или денег.

Жизненный цикл атаки методами социальной инженерии позволяет преступникам выстроить относительно надёжную схему обмана пользователя. Как правило, подобная атака включает следующие стадии:

- Подготовка - сбор информации о жертве или группе, к которой он (она) принадлежит;
- Проникновение - установление контакта с жертвой и завоевание доверия;
- Эксплуатация - поиск и использование уязвимости жертвы;
- Исчезновение - прекращение общения с жертвой после достижения поставленной цели.

Весь этот процесс может уместиться в одном сообщении электронной почты, а может длиться несколько месяцев и занимать много страниц переписки. Иногда злоумышленники даже встречаются с жертвой.

К сожалению, многие пользователи не понимают, что даже незначительные на первый взгляд данные могут открыть преступникам доступ к сетям и учетным записям. Выдавая себя за легитимного пользователя, злоумышленник может обратиться в службу IT-поддержки и узнать личные данные жертвы, например, имя, дату рождения или адрес. Пользуясь этой информацией, преступники могут изменить пароли в аккаунтах жертвы и получить практически неограниченный доступ к ним.

Область того, на что может быть направлена атака с использованием социальной инженерии, может быть разнообразна. С точки зрения выполнения технического противодействия подобного рода атакам, необходимо рассматривать широкий спектр решений, которые могут относиться к данному вопросу. К таким решениям могут относиться: DLP-системы, брандмауэры, IDS и IPS-системы, системы оповещения пользователей и многофакторную аутентификацию.

DLP-система (Data Leak Prevention) представляет собой технологии, предназначенные для предотвращения утечек конфиденциальной информации из информационной системы, а также включает в себя технические устройства (как программные, так и аппаратные) для этой же цели. [2] Основой работы DLP-систем является анализ потоков данных, которые пересекают границы защищаемой информационной системы. При обнаружении конфиденциальной информации в этих потоках активируется компонент системы, который блокирует передачу сообщения, пакета или сессии.

Распознавание конфиденциальной информации осуществляется двумя методами: анализом формальных признаков (например, грифа документа, специальных меток, сравнением хеш-функций) и анализом содержимого. Первый метод помогает избежать ложных срабатываний (ошибок первого рода), но требует предварительной классификации документов, внедрения меток и сбора сигнатур. Однако при этом возможны пропуски конфиденциальной информации (ошибки второго рода), если документ не был заранее классифицирован. Вторым методом может приводить к ложным срабатываниям, но позволяет выявлять

пересылку конфиденциальной информации даже среди документов без специальных меток. В качественных DLP-системах оба метода комбинируются.

DLP-системы состоят из компонентов (модулей) сетевого уровня и компонентов уровня хоста. Сетевые компоненты контролируют трафик, который пересекает границы информационной системы, и обычно размещаются на прокси-серверах, серверах электронной почты или в виде отдельных серверов. Компоненты уровня хоста устанавливаются на персональных компьютерах сотрудников и контролируют такие каналы, как запись данных на компакт-диски и флэш-накопители. Они также следят за изменениями сетевых настроек, установкой программ для туннелирования, стеганографии и другими методами обхода контроля.

Брандмауэры — это программные или аппаратные средства защиты, которые фильтруют входящий и исходящий трафик, блокируя нежелательные соединения и позволяя легитимные. Брандмауэры могут находиться на уровне операционной системы (например, встроенные в Windows - программный вариант) или быть отдельными аппаратными устройствами (аппаратный вариант).

По архитектуре брандмауэры делятся на:

- Бастийный хост - защищает внутреннюю сеть от внешних угроз. Концепция заключается в том, что это брандмауэр, обращённый к общедоступной сети: перед ним нет защиты, он должен нести все последствия атаки, направленной на сеть.
- Экранированная подсеть – «тройной брандмауэр», который имеет три сетевых интерфейса и разделяет трафик на три логических сетевых сегмента, среди которых выделяют общедоступный интернет и внутреннюю сеть.
- Фильтрация пакетов - проверяет заголовки пакетов проходящего трафика на допустимость (такие как, например, IP-адреса источника и получателя), но не их содержимое.
- Шлюзовые брандмауэры - работают на более высоких уровнях модели OSI и могут проверять содержимое трафика.
- Брандмауэры нового поколения - включают в себя межсетевой экран с отслеживанием состояния, осведомлённость о приложениях и системы обнаружения вторжений. Осведомлённость о приложениях означает, что брандмауэр может отличить HTTP-сообщение, отправляемое на веб-сайт, от вредоносного кода в HTTP-сообщении. Кроме того, он поставляется с пользовательским контролем, который нужен для определения того, к чему у пользователя есть доступ [3].

Системы обнаружения вторжений (IDS - Intrusion Detection System) предназначены для выявления вредоносной активности в сети и на устройствах, а также создания отчётов о таких инцидентах. В отличие от брандмауэров, которые блокируют нежелательный трафик, IDS в основном наблюдают и сообщают о потенциальных угрозах. Они могут вести журналы активности, чтобы администраторы могли анализировать данные и выявлять шаблоны атак [4].

Существуют следующие виды IDS:

- IDS на основе сигнатур - сравнивает трафик с известными шаблонами атак.
- IDS на основе статистических аномалий - определяет нормальный трафик и выявляет аномалии.
- Сетевые IDS (NIDS) - занимаются мониторингом трафика в сети.
- Хостовые IDS (HIDS) - работают на конкретных устройствах, отслеживая изменения в файловых системах и конфигурациях.

Системы оповещения пользователей — это программные решения, предназначенные для отправки уведомлений и сообщений пользователям через различные каналы связи. Они позволяют оперативно информировать пользователей о важных событиях, требующих их внимания.

- Антифрод-системы - анализируют звонки и сообщения на наличие подозрительных паттернов. В том числе они могут использовать машинное обучение для выявления мошеннических схем и предупреждения пользователей.
- Системы фильтрации звонков - Многие операторы мобильной связи предлагают услуги, которые автоматически фильтруют звонки от определенных номеров или помечать их как потенциально опасные.
- Системы оповещения о фишинге - могут интегрироваться с мессенджерами и электронной почтой, предупреждая пользователей о подозрительных ссылках и сообщениях, которые могут содержать фишинговые атаки.

Многофакторная аутентификация — это метод защиты, который требует от пользователя предоставить два или более доказательства своей идентичности перед получением доступа к системе, приложению или данным. Это может быть, как код, присылаемый на номер телефона или почту, так и биометрические данные. Подобный метод уменьшает возможность несанкционированного доступа, даже при получении третьими лицами данных об учётной записи пользователя.

Рассматривая возможные направления решения вопроса применения технических методов противодействия социальной инженерии, сначала необходимо точно определить, на какую область проблемы будет распространяться эти решения. Существуют две области применения методов социальной инженерии: методы социальной инженерии, направленные на обычных пользователей, и атаки на компании.

На наш взгляд, в первом случае способ решить проблему социальной инженерии имеется с программной стороны. Во втором же случае есть возможность применить не только программные, но и технические средства противодействия.

Первым предложением с нашей стороны является *введение статуса проверенного лица* в почтовых системах. Суть состоит в том, что сервис электронной почты должен обязывать коммерческие организации проходить проверку

при создании почтового ящика, с которого будет производиться рассылка каких-либо сообщений их клиентам, а также возможность самому пользователю делать пометки для ящиков, которые для него являются проверенными. Такое решение, с недавнего времени, было реализовано в сервисе Mail.ru, однако оно затрагивает только аспект писем от коммерческих организаций.

Также при открытии сообщения необходимо предупреждать пользователя электронной почты о сходстве адреса почтового ящика сообщения с адресом почтового ящика проверенного пользователя (например, при расхождении или подмене 1-2 символов в адресе проверенного пользователя). Такое решение может быть применено и эффективно работать как для компаний, так и для отдельных пользователей.

Также введение статуса проверенного лица необходимо ввести в мессенджерах и телефонных звонках. Пользователь может предоставить оператору связи разрешение на подтверждение его номера телефона, как номера определённого человека и, при исходящем от этого пользователя звонке, передавать вызываемому абоненту статус подтверждённого пользователя и своё ФИО. Таким образом вызываемый абонент сможет понять, что вызов поступает от человека, ФИО которого указано оператором связи. Но у этого предложения могут возникнуть проблемы с законодательной стороны, поэтому оно может нуждаться в доработке.

Вторым предложением с нашей стороны является создание *корпоративной системы обмена данными для предприятия*. Указанная система может включать в себя все необходимые средства коммуникации сотрудников – почту, мессенджер, телефонную связь и т.д. При этом все остальные системы обмена данными должны быть запрещены. Также доступ к этой системе должен осуществляться исключительно по внутренней сети предприятия, что закрывает потребность передачи информации между офисами компании или для сотрудников, работающих удалённо. Считаем, что подобное решение сильно затруднит попытку атаки при помощи фишинговых сообщений на компанию. Также программный запрет использования систем обмена данными на рабочей технике позволит снизить риск попадания вредоносного ПО или хищения информации обманным путём.

По нашему мнению, эти два варианта решения проблемы являются необходимыми к осуществлению, ведь есть только два способа защиты незнающего пользователя от фишинга: оповестить пользователя о возможном фишинге и не допустить этой возможности. Существующие на данный момент решения либо закрывают эти два аспекта проблемы, либо помогают избавиться от проблемы после её появления. С учётом сложности влияния на человеческий фактор в данном вопросе, совокупность существующих и предложенных методов позволит снизить риски, которые возникают при использовании в атаках социальной инженерии.

Список литературы

1. Информационная статья на тему «Что такое социальная инженерия?» от Лаборатории Касперского [Электронный ресурс]. URL: <https://www.kaspersky.ru/resource-center/definitions/what-is-social-engineering> (дата обращения 20.03.2025).
2. Информационная статья на тему «Обзор DLP-систем на мировом и российском рынке» от Anti-malware [Электронный ресурс]. URL: https://www.antimalware.ru/analytics/Technology_Analysis/DLP_market_overview_2014 (дата обращения 20.03.2025).
3. Информационная статья на тему «Типы брандмауэров» [Электронный ресурс]. URL: <https://habr.com/ru/articles/680010/> (дата обращения 20.03.2025).
4. Информационная статья на тему «IDS Системы обнаружения вторжений» [Электронный ресурс]. URL: <https://habr.com/ru/articles/680028/> (дата обращения 20.03.2025).

TECHNICAL METHODS OF COUNTERING SOCIAL ENGINEERING

I.S. Sypachev, E.Y. Nikitina

Perm State University

Abstract. Today, information technology is firmly embedded in life, making it easier and more convenient. However, these technologies have opened up many opportunities for attackers to obtain all kinds of information, including information that they are not allowed to access. The most popular way to obtain such information today is through social engineering. It allows you to bypass information security systems without hacking. The human factor plays an essential role in building an information security system. Technical methods of countering social engineering are considered and several new solutions are proposed.

Keywords: *social engineering, information technology, phishing, information security, counteraction methods.*

ЗАЩИТА ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА НА ФИЗИЧЕСКОМ УРОВНЕ

А.Н. Трухин, А.В. Черников

Пермский государственный национальный исследовательский университет

Аннотация. в рамках работы показана актуальность проблемы несанкционированного доступа (НСД) к информации. Основная проблематика данной статьи: получение НСД к информации именно физическим способом. В работе ставится задача выяснить, что является несанкционированным доступом, какими средствами обеспечивается защита информации от НСД на физическом уровне, а также рассмотреть средства защиты от НСД на физическом уровне, предложить варианты совершенствования текущих средств защиты.

Ключевые слова: информация, физическая защита информации, несанкционированный доступ, информационная безопасность.

Введение

Для начала определимся, что же такое несанкционированный доступ и защита информации от НСД. Для того обратимся к официальным источникам [1,2]:

Несанкционированный доступ (НСД) — доступ к информации или действия с информацией, осуществляемые с нарушением установленных прав и (или) правил доступа к информации или действий с ней с применением штатных средств информационной системы или средств, аналогичных им по функциональному назначению и техническим характеристикам [2].

Защита информации от несанкционированного доступа — деятельность, направленная на предотвращение получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации [1].

Далее рассмотрим основные системы защиты информации на физическом уровне (рис. 1):

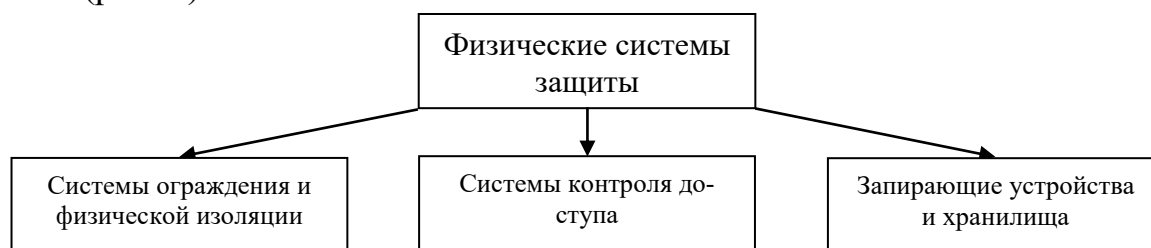


Рис. 1. Классификация физических систем защиты

Системы ограждения и физической изоляции обеспечивают:

- защиту объектов по периметру;
- защиту элементов зданий и помещений;
- защиту объемов зданий и помещений.

Системы контроля доступа реализуют:

- контроль доступа на охраняемые объекты;
- защиту документов, данных, файлов.

Запирающие устройства и хранилища включают:

- различные системы запирающих устройств;
- различные системы сейфов и хранилищ. [3]

Ниже рассмотрим подробнее системы защиты.

Системы ограждения и физической изоляции

Инженерные конструкции.

Для защиты территории используют прочные заборы из бетона, кирпича или металла, усиленные колючей проволокой или спиральной лентой диаметром до 955 мм. Дополнительно применяют малозаметные препятствия, такие как металлические сети, замедляющие злоумышленников [4].

Уязвимые точки зданий — двери и окна. Двери классифицируют по взломостойкости (ГОСТ Р 51072-97). Для защиты помещений от НСД подходят двери 1–4 классов: от минимальной защиты, взламываемой за 5–9 минут, до устойчивых к мощному электроинструменту и легкому оружию, с бронированной сталью и сложными замками. Замки бывают *механическими* (с ключом) и *электроуправляемыми* (соленоидные, электромагнитные, электромеханические), последние могут работать без питания [5,6].

Окна, особенно на первом этаже, защищают закаленным или армированным стеклом, решетками, ставнями. По уровню безопасности их делят на четыре класса: от обычного стекла до пулестойкого или бронированного. Важно убрать объекты, облегчающие доступ к окнам, например, лестницы или деревья [5].

Охранная сигнализация.

Охранная сигнализация выявляет попытки несанкционированного проникновения на объект. Она может быть *однорубежной* (один тип датчиков) или *многорубежной* (несколько рубежей для отслеживания движения нарушителя и повышения надежности). Система учитывает климат (температура, осадки, промерзание) и помехи (транспорт, животные). Требования: полный охват периметра, высокая чувствительность, надежность в любую погоду, устойчивость к помехам, точное определение места нарушения, централизованный контроль.

Основные виды датчиков: *электромеханические, вибрационные, инфракрасные, емкостные, индуктивные и др.* Каждый тип реагирует на определенные действия нарушителя (перелезание, резка, движение) и адаптирован к разным условиям, но может требовать настройки для исключения ложных срабатываний [4,5].

Средства наблюдения.

Система видеонаблюдения следит за въездами-выездами, движением людей и зонами хранения данных, записывая видео для последующего анализа. Она решает задачи мониторинга доступа, контроля серверных и прилегающих территорий, а также фиксации инцидентов. Системы бывают простыми, с одной камерой, или сложными, с многокамерной обработкой видео в реальном времени. Для защиты данных нужны камеры высокого разрешения с ночным режимом.

Камеры выбирают по условиям эксплуатации. Черно-белые обеспечивают высокое разрешение для удаленных объектов, цветные дают детализированное изображение для идентификации, но стоят дороже. Камеры «день-ночь» переключаются между цветным и черно-белым режимами, используя ИК-подсветку для съемки в темноте на расстоянии до 30–50 м.

Объективы влияют на качество изображения. Монофокальные с фиксированным фокусом подходят для статичных зон благодаря высокой светосиле. Вариофокальные позволяют вручную настраивать фокус и угол обзора для переменных условий. Трансфокаторы с дистанционным зумом удобны для динамического наблюдения за удаленными объектами.

Камеры делятся на аналоговые, которые дешевле и проще, но ограничены в разрешении, и цифровые (IP), обеспечивающие высокое разрешение и удаленный доступ, но требующие стабильной сети. Беспроводные Wi-Fi-камеры подходят для объектов, где невозможно проложить кабели, но их сигнал может быть нестабилен из-за помех.

По конструкции камеры бывают стационарными для узких зон, вроде входов или коридоров, поворотными для больших территорий с управлением оператором, купольными для скоростного наблюдения внутри и снаружи, а также уличными с антивандальными корпусами, защищенными от пыли, влаги и температур от -60°C до $+50^{\circ}\text{C}$ [7].

Экранирование.

Экранирование предотвращает утечку данных и помехи, вызванные электромагнитными полями от токов или перепадов напряжения. Оно делится на три типа: *электростатическое* (защита от электрических полей, требует заземленного металлического экрана), *магнитостатическое* (защита от низкочастотных магнитных полей с помощью материалов вроде пермаллоя) и *электромагнитное* (ослабление высокочастотных полей вихревыми токами).

Экраны должны быть герметичными, с минимальными щелями (не больше длины волны) и прочными соединениями (сварка, пайка). Для оборудования и помещений используют листовую сталь (0,35–2 мм) или сетки (ячейки 0,4–2,5 мм), которые ослабляют излучение до 90 дБ. Стены покрывают токопроводящими красками, окна — металлизированными стеклами, а двери и окна оснащают пружинными контактами. Для кабелей применяют коаксиальные или витые пары с экранирующей оплеткой, минимизирующей помехи [7].

Звукоизоляция.

Звукоизоляция предотвращает утечку акустических сигналов (например, разговоров) через щели, окна, двери, вентиляцию или вибрации стен и коммуникаций. Цель — снизить уровень звука снаружи до незаметного на фоне обычных шумов, чтобы его не уловили шпионские устройства. Эффективность зависит от отражения и поглощения звука: плотные материалы (кирпич, бетон) отражают, пористые (вата, поролон) поглощают.

Некоторые средства звукоизоляции:

- *Звукопоглощающие материалы:* минвата, стекловата, войлок (толщиной 25 мм) поглощают до 0,85 звука, особенно на высоких частотах. Применяют для стен, потолков, в виде плит или рельефов.
- *Акустические экраны:* временные конструкции перед окнами/дверями, гасят 8–10 дБ.
- *Звукоизолирующие кабины:* каркасные (гасят на 35–40 дБ) или бескаркасные (до 50–55 дБ) с глушителями вентиляции.

Для высокой защиты комбинируют плотные и поглощающие материалы, используют многослойные конструкции. При необходимости добавляют шумогенераторы для виброакустической маскировки [7].

Визуально-оптическая защита.

Визуально-оптическая защита предотвращает утечку информации через световые сигналы, блокируя их или делая бесполезными для злоумышленников.

Основные методы:

- *Расположение объектов:* документы и мониторы размещают под углом к окнам, чтобы избежать отражений, видимых снаружи.
- *Снижение отражений:* поверхности покрывают матовыми красками или материалами, уменьшающими блики.
- *Преграды для света:* применяют шторы, жалюзи, тонированные стекла или ширмы для блокировки обзора.

Для надежности комбинируют несколько методов, например, тонировку окон и матовые покрытия, продумывая расположение объектов и освещение [8].

Уничтожение данных.

Физическое уничтожение данных с помощью механического, термического, химического или магнитного воздействия делает носитель непригодным для чтения. Выбор метода зависит от типа носителя и уровня секретности.

- *Механическое уничтожение:* носитель измельчают в шредере до частиц менее 2 мм (для HDD — промышленные шредеры). Простые методы (сверление, удары) ненадежны, так как фрагменты могут быть восстановлены.
- *Термическое уничтожение:* нагрев до 800–1000 °С (выше точки Кюри ~770 °С) разрушает магнитный слой HDD или чипы SSD, делая данные невозможными. Используют печи или горелки.
- *Химическое уничтожение:* агрессивные вещества (кислоты) разъедают магнитный слой или чипы. Эффективно, но опасно и требует спецусловий.

- *Размагничивание*: для HDD применяют мощное магнитное поле (≥ 500 кА/м), стирающее данные и форматирование. Для SSD не подходит [9], [10].

Все методы надежны, но уничтожают носитель без возможности повторного использования. Для HDD предпочтительно размагничивание, для SSD — механическое или термическое уничтожение.

Системы контроля доступа

Организация допуска на объект с конфиденциальной информацией требует *идентификации* (присвоение уникального идентификатора) и *аутентификации* (подтверждение подлинности предъявителя). Это предотвращает несанкционированный доступ к защищенным зонам. Существует два основных способа идентификации: атрибутивный и биометрический.

Атрибутивный способ.

Основан на выдаче уникального предмета или кода:

- *Пропуска, жетоны, ключи*: просты, но зависят от контролера, что усложняет автоматизацию.

- *Пароли и коды*: комбинации символов для входа в системы или помещения.

- *Пластиковые карты*: содержат код, считываемый устройством. Должны быть устойчивы к подделке, внешним воздействиям [11].

Минус: идентификатор может быть украден или передан, поэтому для важных объектов комбинируют с биометрией.

Биометрический способ.

Использует физиологические (*статические*) или поведенческие (*динамические*) характеристики. Процесс: сканирование, создание шаблона, сравнение с базой.

- *Дактилоскопия*: отпечатки пальцев (папиллярные узоры). Сканирование за 2–3 секунды, шаблон размером до 1 Кб. Надежность высокая (вероятность НСД 0,0001%), но чувствительна к состоянию кожи.

- *Геометрия лица*: анализ черт лица (Faceprint), устойчива к освещению и ракурсу до 35°. Бесконтактна, надежна, но дорога и чувствительна к мимике.

- *Венозный рисунок руки*: сканирование подкожных вен ИК-камерой. Бесконтактен, устойчив к подделке, точность как у радужки, но чувствителен к за светке.

- *Динамика подписи*: анализ скорости, давления, траектории подписи. Надежнее визуального сравнения, но уязвима к копированию.

- *И другие виды биометрии* [12].

Биометрия надежнее атрибутивных методов, так как привязана к личности, но требует специального оборудования и может быть чувствительна к внешним факторам.

Запирающие устройства и хранилища

Сейфы классифицируются по взломоустойчивости (0–10 класс) и огнестойкости (30Б, 60Б, 90Б) (по ГОСТ Р 50862-2017 и ГОСТ 34360-2017):

- *Нулевой и первый класс*: базовая защита, взламываются за 5–10 минут (монтаж, дрель). Подходят для офисов с обычными документами.

- *Второй и третий класс*: выдерживают электроинструмент 15–20 минут, оснащены сложными замками (механическими, кодовыми, биометрическими). Используются для серверных шкафов или данных средней важности.

- *Четвертый и пятый класс*: бронированные стенки (≥ 10 мм), многоточечные замки, защита от взлома до 30–50 минут. Для особо ценных данных, например, резервных копий серверов.

- *Выше пятого класса*: для банков или военных объектов, защищают от взрывов и резак, но избыточны для обычных организаций из-за цены и веса (до нескольких тонн).

Огнестойкость: сейфы с термоизоляцией (пенобетон, вермикулит) и уплотнителями защищают магнитные носители. Класс 60Б сохраняет содержимое час при пожаре, подходит для HDD и SSD-накопителей. Комбинированные сейфы (взломоустойчивость + огнестойкость) дорогие и требуют анкерного крепления.

Специализированные хранилища (сейфовые комнаты, бункеры, модульные дата-центры): стены из армированного бетона (≥ 200 мм) или стали (≥ 10 мм), двери 3–4-го класса взломоустойчивости, пулестойкое остекление. Интегрированы с СКУД (биометрия + PIN), охранной сигнализацией (например, вибрационные и инфракрасные датчики), видеонаблюдением и экранированием от электромагнитных утечек. Применяются в банках, госучреждениях и крупных дата-центрах [13].

Проблемы защиты информации от НСД

Согласно отчету экспертно-аналитического центра InfoWatch за 2023–2024 годы, ситуация с утечками информации ограниченного доступа в России остается тревожной, подчеркивая необходимость усиления физической защиты:

- *Рост объема утечек*: В 2024 году зарегистрировано 778 инцидентов утечек информации, а объем скомпрометированных записей персональных данных вырос на 30%, достигнув 1,5 млрд записей. Это указывает на масштаб угроз, включая физический доступ к носителям данных.

- *Умышленные инциденты*: 98% всех утечек в 2024 году носили умышленный характер, причем 95% нарушений, совершенных сотрудниками, также были умышленными. Это подчеркивает важность контроля физического доступа к рабочим станциям, серверам и носителям информации.

- *Рост инсайдерских угроз*: почти каждое пятое нарушение (20%) связано с действиями внутренних нарушителей, включая руководителей организаций. Физический доступ сотрудников к конфиденциальной информации остается ключевым каналом утечек.

- *Уязвимость малых организаций*: Доля утечек из малых организаций (до 49 сотрудников) выросла с 18,1% в 2023 году до 27,8% в 2024 году. Такие компании часто не имеют ресурсов для обеспечения физической безопасности, таких как системы контроля доступа, видеонаблюдение или сейфы [14].

Также, например, 3D-печать позволяет создавать копии механических ключей на основе фотографии или слепка замочной скважины. С помощью программ фотограмметрии (научно-техническая дисциплина, которая занимается определением формы, размеров, положения и иных характеристик объектов по их фотоизображениям) и бытового 3D-принтера можно изготовить бамп-ключ за короткое время. Такие методы становятся популярными благодаря мобильным приложениям, которые автоматически генерируют модели ключей из снимков. Атаки на бесконтактные системы контроля доступа также упрощаются: клоны RFID-карт создаются с помощью недорогих считывателей и ноутбука. Компактные устройства могут копировать данные метки в момент ее использования и перехватывать доступ [14-17].

Термическая атака, использующая тепловизоры для фиксации следов от пальцев на клавиатуре, позволяет восстанавливать пароли. Система ThermoSecure, разработанная в 2023 году, восстанавливает до 67% паролей длиной 12–16 символов, если тепловой снимок сделан в течение 20 секунд после ввода [17].

Таким образом, разработка и внедрение новых технологий в этой области остаются приоритетными для обеспечения устойчивости организаций к современным вызовам в сфере информационной безопасности.

Направления решения проблем информационной безопасности от НСД

Замки с изменяемой структурой.

Предлагается создать замки, у которых внутренние штифты меняют положение после каждого открытия. Замок работает с ключом, содержащим микрочип, который через зашифрованный сигнал передает команду для перестройки штифтов. Для дополнительной защиты пользователь вводит одноразовый код через приложение на смартфоне. Например, сотрудник вставляет ключ в замок серверной комнаты, вводит код в приложении, замок открывается, а штифты внутри перестраиваются сервоприводами в новую комбинацию. Это делает отмычки и копии ключей бесполезными, так как структура замка постоянно меняется. Сигнал защищен шифрованием и действует на расстоянии 1–2 см, что предотвращает перехват. Такое решение усиливает физический контроль доступа и подходит для защиты серверных комнат и сейфов.

Носители данных с самоуничтожением.

Для надежной защиты предлагается разработать жесткие диски и SSD с встроенными капсулами, которые при попытке вскрытия выпускают кислоту, растворяющую чипы памяти. Капсула активируется датчиком давления или сигналом, если кто-то пытается открыть корпус без ввода PIN-кода через защищенный порт. Например, если злоумышленник вскрывает SSD в серверной без правильного кода, датчик срабатывает, и кислота уничтожает данные за секунды. Или же можно использовать еще один вариант – механизм нагрева чипа памяти. Это не требует громоздких устройств для утилизации и работает с любыми носителями.

Защита от тепловых атак.

Тепловизоры помогают злоумышленникам считывать пароли с клавиатур. Для защиты предлагается внедрить клавиатуры с теплопоглощающими пластинами, которые мгновенно рассеивают тепло от касаний пальцев. Например, пластина из теплопроводящего материала, встроенная под клавиши, убирает тепловой след за 2–3 секунды, делая тепловизионный анализ бесполезным.

Предложенные решения — лишь возможные варианты решения обхода определенных средств защиты информации, закрывающие слабые места существующих методов.

Самый актуальный вариант – *использование средств физической защиты информации в совокупности между собой, а также другими уровнями защиты информации. Только так можно достигнуть максимального уровня защищенности информации.*

Заключение

В результате проведенной работы становится ясно, что вопрос защиты информации от НСД остается открытым. Существующие методы и средства физической защиты не в полной мере закрывают данную проблематику.

Список литературы

1. ГОСТ Р 50922–2006. Защита информации. Основные термины и определения. [Электронный ресурс] URL: <https://ksc-alternativa.com.ru/wp-content/uploads/2019/08/ГОСТ-Р-50922-2006.pdf> (дата обращения: 23.06.2025).
2. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (Выписка) (утв. ФСТЭК РФ 15.02.2008). [Электронный ресурс] URL: https://www.consultant.ru/document/cons_doc_LAW_99662/ (дата обращения: 23.06.2025).
3. Т.А. Маркина Средства защиты вычислительных систем и сетей. [Электронный ресурс] URL: <https://books.ifmo.ru/file/pdf/2121.pdf> (дата обращения: 23.06.2025).
4. Ю.А. Гатчин, В.В. Сухостат, А.С. Куракин, Ю.В. Донецкая Теория информационной безопасности и методология защиты информации. [Электронный ресурс] URL: <https://books.ifmo.ru/file/pdf/2372.pdf> (дата обращения: 23.06.2025).
5. Е.В. Бурькова Физическая защита объектов информатизации. [Электронный ресурс] URL: http://elib.osu.ru/bitstream/123456789/13741/1/36384_20170503.pdf (дата обращения: 23.06.2025).
6. А.М. Голиков Защита информации от утечки по техническим каналам. [Электронный ресурс] URL: <https://edu.study.tusur.ru/publications/5263/download> (дата обращения: 23.06.2025).
7. Л.А. Полякова, В.Г. Прожерин, Я.И. Савченко Средства инженерно-технического обеспечения охраны объектов. [Электронный ресурс] URL: <https://books.ifmo.ru/file/pdf/1621.pdf> (дата обращения: 23.06.2025).

8. В.А. Ворона, В.О. Костенко. Способы и средства защиты информации от утечки по техническим каналам. [Электронный ресурс] URL: <https://cyberleninka.ru/article/n/sposoby-i-sredstva-zaschity-informatsii-ot-utechki-po-tehnicheskim-kanalam> (дата обращения: 23.06.2025).
9. С. Коженевский, С. Прокопенко Методы гарантированного уничтожения данных на жестких магнитных дисках. [Электронный ресурс] URL: <https://masters.donntu.ru/2011/ftr/riabtsev/library/article15.htm> (дата обращения: 23.06.2025).
10. nplus1.ru. Большая стирка. Как без остатка удалить данные с цифрового носителя. [Электронный ресурс] URL: <https://nplus1.ru/material/2019/12/02/akronis> (дата обращения: 23.06.2025). ГОСТ Р 50862–2017.
11. В.И. Завгородний Комплексная защита информации в компьютерных сетях. [Электронный ресурс] URL: <https://www.elec.ru/library/nauchnaya-i-tehnicheskaya-literatura/kompleksnaya-zashita-informacii/> (дата обращения: 23.06.2025). InfoWatch.ru.
12. В.А. Ворона, В.О. Костенко Биометрические технологии идентификации в системах контроля и управления доступом. [Электронный ресурс] URL: <https://cyberleninka.ru/article/n/biometricheskie-tehnologii-identifikatsii-v-sistemah-kontrolya-i-upravleniya-dostupom> (дата обращения: 23.06.2025).
13. Сейфы, сейфовые комнаты и хранилища ценностей. [Электронный ресурс] URL: https://apit-kovrov.ru/files/uploads/knowledge_base/GOST-R-50862-2017.pdf (дата обращения: 23.06.2025).
14. Россия: утечки информации ограниченного доступа 2023-2024. [Электронный ресурс] URL: <https://www.infowatch.ru/sites/default/files/analytics/files/rossiya-utechki-informatsii-ogranichenного-dostupa-2023-2024.pdf> (дата обращения: 23.06.2025).
15. Kaspersky.ru Как 3D-принтеры помогают вскрывать замки [Электронный ресурс] URL: <https://www.kaspersky.ru/blog/3d-printed-keys/10497/> (дата обращения: 23.06.2025).
16. Plus-One.rbc.ru Как преступники используют 3D-печать для обхода физических замков [Электронный ресурс] URL: <https://plus-one.rbc.ru/society/3d-pechat-dlya-vzloma-dverei> (дата обращения: 23.06.2025).
17. Anti-Malware.ru Клонирование RFID и уязвимости бесконтактных пропусков [Электронный ресурс] URL: <https://www.anti-malware.ru/news/2024-08-09-121598/43896> (дата обращения: 23.06.2025).

PROTECTING INFORMATION FROM UNAUTHORIZED ACCESS AT THE PHYSICAL LEVEL

A.N. Trukhin, A.V. Chernikov

Perm State University

Abstract. The relevance of the problem of unauthorized access (UA) to information is shown within the framework of the work. The main problem of this article is the physical method of obtaining unauthorized access to information. The work aims to determine what constitutes unauthorized access, what measures are taken to protect information from UA at the physical level, and to review the means of protecting against UA at the physical level, as well as to propose improvements to current security measures.

Keywords: *information, physical protection of information, unauthorized access, information security.*

МЕДИАРЕСУРСЫ ДВИЖЕНИЯ «АНТИФА» В АНТИРОССИЙСКОЙ ПОВЕСТКЕ

А.Р. Усманов

Пермский государственный национальный исследовательский университет

Аннотация. Рассматривается информационный аспект деятельности ультралевых экстремистских сообществ в контексте вооруженного конфликта на современной Украине. Анализируются информационные каналы, сопровождающие антироссийскую повестку и их нарративы

Ключевые слова: *антифа, экстремизм, терроризм, специальная военная операция, пропаганда,*

Одними из мегатрендов вовлечения в экстремистскую и террористическую деятельность являются цифровизация, виртуализация общественных отношений и глобализация [1]. Эти явления приводят к насаждению культурных кодов, никогда не присутствовавших на территории и не имеющих никаких связей с исторически сложившимися общественными явлениями. Способны вовлечь в деструктивные сообщества лиц, не имевших ранее склонности к радикальной идеологии и проживавших на значительной удаленности от мест дислокации группировок. Яркий пример пропаганды идей насилия через Интернет продемонстрировала в недавнем прошлом террористическая организация ИГИЛ* (Верховный суд России в 2014 году признал данную организацию террористической и запретил ее деятельность на территории Российской Федерации). В 2015 году на Западе распространился их ролик, в котором молодой человек Андре Пулен убеждал соотечественников-канадцев присоединиться к организации, при этом места, по его словам, хватало всем желающим: «Не можешь сражаться – дай денег» [2]. Такие призывы, распространяемые через сеть Интернет, привели к тому, что в 2017 году к ИГИЛ присоединились свыше 7000 западных последователей и выходцы из 120 разных стран мира [2]. По данным США и ООН, численность группировки в 2016 году насчитывала 36,5 тысячи человек, при этом каждый шестой был гражданином стран Европы. Часто это была суннитская молодежь, которая оказалась восприимчива к пропаганде ИГИЛ в интернете. Были представлены многочисленные выходцы из Индонезии, а так же граждане России и стран СНГ. В июне 2015-го по данным российской полиции численность россиян в ИГИЛ насчитывала 1,8 тыс. человек [3].

Развитие интернета не только позволяет осуществлять вербовку в экстремистскую/террористическую деятельность дистанционно, но и в принципе стирает временные и пространственные ограничения трансляции сцен насилия. Вдобавок меняются формы организаций таких сообществ и принципы их деятельности. От фанатичных сектантов и квази-государства до не имеющих в принципе никакой организованной структуры сверху политизированных радикалов, вышедших из молодежной культурной сцены. Как пример, можно при-

вести движения ультраправых скинхедов и их политических оппонентов «антифа», признанных в США в сентябре 2025 году указом президента Д.Трампа внутренней террористической организацией. В указе говорится о том, что «Антифа — это милитаристская, анархистская организация, которая открыто призывает к свержению правительства Соединенных Штатов, правоохранительных органов и нашей правовой системы. Она использует незаконные средства для организации и проведения кампании насилия и терроризма по всей стране для достижения этих целей». При этом очевидное недоумение вызывает факт отсутствия организации как таковой. По своей сути, антифа могут даже не исповедовать идеи анархизма, т.е. идеи антигосударственные. Участники таких сообществ могут позиционировать себя марксистами, субкультурщиками, радикальными экологами, либертарианцами и др., либо просто выйти на акцию протеста против преступлений на почве этнической ненависти. Отсутствуют как таковые лидеры, идейные программные документы и прочая составляющая механизма политической радикальной организации, соответствующей эпохам XIX-XX вв.

Однако, данные группировки не только нередко становятся участниками серьезных беспорядков, но и порождают индивидуальных террористов. Под идею антифашизма может мимикрировать экстремистская идеология ненависти. Медийное пространство их коммуникационных каналов выстраивает отчетливый конструкт противостояния с некоей «системой», под которой понимается государство, общество, рядовые граждане. Показателен пример «читинского» дела представителей движения антифа. 25 апреля 2024 года десятиклассницу Лизунову Л.* (Включена в перечень организаций и физических лиц, в отношении которых имеются сведения об их причастности к экстремистской деятельности или терроризму под номером 9669) и ее друга Снежкова А.* (Включен в перечень организаций и физических лиц, в отношении которых имеются сведения об их причастности к экстремистской деятельности или терроризму под номером 14990) признали виновными по обвинению в призывах к осуществлению террористической деятельности и экстремистской деятельности (ст.ст. 205.2, 280 УК РФ). Показателен заголовок BBC News: «За граффити «Смерть режиму» школьницу из Читы приговорили к трем с половиной годам колонии». Западные СМИ писали: «Молодых людей обвиняли в создании граффити «Смерть режиму», а также администрировании телеграм-каналов, где публиковались новости об «антивоенных акциях прямого действия» – в частности, о поджогах военкоматов» [5]. Подростки вели телеграм-каналы откровенно террористической тематики. Так, Лизунова описывала порядок действий при осуществлении террористического акта: «Рекомендуемый порядок действий таков: сначала вы закончили акцию, на которой вы сделали фото или видео, затем сразу же отправили по «полевому» телефону в безопасном мессенджере еще одному доверенному лицу... и т.д.». Помимо этого, контент каналов включал оправдание терроризма, в частности подрывы железных дорог и негативное отношение к ликвидации террористов, которых называли «несогласными». Незадолго до суда с Лизуновой и Снежковым вышло интервью на канале «Ромб» Youtube: «Когда мне было 14 лет и только начинала понимать свои взгляды, я

сожгла флаг России, завели административное дело, но ничего страшного не произошло... Я искала причины несправедливости и таким образом начинаешь ознакамливаясь с идеологиями, читать какую-то литературу, статьи, музыку слушать. Ищешь причины, находишь альтернативы. Примерно так знакомство с анархо-коммунизмом произошло. Когда ты в теории понимаешь, что да как, ты считаешь нужным проецировать взгляды на окружающих... Лично для меня анархизм всегда был высшей эволюцией человеческого сознания» [6]. Такого рода императивы характерны для сект и террористических сообществ: культ жертвенности и борьбы во имя некоей утопической идеи, следование которой занимает все больше времени. При этом идея, по мнению адепта, призвана помочь обществу. Но с самим этим обществом он находится в нереалистическом деструктивном противостоянии.

Не все участники этого неорганизованного движения выступили против внешнеполитического курса нашей страны. Показательны примеры музыкальных коллективов, участники которых открыто причисляют себя к сторонникам антифа и левых идей: Klowns (Россия), Banda Bassotti (Италия) и др., которые поддерживают население Донбасса в борьбе против геноцида, развязанного украинскими нацистами. Довольно тяжело отследить (если вообще возможно) статистику неорганизованного движения, отдельных представителей, сочувствующих лиц по их отношению к проводимой Россией специальной военной операции. Но можно уверенно утверждать, что работа спецслужбами недружественных государств проводится, существует большое количество т.н. антифашистов вовлеченных в антироссийскую повестку не только путем распространения материалов с сети Интернет и рисования политизированных граффити.

Украинские футбольные фанаты антифашистских взглядов Hoods Hoods Klan преобразовались в батальон в составе Сил территориальной обороны (ТСО) для борьбы с российскими вооруженными силами в 2022 году, сохранив цвета своего клуба в качестве боевого знамени. Это первое хулиганское формирование на Украине, официально объявившая себя антифа. НХК обрела свою окончательную форму в 2022 году. ННК входит в состав т.н. «Комитета Сопротивления», также известного как «Чёрный штаб», координационного органа ультралевых боевых группировок на СВО. Командир обеих организаций, Ю. Самойленко был уничтожен в сентябре 2022 года. ННК находится под командованием СБУ, но адресная поддержка также оказывается ультралевыми активистами и иными сочувствующими [7]. К одобрению политики Украины также пришли представители другого антифашистского фанатского сообщества – МТЗ РИПО из г.Минска, участники которого также отмечены в антироссийских формированиях. Показательны посты в телеграм-канале «Crust museum» («Электронный музей культуры краст панка»): «Забавно наблюдать, как вчерашние антифа, большей частью сталинисты и красносолевые активно легли под нацболов и пытаются переманить остатки антифа-движений на их сторону... Принимаем в музей футболку с изображением антифашистки из Украины, сражающейся на фронте против рузких фашистов» и прочее [8]. Бот принимает публикации с информацией, дискредитирующей вооруженные силы Россий-

ской Федерации, контент канала полон пейоративов в отношении антифашистов, которые поддерживают внешнюю политику России.

Другой информационный ресурс антифа – англоязычный «Good night imperial pride», названный по созвучию с популярным международным лозунгом антифашистов «Good night white pride», приглашает к теоретическому осмыслению проводимой Украиной политики: «Нарративы о крайне правом перевороте, об Украине как марионетке США и Европы, а также о притеснении русскоязычного населения активизировались именно тогда и продолжают продвигаться идеологами «русского мира» не только в России, но и за рубежом. 12 декабря мы встречаемся с исследователем Эмили Ченнел-Джастис, которая присутствовала на Майдане в 2013–2014 годах и брала интервью у левых активистов. Вместе мы рассмотрим формы самоорганизации, сформировавшиеся во время протестов, и то, как опыт Майдана и предыдущих протестных циклов повлиял на современный левый активизм в Украине. После лекции состоится дискуссия, в ходе которой мы обсудим центральный вопрос: как прогрессивные движения в Европе могут интерпретировать эти события исторически обоснованно и политически осмысленно?». Лекцию читает руководитель научной программы, посвященной современной Украине в Украинском научно-исследовательском институте Гарвардского университета доктор Эмили Ченнел-Джастис [9]. На странице университета приведена следующая информация о сотруднице: «Будучи социокультурным антропологом, она начала изучать украинский язык и проводить исследования в Украине в 2012 году. Занималась исследованиями политического активизма и социальных движений среди студентов и феминисток во время мобилизаций Евромайдана 2013 – 2014 гг. Автор этнографического труда «Без государства: самоорганизация и политический активизм в Украине» (Университет Торонто; 2022) и отредактированного тома «Декolonизация квир-опыта: ЛГБТ (В 2023 году Верховным судом Российской Федерации международное общественное движение ЛГБТ и его структурные подразделения признаны экстремистскими организациями и запрещена их деятельность на территории Российской Федерации) + нарративы из Восточной Европы и Евразии» [10]. Основанный в июне 1973 года научно-исследовательский институт при Гарвардском университете – HURI, занимается продвижением антироссийской повестки и трансляцией неолиберальных ценностей при помощи т.н. «мягкой силы». Сотрудникам и студентам оказывается финансовая поддержка : постдокторская стипендия Михайчука в размере 54 000 долларов США, исследовательские стипендии HURI OPEN-RANK – 24 000 долларов США, Выдающаяся стипендия имени Яцика – 35 000 долларов США и т.д. [11]

Мы полагаем, что сторонники украинских террористических формирований по достоинству оценят компетентность лекций доктора Эмили Ченнел-Джастис, рассказывающей про феминисток, гендеры и нетрадиционные половые отношения, но выражаем сомнение в актуальности данной повестки в деле профилактическое борьбы с неонацизмом как таковым.

Таким образом, для лиц, вовлеченных в такое децентрализованное движение как антифа, сформированы разные пути входа в активное противостоя-

ние государственной политики России. Это могут быть как субкультурные каналы музыкальной направленности, сообщества, где подростки транслируют поверхностную теоретическую аргументацию в пользу радикальных идей, так и ресурсы с дискурсивным контентом, с привлечением исследователей из академических кругов. К сожалению, под «независимыми» исследованиями могут скрываться догматические антироссийские установки и жесткая леволиберальная западная цензура. Развитие информационных технологий позволяет любому заинтересовавшемуся лицу с минимальными временными затратами ознакомиться с подобной информацией и как следствие быть вовлеченным в радикальные движения.

У лиц, с которыми систематические работали политтехнологи, культурные деятели и иные акторы невидимого идеологического фронта, появляется совершенное оружие – сознание, в которое вшит образ внешнего врага, идея жертвенности во имя идеи и готовность к бескомпромиссным жестоким действиям. Такого рода конфликт, в сочетании с другими угрозами (например, экономическим давлением, классическими военными действиями) называют гибридной войной. Одной из важнейших задач нашей системы образования всех уровней мы видим в том, чтобы не допускать распространения подобной информации среди обучающихся и сотрудников, дать достойный отпор не только на уровне организации профилактических мероприятий, но и в научных исследованиях. Гибридная война, с которой столкнулась наша страна не завершается в один победоносный удар и не зависит от мирных соглашений. Геополитическая реальность убеждает нас в том, что данный конфликт будет тянуться продолжительное время и победителем выйдет тот, чьи идеалы, духовные ценности и повседневный жизненный уклад окажутся в морально-этическом плане выше нежели у противника.

Список литературы

1. Красинский В.В. Трансформация международного терроризма в условиях влияния ключевых мегатрендов / В. В. Красинский // Мегатренды мировой политики: глобализация, поляризация, экстремизм : Сборник материалов Международной научно-практической конференции, Москва, 26–28 октября 2022 года. – Москва: Московский государственный лингвистический университет, 2023. – С. 66-75. EDN: ZSRKYJ

2. Хорган Д. Психология террориста: почему люди начинают убивать ради идеи. Columbia University Press This Russian language edition is a complete translation of the U.S. edition, specially authorized by the original publisher, Columbia University Press. Издание на русском языке, перевод, оформление. — М.: ООО «Альпина Паблишер», 2025. — 351 с.: ил.

3. Целунов А.Б. Что такое «Исламское государство Ирака и Леванта» (ИГИЛ) // РБК [Электронный ресурс] URL: <https://www.rbc.ru/base/11/03/2025/67cdc6a59a79473abb08ab87> (дата обращения: 01.12.2025)

4. Designating antifa as a domestic terrorist organization. Executive Orders. September 22, 2025. [Электронный ресурс] URL:

<https://www.whitehouse.gov/presidential-actions/2025/09/designating-antifa-as-a-domestic-terrorist-organization> (дата обращения: 01.12.2025)

5. BBC News. Русская служба. За граффити «Смерть режиму» школьницу из Читы приговорили к трем с половиной годам колонии. [Электронный ресурс] URL: <https://t.me/bbcruussian/64182> (дата обращения: 01.12.2025)

6. «Никто не хочет быть рабом» / Подростков-антифашистов хотят посадить из-за граффити «Смерть режиму» / Ромб. URL: https://www.youtube.com/watch?v=9CzBS871_l8 (дата обращения: 01.12.2025)

7. Modern insurgent. Hoods Hoods Klan (ННК). Mar 5, 2024. Antoine Guignard [Электронный ресурс] URL: <https://www.moderninsurgent.org/post/hoods-hoods-klan-hhk-1> (дата обращения: 01.12.2025)

8. Online museum of crust punk culture. [Электронный ресурс] URL: t.me/crustmuseum (дата обращения: 01.12.2025)

9. Good night imperial pride. [Электронный ресурс] URL: t.me/gnimperialpride (дата обращения: 01.12.2025)

10. Harvard university / Emily Channell-Justice Director, Temerty Contemporary Ukraine Program. [Электронный ресурс] URL: <https://www.huri.harvard.edu/people/emily-channell-justice> (дата обращения: 01.12.2025)

11. Harvard university / Fellowships. [Электронный ресурс] URL: <https://www.huri.harvard.edu/fellowships> (дата обращения: 01.12.2025)

MEDIA RESOURCES OF THE ANTIFA MOVEMENT IN THE ANTI-RUSSIAN AGENDA

A.R. Usmanov

Perm State University

Abstract. This article examines the information aspect of the activities of far-left extremist communities in the context of the armed conflict in modern Ukraine. It analyzes the information channels supporting the anti-Russian agenda and their narratives.

Keywords: *antifa, extremism, terrorism, special military operation, propaganda*

МЕТОДЫ ЗАЩИТЫ БИОМЕТРИЧЕСКОЙ ИНФОРМАЦИИ ЧЕЛОВЕКА

А.А. Федорочев, А.В. Черников

Пермский государственный национальный исследовательский университет

Аннотация. В работе рассматриваются современные подходы к обеспечению безопасности биометрических данных при их хранении и использовании. Показаны особенности биометрии как уникального идентификатора личности, рассмотрены риски утечки и компрометации. Приведён анализ действующей нормативно-правовой базы в Российской Федерации, описаны государственные инициативы в области биометрии, даны примеры практических методов защиты, включая криптографические средства, шифрование и распределённое хранение данных. Выделены перспективные направления развития защиты, такие как саморазвивающиеся биометрические шаблоны, контекстная аутентификация и шардирование.

Ключевые слова: *биометрия, защита данных, персональные данные, информационная безопасность.*

Введение

Биометрические технологии занимают ключевое место в современных системах идентификации и аутентификации. Среди них особое распространение получили методы распознавания лица, такие как FACE-ID, обеспечивающие высокий уровень удобства для пользователей и широкие возможности интеграции в распределённые информационные системы. Использование уникальных физиологических характеристик человека позволяет повысить надёжность проверки личности, но одновременно порождает новые вызовы в сфере безопасности и защиты персональных данных.

Хранение и использование биометрических данных требует особого подхода, так как в отличие от паролей или токенов биометрические признаки невозможно изменить при их компрометации. Утечка таких данных способна привести к необратимым последствиям и использованию их в злоумышленных целях. В этой связи разработка методов защиты биометрии становится критически важной задачей при проектировании и сопровождении современных информационных систем, особенно в условиях эксплуатации, где повышены риски несанкционированного доступа и внешнего воздействия.

Нормативная документация, действующая на территории РФ

Основными документами, регулирующими деятельность в области биометрии и методов ее защиты, а также наказания в случае несоблюдения этих правил являются:

1. 152 ФЗ - «О персональных данных» 11 Статья,

2. 572 ФЗ - «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных,

3. Постановление Правительства Российской Федерации от 6 июля 2008 г. № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных» [1],

4. Письмо Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 28 августа 2020 г. № ЛБ-С-074-24059 «О методических рекомендациях»,

5. 195 ФЗ КоАП РФ «Нарушение требований в области размещения биометрических персональных данных.

Согласно 152 ФЗ: **Биометрические персональные данные** – это данные, характеризующие биологические и физиологические особенности человека [2].

Согласно Письму Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 28 августа 2020: **Биометрические персональные данные** – это сведения, характеризующие физиологические и биологические особенности человека, на основе которых можно установить его личность и которые используются оператором для установления личности субъекта персональных данных [3].

Биометрические персональные данные будут являться таковыми при наличии условий:

1. Они признаны таковыми в силу положений нормативных правовых актов,

2. Они характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность,

3. Они используются оператором для установления личности субъекта персональных данных.

К биометрическим персональным данным относятся физиологические параметры (дактилоскопические данные, радужная оболочка глаз, анализы ДНК, рост, вес и др.) и иные физиологические или биологические характеристики человека, в том числе его изображения (фотография и видеозапись), в частности фотографические изображения обучающихся, сотрудников и посетителей организации, поскольку они характеризуют физиологические и биологические особенности человека.

Не относятся к биометрическим персональным данным:

1. Данные, полученные при сканировании паспорта оператором персональных данных для подтверждения осуществления определенных действий конкретным лицом (например, заключение договора на оказание услуг, в том числе банковских, медицинских и т.п.), т.е. без проведения процедур идентификации (установления личности);

2. Данные, полученные при осуществлении ксерокопирования документа, удостоверяющего личность,

3. Фотографическое изображение, содержащееся в личном деле работника,

4. Подпись лица, наличие которой в различных договорных отношениях является обязательным требованием, и почерк, в том числе анализируемый уполномоченными органами в рамках почерковедческой экспертизы,

5. Рентгеновские или флюорографические снимки, характеризующие физиологические и биологические особенности человека и находящиеся в истории болезни (медицинской карте) пациента (не имеет значения, бумажной или электронной), поскольку они не используются оператором (медицинским учреждением) для установления личности пациента,

6. Материалы видеосъемки в публичных местах и на охраняемой территории.

Отдельно рассматриваются общедоступные персональные данные - это сведения, доступные неограниченному кругу лиц, информация из открытых справочников, к которой доступ имеет любой желающий.

Обработка персональных данных

Обработка персональных данных должна соответствовать определенным целям, а обработка персональных данных, несовместимая с целями сбора персональных данных, не допускается [3].

Основополагающими началами обработки персональных данных являются заложенные в Законе о персональных данных принципы обработки персональных данных:

1. Обработка персональных данных на законной и справедливой основе;
2. Ограничение обработки персональных данных достижением конкретных, заранее определенных и законных целей;
3. Недопустимость обработки персональных данных, несовместимой с целями сбора персональных данных;
4. Обработка персональных данных, которые отвечают целям их обработки;
5. Соответствие содержания и объема обрабатываемых персональных данных заявленным целям обработки;
6. Исключение обработки персональных данных, являющихся избыточными по отношению к заявленным целям их обработки;
7. Удаление биометрических персональных данных по завершении срока их хранения или использования

Выделяют несколько способов обработки персональных данных [3]:

1. Автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники;
2. Неавтоматизированная обработка персональных данных -
3. Смешанная обработка персональных данных.

Критерии обработки персональных данных без использования средств автоматизации установлены Постановлением Правительства РФ от 15.09.2008 N 687, утвердившим Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации.

Единая биометрическая система

В ЕБС для идентификации используются одновременно два параметра — голос и лицо (фотоизображение лица человека) [4]. Система является одним из ключевых элементов механизма удалённой идентификации, позволяющего гражданам дистанционно получать финансовые услуги, она работает в тесной взаимосвязи с Единая система идентификации и аутентификации (ЕСИА).

С 30 сентября 2023 года ЕБС - единственный в РФ оператор биометрии. Ему были переданы все биометрические данные, накопленные банками, операторами связи и иными владельцами биометрических данных граждан России.

За все время работы ЕБС её высокая степень защищённости системы и надёжности распознавания (идентификации) позволяют банкам использовать ЕБС в том числе и как инструмент борьбы с таким распространённым видом мошенничества, как получение кредита по подложному или украденному паспорту. Каждый год ЕБС помогает банкам сберечь более 10 млрд. рублей, которые в ином случае достались бы мошенникам.

Несмотря на то, что система существует с 2019 года, граждане РФ не спешат подавать заявки со своей биометрией в данную сферу.

Отдельно стоит обозначить тот факт, что все мигранты при прибытии в страну, а также все военнослужащие в РФ в обязательном порядке сдают полную биометрию [5]:

1. Отпечатки всех пальцев, ладоней рук и стоп ног.
2. Биометрический скан лица
3. Запись голоса человека.

Несмотря на существующие проблемы, включая риски подмены биометрических параметров с использованием технологий deepfake, сфера биометрии продолжит активно развиваться. Это связано с тем, что биометрия остаётся одним из самых удобных и эффективных инструментов государственного контроля. Для обычного гражданина такое развитие, как правило, не несёт серьёзных угроз и сопровождается определёнными преимуществами — в частности, упрощением доступа к различным услугам в обмен на предоставление биометрических данных.

Кодирование биометрии

Помимо общих теоретических положений, важно рассмотреть биометрию в практическом контексте — с точки зрения программных средств и технических комплексов, обеспечивающих её сбор, обработку и применение.

В большинстве устройств, генерируемая биометрия выглядит следующим образом [3,6]:

[0.45672, 0.89214, 0.37185, 0.64729, 0.21347, 0.58963, 0.73482, 0.12894, 0.96231, 0.30576, 0.48125, 0.67914, 0.82467, 0.25739, 0.39718 ...]

Причина подобного представления заключается в том, что это числовые векторы, отражающие биометрические признаки, — так называемые биометри-

ческие шаблоны (или шаблоны признаков). При сканировании лица, отпечатка пальца, радужной оболочки глаза или при регистрации голосового образца, устройство не сохраняет визуальное изображение или аудиофайл. Вместо этого проводится математическая обработка полученной информации, в результате которой выделяются уникальные характеристики, представляемые в виде числовых векторов.

Каждый элемент такого вектора отражает значение конкретного параметра, например, расстояние между ключевыми точками лица, текстурные особенности отпечатка, спектральные характеристики голоса и т.п. Полученные данные проходят процесс нормализации и преобразуются в векторы с элементами типа float, находящимися в диапазоне от 0 до 1. Это обеспечивает возможность удобного сопоставления биометрических шаблонов и ускоряет процесс аутентификации.

Подобный формат является универсальным, стандартизированным и легко обрабатывается вычислительными системами. Он компактен, не содержит визуальной или аудиальной информации, что способствует обеспечению конфиденциальности, и обеспечивает эффективный поиск и сравнение данных в биометрических базах.

Наиболее распространёнными являются следующие типы биометрии, для которых описанный векторный формат является основным способом представления данных [3,6]:

1. Биометрия лица,
2. Отпечатки пальцев, ладоней,
3. Радужки / Сетчатки глаза,
4. Голос (требует отдельной обработки).

Размер генерируемых точек может отличаться в зависимости от требуемой точности или настройки самого прибора, условий его эксплуатации.

Биометрия, интегрируемая в ЕБС, собирается с максимальной точностью допустимой прибором измерения.

Отдельного рассмотрения заслуживает вопрос хранения и обработки так называемой «нестандартной» биометрической информации — в частности, голосовых данных. В отличие от более традиционных биометрических признаков, таких как отпечатки пальцев или изображение лица, голос характеризуется высокой вариативностью, зависимостью от условий записи, шумов и физиологических изменений. Эти особенности требуют специфических подходов к представлению, структурированию и защите голосовых шаблонов, отличных от классических векторных моделей, применяемых для статичных биометрических признаков.

Мел-частотные кепстральные коэффициенты (MFCC)

Аудиосигнал делится на последовательность коротких временных фреймов длительностью 20–40 мс. Из каждого фрейма извлекаются 12–20 мел-частотных кепстральных коэффициентов (MFCC), отражающих спектральные характеристики речи в форме, приближённой к восприятию звука человеческим

ухом. Результатом обработки является матрица, в которой каждая строка соответствует одному фрейму и содержит набор вычисленных коэффициентов.

Для повышения точности анализа используется частичное перекрытие фреймов: каждый следующий формируется с шагом, равным примерно половине длины предыдущего. Это позволяет улучшить устойчивость к шуму и сохранить непрерывность признаков.

Результат — матрица коэффициентов:

```
[  
[12.13, 5.27, ..., 3.91],  
[11.76, 5.81, ..., 4.22],  
]
```

Спектрограмма / мел-спектрограмма

Спектрограмма или мел-спектрограмма представляет голосовой сигнал в виде двумерного массива, где горизонтальная ось соответствует времени, вертикальная — частотным компонентам, а интенсивность сигнала передаётся через цветовую яркость или числовые значения амплитуд. Матрица спектрограммы может сохраняться как изображение либо как массив, в котором каждая строка отражает частотное распределение сигнала в рамках одного временного фрейма длительностью 20–40 мс.

```
[  
[0.1, 0.3, ..., 0.8],  
[0.2, 0.5, ..., 0.6],  
]
```

Обработка биометрических и других данных

Любая система хранения биометрических данных по своей природе является распределённой [7]. Это накладывает дополнительные сложности на процессы передачи и синхронизации этих данных между различными узлами системы. В таких системах информация может быть распределена по множеству серверов, что требует чёткого регулирования механизмов доступа и обмена данными. В условиях российского законодательства, а именно с учётом положений Кодекса об административных правонарушениях (КоАП РФ), эти сложности ещё больше усугубляются, поскольку нарушение норм, регулирующих обработку и передачу персональных данных, может привести к юридическим последствиям. В частности, множественная передача биометрических данных без должного контроля и соблюдения нормативных требований фактически становится незаконной, что ставит под угрозу как безопасность данных, так и соблюдение прав граждан [3,6].

В общем случае при работе с биометрическими данными и устройствами, считывающими их, применяется следующая схема:

1. Биометрические данные пользователя считываются устройством

2. В случае если сеть имеет «Сертификат соответствия требованиям безопасности информации», данную информацию можно передавать в рамках внутренней сети в централизованную базу, где хранится и обрабатывается информация организации. В ином случае – нигде не сохраняется, используется лишь при обработке на устройстве.

3. Полученная информация преобразуется в уникальный идентификационный номер (UUID или GUID) следующего вида:

xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx

Это стандарт, определённый в RFC 4122. UUID используется для создания уникальных идентификаторов в распределённых системах и базах данных, где важно, чтобы идентификатор был уникальным в глобальном масштабе.

Полученный таким образом номер уже не является биометрическими данными и может быть передан по сети интернет для хранения в распределённых базах данных.

В случае проведения аутентификации при помощи биометрии выполняются следующие действия:

1-3 пункты повторяются устройством.

4. Если в локальной базе данных отсутствуют данные об данном пользователе (UUID не совпал ни с чем), то отправляется запрос с подобным UUID в распределённую базу данных, на что получается ответ о допуске или нет. В случае же ЕБС локальная база не используется.

Подобный подход является универсальным и используется в большинстве случаев.

Методы защиты информации при ее передаче и хранении

С увеличением объема данных и распространением технологий, требующих обработки и хранения персональной информации, включая биометрические данные, встает задача обеспечения надежной защиты этих данных. Для защиты информации при передаче и хранении применяются различные методы и технологии, включая средства криптографической защиты, шифрование данных и общепринятые методики защиты информации.

СКЗИ — это средства, предназначенные для защиты информации с помощью криптографических методов, таких как шифрование, цифровая подпись, защита целостности и аутентификация. В зависимости от требуемого уровня безопасности, можно выбрать программные и аппаратные решения.

Программные СКЗИ. Программные средства защиты обычно доступны по цене и широко используются для обеспечения безопасности данных в небольших и средних организациях. Эти системы обеспечивают защиту информации на уровне программных приложений и серверов.

• **VipNet** — одно из популярных решений для защиты данных в корпоративных сетях. Стоимость лицензии может достигать до 10 000 рублей за копию. VipNet предоставляет криптографическую защиту для передачи данных и

аутентификации пользователей, поддерживая шифрование на уровне канала передачи данных.

- **КриптоАРМ** — система для защиты персональных данных, которая применяется в системах документооборота и для криптографической подписи документов. Стоимость также укладывается в рамки до 10 000 рублей за копию.

- **КриптПРО** — одно из ведущих решений на российском рынке для цифровой подписи и шифрования данных. Оно используется для защиты различных типов информации, включая биометрические данные, в соответствии с требованиями российского законодательства.

Эти решения обеспечивают надежную защиту данных в пределах локальных сетей, но их функциональность и уровень защиты ограничены программными средствами, что может быть недостаточным для защиты особо чувствительных данных.

Аппаратные СКЗИ. Для более высокоуровневой защиты, особенно для данных, которые требуют повышенной безопасности, применяются аппаратные средства защиты. Такие устройства обеспечивают хранение криптографических ключей в защищённых хранилищах, а также шифрование и дешифрование данных непосредственно на аппаратном уровне.

- **Континент и Квazar** - примеры аппаратных средств криптографической защиты, используемых для защиты данных на уровне устройств. Эти решения часто применяются в государственных учреждениях или крупных корпорациях, где требуется высокая степень защиты. Стоимость таких устройств начинается от 1 миллиона рублей за штуку и растет в зависимости от функционала и уровня безопасности.

Аппаратные средства криптографической защиты предоставляют наибольшую безопасность, так как они исключают возможность извлечения криптографических ключей или других чувствительных данных при попытке несанкционированного доступа.

Шифрование данных

Одним из ключевых методов защиты данных является шифрование, которое позволяет обеспечить конфиденциальность информации как при ее передаче, так и при хранении.

HTTPS — это протокол, который используется для защищенной передачи данных по сети Интернет. Он использует SSL/TLS для шифрования данных, передаваемых между клиентом и сервером, что исключает возможность перехвата и дешифровки информации третьими лицами. HTTPS является стандартом для защиты любых данных, включая биометрические, в процессе их передачи через Интернет [8].

VPN. Они представляет собой технологию, позволяющую создавать защищённые каналы для передачи данных через публичные сети, такие как Интернет. VPN использует шифрование для защиты передаваемых данных, что делает его полезным инструментом для безопасной передачи биометрической информации между удаленными серверами или клиентами. VPN не только

шифрует данные, но и скрывает реальный IP-адрес, обеспечивая дополнительную анонимность [9].

Хеширование данных — это процесс преобразования исходных данных в фиксированную строку символов (хеш), которая является представлением этих данных. Хеширование необратимо, то есть из хеша невозможно восстановить исходные данные. Это метод, который часто применяется для защиты биометрии, например, при хранении биометрических шаблонов. Вместо хранения самих биометрических данных, хранятся только их хеши, что делает невозможным восстановление оригинальных данных в случае утечки базы данных.

Общепринятые методики защиты биометрии

Для защиты биометрических данных, которые являются крайне чувствительными, существует ряд методик, направленных на минимизацию рисков их утечки и использования третьими лицами [10].

- **Локальное хранение данных [11]**

- Классификацию и маркировку биометрических шаблонов для применения адекватных мер защиты

- Шифрование данных «at rest» и «in transit» с использованием сертифицированных криптографических алгоритмов

- Управление доступом по принципу наименьших привилегий и сегментацию хранилищ

- Применение аппаратных модулей безопасности (HSM) для защиты криптографических ключей

- Аудит и мониторинг операций доступа к биометрическим данным

- Безопасное удаление и уничтожение устаревших или избыточных шаблонов в соответствии с регламентом жизненного цикла информации [3].

Методы защиты биометрических данных при хранении и использовании актуальны по трем ключевым причинам:

1. **Неизменяемость и долговременность данных:**

Биометрические характеристики (отпечатки, лицо, радужка, голос) неизменно привязаны к человеку. В случае утечки обычные средства (смена пароля, блокировка карты) бессильны — скомпрометированный шаблон остаётся навсегда. Поэтому механизмы защиты на этапе формирования, хранения и передачи должны быть на порядок надёжнее традиционных [12].

2. **Роль государства:**

Оператор - государство организует и управляет масштабными проектами по сбору и обработке биометрических данных, включая Единую биометрическую систему (ЕБС) и цифровую идентификацию. Это делает его активным участником всех этапов работы с биометрией [13].

Регулятор – государство формирует законодательную базу, регулирующую обращение с биометрическими данными. При этом нормативные акты зачастую включают исключения, позволяющие самому государству и его сило-

вому аппарату обходить установленные ограничения там, где это необходимо [14,15].

Бенефициар - получая прямой доступ к биометрическим данным, государство использует их для повышения эффективности предоставления цифровых услуг, контроля и обеспечения безопасности [16].

Политический и стратегический субъект - защита биометрических данных становится не только задачей информационной безопасности, но и элементом цифровой политики. Это напрямую влияет на уровень доверия к государственной инфраструктуре и воспринимается как инструмент обеспечения национальной безопасности [13].

3. Удобство и массовое применение

Биометрическая идентификация стала повсеместным стандартом в таких сферах, как оплата услуг, здравоохранение, государственные сервисы, логистика и образование. Её использование упрощает доступ к системам, устраняет необходимость запоминания паролей, ускоряет обслуживание и позволяет автоматизировать рутинные задачи, тем самым повышая эффективность использования человеко-часов.

Высокий уровень удобства способствует стремительному росту охвата: несмотря на риски, связанные с добровольной передачей биометрических данных государству, всё больше граждан начинают пользоваться услугами биометрии. Параллельно бизнес активно развивает стартапы и решения, работающие на границе правового регулирования биометрии. Например, размещение фотографий сотрудников в интернете позволяет считать передачу фотографий по сети обычными персональными данными [5].

Основные направления решения вопроса безопасности биометрических данных

Одним из ключевых направлений решения проблем в области защиты биометрической информации выступает нормативно-правовое регулирование. На сегодняшний день законодательная база в этой сфере состоит из фрагментарных норм, содержащихся в различных федеральных законах, подзаконных актах и ведомственных методических рекомендациях, и постановлениях, затрудняющее понимание общей картины. Такое положение создаёт правовую неопределённость, особенно в вопросах определения объёма и характера биометрических данных, условий их обработки, передачи и хранения

На этом фоне необходимость в отдельном, специализированном Федеральном законе становится особенно актуальной. Такой закон должен централизованно закрепить понятийный аппарат: что считается биометрией, какие технологии попадают под регулирование, в каких условиях допускается обработка без согласия субъекта, и каким требованиям должны соответствовать системы хранения и обработки биометрической информации. Это позволит устранить существующие правовые лакуны и обеспечить единообразие в трактовке норм.

В рамках такого закона важно определить единые требования к информационной безопасности, регламентировать применение технологий криптогра-

фической защиты, обеспечить независимый аудит систем хранения, ввести обязательную сертификацию решений, обрабатывающих биометрические данные, а также определить степень ответственности субъектов за утечку, неправомерную обработку и несанкционированный доступ. Дополнительно, необходимо предусмотреть исключения и особые режимы, например, при применении биометрии в рамках государственных сервисов и в целях национальной безопасности, при этом сохранив баланс между интересами государства и правами граждан.

Таким образом, правовая унификация и систематизация требований к обработке и защите биометрических данных выступает базовым направлением, без которого невозможно обеспечить как безопасность, так и доверие к биометрическим технологиям. Это направление требует приоритетного внимания со стороны законодателя, с участием технических экспертов, юристов и представителей гражданского общества.

Другим важным направлением в решении вопросов защиты биометрической информации является разработка новых методов хранения данных. В отличие от правовой составляющей, эта область находится в постоянной эволюции, поскольку с развитием технологий появляются новые способы считывания биометрических данных, что требует соответствующих изменений в методах их хранения. Рассмотрим их ниже.

Саморазвивающиеся биометрические шаблоны

При каждой успешной аутентификации система сравнивает новый образ биометрии пользователя с текущим шаблоном. Если совпадение подтверждено, шаблон обновляется постепенно, используя веса, которые определяют, насколько новые данные влияют на старые значения: каждый элемент шаблона обновляется как комбинация старого и нового значения с учётом веса. Исторические версии сохраняются для отката в случае ошибок или атак. Шаблон остаётся защищённым криптографически или в защищённом хранилище устройства. Это позволяет учитывать естественные изменения биометрии пользователя со временем, обеспечивая постепенное эволюционирование шаблона.

Контекстная аутентификация при помощи биометрии

Система связывает биометрический шаблон с текущим контекстом, например устройством, местоположением или временем. Для успешной аутентификации необходимо, чтобы и биометрия, и контекст совпадали с ожидаемыми параметрами. Если контекст не совпадает, доступ блокируется, даже при корректной биометрии. Контекст проверяется автоматически, без действий пользователя. Это повышает безопасность без ухудшения удобства.

Шардирование биометрических данных

Биометрический шаблон делится на несколько фрагментов, каждый из которых шифруется и хранится в отдельном месте. Для аутентификации необходимо собрать все фрагменты и объединить их в целостный шаблон. Один украденный фрагмент не позволяет восстановить исходные данные. Процесс проис-

ходит прозрачно для пользователя, который просто проходит обычное сканирование. Это значительно снижает риск компрометации биометрических данных.

Заключение

В результате проведенной работы были исследованы вопросы защиты биометрических данных. Область защиты биометрических данных, на сегодняшний день, проработана не полностью. Необходимо в дальнейшем более подробно уделять внимание как правовым аспектам, так и техническим в защите биометрических данных.

Список литературы

1. Импортозамещение в ИТ: вызовы и перспективы [Электронный ресурс] // Habr. URL: <https://habr.com/ru/articles/599671/> (дата обращения: 17.04.2025).
2. Импортозамещение вычислительной техники и микроэлектроники [Электронный ресурс] // TAdviser. URL: https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%98%D0%BC%D0%BF%D0%BE%D1%80%D1%82%D0%BE%D0%B7%D0%B0%D0%BC%D0%B5%D1%89%D0%B5%D0%BD%D0%B8%D0%B5_%D0%B2%D1%8B%D1%87%D0%B8%D1%81%D0%BB%D0%B8%D1%82%D0%B5%D0%BB%D1%8C%D0%BD%D0%BE%D1%8F_%D1%82%D0%B5%D1%85%D0%BD%D0%B8%D0%BA%D0%B8_%D0%B8_%D0%BC%D0%B8%D0%BA%D1%80%D0%BE%D1%8D%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%B8%D0%BA%D0%B8 (дата обращения: 17.04.2025).
3. Импортозамещение в системах безопасности и ИТ [Электронный ресурс] // Secuteck. URL: <https://www.secuteck.ru/articles/importozameshchenie-v-sistemah-bezopasnosti-i-it-vremya-vozmozhnostej-dlya-otchestvennyh-proizvoditelej-i-razrabotchikov> (дата обращения: 17.04.2025).
4. Официальный сайт компании Микрон [Электронный ресурс] // Mikron. URL: <https://mikron.ru/> (дата обращения: 17.04.2025).
5. Stuxnet [Электронный ресурс] // Wikipedia. URL: <https://ru.wikipedia.org/wiki/Stuxnet> (дата обращения: 17.04.2025).
6. Импортозамещение в России: как это работает на практике [Электронный ресурс] // Habr. URL: <https://habr.com/ru/articles/796971/> (дата обращения: 17.04.2025).
7. Эльбрус-4С [Электронный ресурс] // Wikipedia. URL: <https://ru.wikipedia.org/wiki/%D0%AD%D0%BB%D1%8C%D0%B1%D1%80%D1%83%D1%81-4%D0%A1> (дата обращения: 17.04.2025).
8. Ангстрем (компания) [Электронный ресурс] // Wikipedia. URL: [https://ru.wikipedia.org/wiki/%D0%90%D0%BD%D0%B3%D1%81%D1%82%D1%80%D0%B5%D0%BC_\(%D0%BA%D0%BE%D0%BC%D0%BF%D0%B0%D0%BD%D0%B8%D1%8F\)](https://ru.wikipedia.org/wiki/%D0%90%D0%BD%D0%B3%D1%81%D1%82%D1%80%D0%B5%D0%BC_(%D0%BA%D0%BE%D0%BC%D0%BF%D0%B0%D0%BD%D0%B8%D1%8F)) (дата обращения: 17.04.2025).
9. ЭЛВИС НПЦ (Электронные вычислительно-информационные системы) [Электронный ресурс] // TAdviser. URL:

[https://www.tadviser.ru/index.php/%D0%9A%D0%BE%D0%BC%D0%BF%D0%B0%D0%BD%D0%B8%D1%8F:%D0%AD%D0%9B%D0%92%D0%98%D0%A1_%D0%9D%D0%9F%D0%A6_\(%D0%AD%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%BD%D1%8B%D0%B5_%D0%B2%D1%8B%D1%87%D0%B8%D1%81%D0%BB%D0%B8%D1%82%D0%B5%D0%BB%D1%8C%D0%BD%D0%BE-%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D1%8B%D0%B5_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D1%8B\)](https://www.tadviser.ru/index.php/%D0%9A%D0%BE%D0%BC%D0%BF%D0%B0%D0%BD%D0%B8%D1%8F:%D0%AD%D0%9B%D0%92%D0%98%D0%A1_%D0%9D%D0%9F%D0%A6_(%D0%AD%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%BD%D1%8B%D0%B5_%D0%B2%D1%8B%D1%87%D0%B8%D1%81%D0%BB%D0%B8%D1%82%D0%B5%D0%BB%D1%8C%D0%BD%D0%BE-%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D1%8B%D0%B5_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D1%8B)) (дата обращения: 17.04.2025).

10. Проблематика импортозамещения в производстве РЭА и ПО [Электронный ресурс] // СТА. URL: <https://www.cta.ru/articles/soel/2023/2023-6/169590/> (дата обращения: 17.04.2025).

11. Федеральные законы и постановления [Электронный ресурс] // Consultant. URL: <https://www.consultant.ru/> (дата обращения: 17.04.2025).

12. Список микропроцессоров Core i7 [Электронный ресурс] // Wikipedia. URL: https://ru.wikipedia.org/wiki/%D0%A1%D0%BF%D0%B8%D1%81%D0%BE%D0%BA_%D0%BC%D0%B8%D0%BA%D1%80%D0%BE%D0%BF%D1%80%D0%BE%D1%86%D0%B5%D1%81%D1%81%D0%BE%D1%80%D0%BE%D0%B2_Core_i7 (дата обращения: 17.04.2025).

13. Электронная промышленность (рынок России) [Электронный ресурс] // TAdviser. URL: [https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%AD%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%BF%D1%80%D0%BE%D0%BC%D1%8B%D1%81%D0%BB%D0%B5%D0%BD%D0%BD%D0%BE%D1%81%D1%82%D1%8C_\(%D1%80%D1%8B%D0%BD%D0%BE%D0%BA_%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D0%B8\)](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%AD%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%BF%D1%80%D0%BE%D0%BC%D1%8B%D1%81%D0%BB%D0%B5%D0%BD%D0%BD%D0%BE%D1%81%D1%82%D1%8C_(%D1%80%D1%8B%D0%BD%D0%BE%D0%BA_%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D0%B8)) (дата обращения: 17.04.2025).

14. Intel Management Engine [Электронный ресурс] // Wikipedia. URL: https://ru.wikipedia.org/wiki/Intel_Management_Engine (дата обращения: 17.04.2025).

15. TSMC вложит в производство чипов \$100 млрд [Электронный ресурс] // РБК. URL: <https://www.rbc.ru/quote/news/article/606586539a79475feb1f8a2c?from=copy> (дата обращения: 17.04.2025).

16. Baikal-T1 [Электронный ресурс] // Wikipedia. URL: <https://ru.wikipedia.org/wiki/Baikal-T1> (дата обращения: 17.04.2025).

METHODS OF PROTECTING HUMAN BIOMETRIC INFORMATION

A.A. Fedorochev, A.V. Chernikov

Perm State University

Abstract. The paper discusses modern approaches to ensuring the security of biometric data during its storage and use. It highlights the features of biometrics as a unique personal identifier and examines the risks of data leakage and compromise. The paper provides an analysis of the current regulatory framework in the Russian Federation, describes government initiatives in the field of biometrics, and provides examples of practical methods for protecting data, including cryptographic tools, encryption, and distributed data storage. The paper also highlights promising areas for developing security measures, such as self-learning biometric templates, contextual authentication, and sharding.

Keywords: *biometrics, data protection, personal data, and information security.*

СОВРЕМЕННЫЕ МЕТОДЫ СТЕГАНОАНАЛИЗА И ЗАЩИТА ОТ СТЕГАНОГРАФИЧЕСКИХ АТАК

И.Н. Хиривимский, А.П. Шкарапута

Пермский государственный национальный исследовательский университет

Аннотация. Статья посвящена сравнительному анализу современных методов стеганографии и стегоанализа. Рассмотрены принципы работы базовых алгоритмов сокрытия информации: LSB-методов, подходов на основе дискретного косинусного преобразования (DCT), а также методов, использующих избыточность форматов. Проанализированы сценарии вредоносного применения стеганографии (внедрение вредоносного кода, скрытая эксфильтрация данных) и соответствующие методы противодействия: визуальный анализ, статистические тесты (включая метод хи-квадрат Вестфельда–Пфитцмана) и подходы на основе машинного обучения. Показано, что эффективность статистических методов существенно снижается при использовании адаптивных схем внедрения с псевдослучайным распределением данных, что актуализирует задачу разработки гибридных детекторов. Обсуждаются ограничения современных DLP-систем в части обнаружения стегоконтейнеров и перспективы их интеграции с алгоритмами стегоанализа. Приведён обзор правового регулирования стеганографии в РФ и сформулированы рекомендации по совершенствованию нормативной базы. На основе проведённого анализа сделан вывод о необходимости комплексного подхода, сочетающего технологические инновации, правовые механизмы и подготовку кадров.

Ключевые слова: *стеганография, стегоанализ, LSB, DCT-методы, метод хи-квадрат, обнаружение внедрений, скрытые каналы передачи данных, информационная безопасность, DLP-системы, цифровые водяные знаки, имперцептивность.*

Введение

Стеганография — наука и практика сокрытия информации, ключевой особенностью которой является маскировка самого факта передачи данных, в отличие от криптографии, обеспечивающей конфиденциальность содержания за счет криптографических преобразований.

На данный момент времени стеганографические методы характеризуются тремя основными параметрами: ёмкостью канала, имперцептивностью (незаметностью внедрения) и робастностью (устойчивостью к обработке контейнера).

Актуальность темы обусловлена ростом использования методов стеганографии в кибератаках с помощью скрытой эксфильтрации данных и обхода средств периметральной защиты. Так, например, в 2024 году APT-группировка PhaseShifters (Sticky Werewolf) атаковала российские компании с

помощью стеганографических методов. При этом традиционные средства защиты (антивирусы, сигнатурные IDS/DLP) оказываются низкоэффективными против адаптивных стегоалгоритмов, что формирует запрос на развитие методов стегоанализа. В работе проводится сравнительный анализ современных методов обнаружения стеганографических внедрений в цифровых изображениях и аудиофайлах, оценивается их эффективность скорости анализа и устойчивости к адаптивным атакам.

Принципы работы и классификация методов стеганографии

В основе современной цифровой стеганографии лежит компромисс между тремя ключевыми параметрами: ёмкостью канала (объем внедряемых данных), имперцептивностью (незаметностью изменений для человеческого восприятия) и робастностью (устойчивостью к обработке контейнера, например, сжатию или масштабированию). Усиление одного параметра, как правило, ведет к ослаблению других.

По типу области внедрения методы можно разделить на две основные группы:

1. Методы пространственной области (Spatial Domain). Здесь данные внедряются непосредственно в значения пикселей или сэмплов.
2. Методы частотной области (Frequency Domain). Контейнер предварительно преобразуется (например, с помощью ДКП или вейвлет-преобразования), и данные внедряются в коэффициенты преобразования.

Наиболее распространенным методом пространственной области является LSB-стеганография (Least Significant Bit). Секретные данные записываются в младшие значащие биты байтов контейнера. Поскольку изменение МЗБ минимально влияет на цвет пикселя или амплитуду звука, визуальные артефакты практически незаметны. Ёмкость включений составляет от 1-го до 4-х бит на 1 байт контейнера, так как замена большего числа бит приводит к большой статистической неестественности и наличию визуальных артефактов. Метод крайне чувствителен к обработке изображений (сжатие JPEG, изменение размера) и легко обнаруживается статистическими методами (например, анализом хи-квадрат).

Методы на основе дискретного косинусного преобразования (DCT) Широко применяются для форматов с потерями (например, JPEG). Изображение разбивается на блоки 8×8 и каждый блок подвергается ДКП. Данные внедряются в среднечастотные коэффициенты (AC-коэффициенты), так как низкочастотные (DC) отвечают за общую яркость и их изменение заметно. Высокочастотные же теряются при сжатии. Основное преимущество таких методов - высокая робастность к сжатию JPEG. Недостатки - ёмкость канала обычно ниже, чем у LSB, а алгоритмическая сложность выше.

Ниже приведены ещё четыре распространенных метода стеганографии.

Текстовая стеганография — наиболее сложный вид из-за низкой избыточности текста. Основные её подходы:

- Форматирование: Изменение межсловных интервалов, использование невидимых символов (Zero-Width Space).

- Лингвистические методы: Замена слов синонимами, генерация текста по грамматическим правилам. Часто приводят к стилистическим аномалиям, detectable при лингвистическом анализе.

Сетевая (протокольная) стеганография строится на основе использования избыточности сетевых протоколов (TCP/IP). Данные могут скрываться в полях заголовков (например, поле Identification в IP, Sequence Number в TCP), которые не влияют на маршрутизацию, либо в временных интервалах между пакетами (timing channels). Особенность данного подхода - высокая скорость передачи, но данные теряются при завершении сессии. Уязвима к нормализации трафика.

Методы расширенного спектра (Spread Spectrum Steganography). Принцип данного метода заключается в том, что сигнал скрытого сообщения распределяется по широкому частотному диапазону контейнера с низкой энергией, имитируя шум. У данного подхода высокая стойкость к попыткам обнаружения и удаления (робастность), так как сигнал скрыт ниже уровня шума контейнера. К недостаткам относится низкая ёмкость и высокая вычислительная сложность кодирования/декодирования.

Соккрытие в служебных полях (Header Manipulation) Внедрение данных в метаданные файла (EXIF, комментарии PNG, поля заголовков). Так как представленный метод не является стойким, то многие средства защиты (файрволы, DLP) автоматически очищают метаданные или проверяют целостность структуры файла.

Применение, угрозы и средства противодействия

Стеганография является двойственной технологией. Легитимные сценарии использования включают защиту авторских прав (цифровые водяные знаки), скрытие метаданных в системах документооборота, обеспечение конфиденциальности связи в условиях цензуры, а также оперативно-розыскную деятельность.

Вредоносное применение стеганографии в киберпространстве осуществляется по трем основным направлениям:

- Скрытая доставка вредоносного ПО (Droppers): Полезная нагрузка внедряется в легитимные медиафайлы (изображения, документы), что позволяет обходить сигнатурный анализ антивирусов.

- Эксфильтрация данных: Конфиденциальная информация разбивается на части и скрыто передается во внешнюю сеть внутри исходящего трафика (например, в изображениях, загружаемых на файлообменники).

- Каналы командования и управления: Зараженные узлы получают инструкции от сервера злоумышленника через скрытые данные в публичном контенте (например, в рекламных баннерах или обновлениях ПО), что усложняет блокировку командных серверов.

Традиционные средства защиты (антивирусы, сетевые экраны) малоэффективны против стегоконтейнеров, так как файл формально остается валидным. Для противодействия применяются специализированные методы стегоанализа.

1. Визуальный анализ — метод, основанный на визуализации младших

значащих битов (МЗБ) цветowych плоскостей. В естественном изображении МЗБ-плоскость содержит структурированный шум, отражающий контуры объектов. В стегоконтейнере (при использовании LSB) эта плоскость превращается в случайный белый шум с высокой энтропией (Рис. 1, 2).



Рис.1. Исходное изображение (Стив Джобс)

Необходимо отметить, что при анализе требуется участие эксперта и автоматизация затруднена. Кроме того, данный метод применим только для несжатых форматов (BMP, PNG, RAW). Для JPEG и других форматов с потерями визуальный анализ неэффективен.



Рис.2. Результат визуальной атаки на изображение (Red plane 7 — старший бит красного канала, который хранит основную форму изображения; Red plane 0 — МЗБ-плоскость красного канала; Random colour map 2 — визуализация битовой плоскости с псевдоцветами для лучшей визуализации структуры)

2. Статистический анализ (метод хи-квадрат) — наиболее известный алгоритмический метод обнаружения LSB-внедрений. Метод анализирует распределение частот пар «цветов-близнецов» оттенков, отличающихся только значением МЗБ (например, 010 и 011). Так в естественном изображении частоты встречаемости цветов в паре существенно различаются из-за естественной корреляции соседних пикселей (Рис. 3а). В стегоконтейнере внедрение случайных битов сообщения выравнивает частоты в парах, стремясь к равномерному распределению (Рис. 3б). Для обнаружения включений вычисляется статистика χ^2 (хи-квадрат). Низкое значение статистики указывает на то, что распределение пар цветов является искусственно выровненным, что служит индикатором наличия скрытого сообщения.

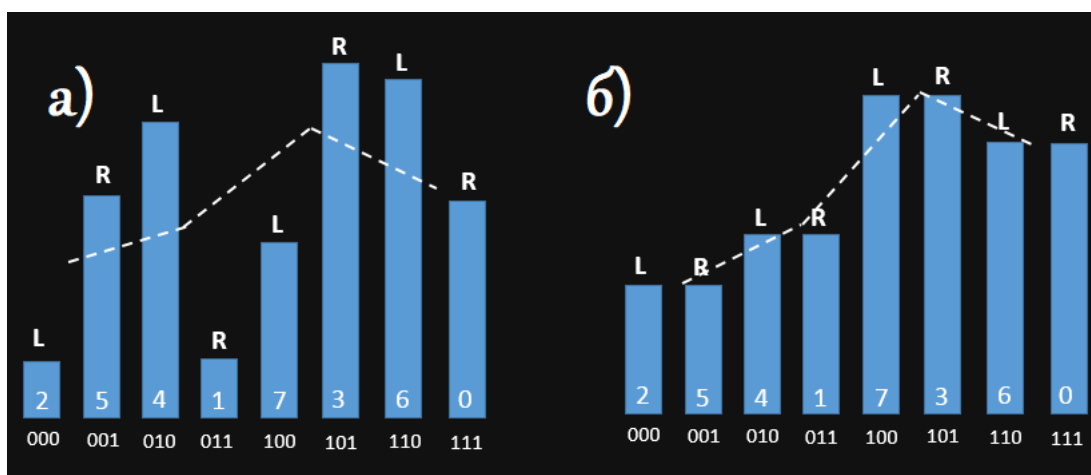


Рис.3. Гистограмма распределения частот пар «цветов-близнецов»
(а - естественное изображение, б - стегоконтейнер после LSB-внедрения)

3. Машинное обучение и глубокий анализ используют классификаторы на основе методов опорных векторов (SVM) и сверточных нейронных сетей (CNN). Алгоритмы извлекают высокоразмерные векторы признаков, выявляя микроскопические искажения, невидимые для статистических тестов. Это позволяет обнаруживать адаптивные методы внедрения (например, HUGO, WOW), устойчивые к простому анализу гистограмм.

4. Сигнатурный анализ основан на изучении известных заголовков или артефактов специфического ПО (например, OpenStego, Steghide). Эффективен против готовых инструментов, но бесполезен против самописных скриптов или модифицированных алгоритмов.

Ниже рассмотрено правовое регулирование и организационные меры. В законодательстве Российской Федерации отсутствует прямой запрет на использование технологий стеганографии. Ответственность наступает за последствия её применения:

- УК РФ ст. 272–274. Если стеганография использовалась для неправомерного доступа, создания вредоносного ПО или нарушения эксплуатации средств хранения информации.

- 152-ФЗ «О персональных данных». Применение стеганографии для обработки ПДн должно соответствовать требованиям по защите информации,

утвержденным ФСТЭК.

- Рекомендации ФСТЭК. Стеганографические каналы включены в модель угроз безопасности информации. Однако массовое внедрение стегоанализа в DLP-системы сдерживается высокой вычислительной сложностью алгоритмов, что создает риски замедления бизнес-процессов при проверке трафика в реальном времени.

Актуальность темы обусловлена совокупностью технологических, угрозных и регуляторных факторов, формирующих современный ландшафт информационной безопасности.

Так в плане угроз наблюдается устойчивый рост использования стеганографических техник в составе сложных целевых атак (APT). Злоумышленники переходят от сигнатурных методов внедрения к адаптивным алгоритмам, устойчивым к статистическому анализу. Стеганография становится ключевым инструментом для организации скрытых каналов командования и управления (C2) и эксфильтрации данных в условиях, когда традиционные периметровые средства защиты (NGFW, IDS) фокусируются на анализе заголовков и сигнатур, игнорируя полезную нагрузку медиафайлов.

Также эффективность существующих средств стегоанализа снижается из-за ряда факторов, связанных с технологическими вызовами и ограничениями защиты:

- Распространение шифрования. Массовый переход на протоколы TLS 1.3 скрывает метаданные трафика, делая сетевую стеганографию менее заметной и переносит точку контроля на эндпоинты, где ресурсы для глубокого анализа ограничены.

- Вычислительная сложность: Глубокий стегоанализ (особенно на базе машинного обучения) требует значительных вычислительных мощностей, что затрудняет его интеграцию в DLP-системы реального времени без деградации производительности бизнес-процессов.

- Новые типы контейнеров: Появление контента, генерируемого нейросетями (Deepfakes, AI-изображения), меняет статистические свойства файлов, делая традиционные методы обнаружения аномалий менее эффективными.

3. Двойственность природы стеганографии (защита авторских прав против скрытия атак) создает сложности для правового регулирования. В РФ отсутствует методологическая база для сертификации средств стегоанализа и четкие критерии квалификации инцидентов, связанных со скрытыми каналами. Фрагментарность нормативных требований (ФСТЭК, Роскомнадзор) не дает организациям четких инструкций по внедрению контрмер.

Таким образом, актуальность работы продиктована необходимостью разработки адаптивных методов обнаружения, способных балансировать между точностью детектирования и производительностью, а также потребностью в систематизации подходов к противодействию стеганографическим угрозам в рамках действующего законодательства.

Направления совершенствования защиты и регулирования

Противодействие угрозам, связанным со злоупотреблением стеганографией, требует комплексного подхода, объединяющего технологическое развитие, адаптацию нормативной базы и подготовку кадров. Односторонние меры (только технические или только правовые) не способны обеспечить достаточный уровень безопасности.

Одним из направлений противодействия является развитие адаптивных алгоритмов стегоанализа. Так ключевыми подходами развития могут быть:

- Внедрение машинного обучения (ML) — использование сверточных нейронных сетей для классификации файлов требует обучения на репрезентативных датасетах.

- Гибридные методы детектирования — комбинация сигнатурного анализа (для известных инструментов), статистических тестов (для выявления аномалий распределения) и ML-классификаторов позволяющая снизить уровень ложных срабатываний и повысить вероятность обнаружения.

- Интеграция в DLP и NGFW — разработка специализированных модулей для систем предотвращения утечек и межсетевых экранов нового поколения.

Другим направлением является совершенствование нормативно-правового регулирования. Ввиду двойственного характера технологии, введение прямых запретов на использование методов стеганографии нецелесообразно, так как это ограничит легитимное применение (водяные знаки, защита авторских прав). Регулирование должно фокусироваться на последствиях использования. Так возможно уточнение формулировок УК РФ и дополнение статей 272–274 УК РФ разъяснениями на использование скрытых каналов передачи данных какотягчающего обстоятельства или квалифицирующего признака при совершении киберпреступлений. Также необходимо повышать ответственность платформ. Вместо тотальной проверки контента, целесообразно внедрение риск-ориентированного подхода, обязывающего платформы анализировать метаданные и подозрительные файлы по запросу регулятора или при наличии индикаторов компрометации.

Существенный вклад в противодействие угрозам, связанным со злоупотреблением стеганографией, вносит повышение уровня осведомленности и квалификации специалистов является фундаментом долгосрочной защиты. Этому может способствовать, например, включение модулей по стеганографии и стегоанализу в стандарты подготовки специалистов по информационной безопасности (вузы, учебные центры).

Заключение

Проведенный анализ современных методов стеганографии и стегоанализа позволяет сделать некоторые выводы. Классические алгоритмы обнаружения, такие как метод хи-квадрат, демонстрируют высокую результативность против базовых схем LSB-внедрения. Однако их эффективность критически снижается при использовании злоумышленниками адаптивных алгоритмов с псевдослучайным распределением данных и шифрованием внедряемого сообщения. Будущее стегоанализа за гибридными системами, сочетающими

статистический анализ с методами машинного обучения. Это позволяет выявлять слабые аномалии в частотной области (DCT), невидимые для традиционных тестов, однако требует значительных вычислительных ресурсов. Основная преграда для массового использования стегоанализа в DLP-системах — высокая вычислительная сложность, создающая риски замедления бизнес-процессов при проверке трафика в реальном времени. С точки зрения права регулирование должно фокусироваться не на запрете технологий (что невозможно из-за их двойственного назначения), а на криминализации действий по использованию скрытых каналов для противоправных целей. Работа охватывала преимущественно графические форматы (BMP, JPEG) и не охватывала в полной мере стеганографию в потоковых медиа и облачных хранилищах, что может являться предметом для дальнейших исследований.

Список литературы

1. Fridrich J. Steganography in digital media principles, algorithms, and applications / Jessica Fridrich. — Cambridge [etc.]: Cambridge univ. press, 2010. — XXIII, 437 с. ил.; 26. ISBN: 978-0-521-19019-0
2. Грибунин В.Г., Оков И.Н., Туринцев И.С. Цифровая стеганография. — М.: Солон-Пресс, 2017. — 262 с. ISBN: 978-5-91359-173-9 EDN: XFUPAN
3. ГОСТ Р 53113.1-2008 Информационная технология. Защита информации. Технологии противодействия несанкционированному доступу. Часть 1. Показатели защищенности информации от несанкционированного доступа. — Введ. 2009-01-01. — М.: Стандартинформ, 2009.
4. ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил управления информационной безопасностью. — Введ. 2013-01-01. — М.: Стандартинформ, 2013.
5. Гражданский кодекс Российской Федерации (часть четвертая) от 18.12.2006 № 230-ФЗ (ред. от 04.11.2022). Ст. 1255. — URL: http://www.consultant.ru/document/cons_doc_LAW_64629/ (дата обращения: 18.04.2025).
6. Лаборатория Касперского. Что такое стеганография? Определение и описание [Электронный ресурс]. — URL: <https://www.kaspersky.ru/resource-center/definitions/what-is-steganography> (дата обращения: 18.04.2025).
7. Солодуха Р. Стеганоанализ в компьютерно-технической экспертизе [Электронный ресурс]. — URL: <https://habr.com/ru/articles/791284/> (дата обращения: 18.04.2025).
8. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 04.11.2022). Ст. 272–274. — URL: http://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения: 21.05.2025).
9. Шульмин А., Крылова Е. Стеганография в современных кибератаках [Электронный ресурс]. — URL: <https://securelist.ru/steganography-in-contemporary-cyberattacks/79090/> (дата обращения: 18.04.2025).

MODERN METHODS OF STEGANALYSIS AND PROTECTION AGAINST STEGANOGRAPHIC ATTACKS

I.N. Hirivimsky, A.P. Shkaraputa

Perm State University

Abstract. The article is devoted to a comparative analysis of modern methods of steganography and steganalysis. The principles of operation of basic algorithms for information hiding are considered: LSB methods, approaches based on discrete cosine transform (DCT), as well as methods using format redundancy. The scenarios of malicious use of steganography (malicious code injection, hidden data exfiltration) and the corresponding methods of counteraction are analyzed: visual analysis, statistical tests (including the Westfeld-Pfitzmann chi-square method) and machine learning-based approaches. It is shown that the effectiveness of statistical methods is significantly reduced when using adaptive embedding schemes with pseudorandom data distribution, which actualizes the task of developing hybrid detectors. The limitations of modern DLP systems in terms of detecting stegocontainers and the prospects for their integration with steganalysis algorithms are discussed. An overview of the legal regulation of steganography in the Russian Federation is given and recommendations for improving the regulatory framework are formulated. Based on the analysis, it is concluded that there is a need for an integrated approach combining technological innovations, legal mechanisms and personnel training.

Keywords: *steganography, steganalysis, LSB, DCT methods, chi-square method, intrusion detection, hidden data transmission channels, information security, DLP systems, digital watermarks, imperceptibility.*

ЗАЩИТА ОТ ФИНАНСОВОГО МОШЕННИЧЕСТВА

Е.К. Шкуренко, Е.Ю. Никитина

Пермский государственный национальный исследовательский университет

Аннотация. Проанализировано текущее состояние финансового мошенничества, выявлены уязвимые зоны в системах защиты и выдвинуты предложения для повышения эффективности противодействия финансовому мошенничеству. Предложены направления совершенствования правовых, технических и образовательных мер противодействия мошенничеству.

Ключевые слова: *финансовое мошенничество, социальная инженерия, искусственный интеллект, киберугрозы, информационная безопасность.*

Финансовое мошенничество представляет собой одну из ключевых угроз современного цифрового мира, охватывая как индивидуальных пользователей, так и крупные финансовые организации.

Актуальность темы обусловлена стремительным ростом киберпреступности, использованием мошенниками передовых технологий, таких как искусственный интеллект и deepfake, а также недостаточной осведомленностью пользователей и уязвимостями существующих систем защиты. В статье анализируются существующие методы защиты, их уязвимости и предлагаются идеи для улучшения ситуации в данном вопросе.

Текущее состояние вопроса

В Российской Федерации защита от финансового мошенничества регулируется рядом законодательных и нормативных актов:

- Уголовный кодекс РФ (УК РФ) статья 272 "Неправомерный доступ к компьютерной информации"— регулирует ответственность за взлом систем и кражу данных [9].
- Уголовный кодекс РФ (УК РФ) статья 273 "Создание, использование и распространение вредоносных программ"— направлена на борьбу с инструментами, используемыми мошенниками. [1].
- Федеральный закон № 161-ФЗ "О национальной платежной системе" (от 27.06.2011) [2] – Устанавливает требования к безопасности операций с электронными средствами платежа и обязывает банки внедрять меры защиты клиентов.
- Федеральный закон № 152-ФЗ "О персональных данных" (от 27.07.2006) [3] – Регулирует обработку и защиту персональных данных, что важно для предотвращения утечек, используемых мошенниками.
- Указание Центрального банка РФ № 5521-У (от 06.08.2020) [4] — определяет порядок взаимодействия банков с клиентами при выявлении мошеннических операций.

Финансовое мошенничество в 2024–2025 годах продолжает оставаться одной из самых серьезных угроз для экономики и безопасности как отдельных граждан, так и организаций. Рассмотрим ключевые тенденции и статистику, характеризующие текущее состояние вопроса.

Рост мошенничества: цифры и тенденции.

Кибератаки становятся все более сложными и изощренными. Если в прошлом мошенники полагались на простые схемы, такие как классический фишинг, то сегодня они используют глубокие социальные манипуляции, автоматизированные боты и AI.

По данным ЦБ РФ, за 2024 год объем хищений без согласия клиентов составил 27,5 миллиардов рублей, что на 74,3% больше, чем в 2023 году. За первые три месяца 2025 года (январь–март) ожидается рост ущерба до 8–10 млрд рублей на основе экстраполяции данных ЦБ РФ за 2024 год с учетом увеличения числа цифровых транзакций. В 2024 году россияне совершили более 2,5 миллиардов операций через Систему быстрых платежей (СБП) на сумму 10,5 триллионов рублей, что вдвое больше, чем в 2023 году [5]. Этот рост транзакций сопровождается увеличением числа атак.

Мошенники используют искусственный интеллект - он помогает мошенникам:

1. Создавать персонализированные фишинговые письма: Анализируя данные из социальных сетей, мошенники составляют сообщения, которые выглядят максимально правдоподобно.
2. Сканировать уязвимости: Автоматизированные системы выявляют слабые места в банковских API или POS-терминалах за считанные минуты.
3. Обходить системы защиты: AI оптимизирует схемы атак, позволяя обойти традиционные antifraud-системы.

Атаки на банки и финансовые компании, использующие инновационные технологии для предоставления услуг.

Финансовые организации ежедневно сталкиваются с миллионами попыток атак. В 2024 году хакеры взломали крупную платежную систему в Европе, украв данные 50 миллионов карт. В России за тот же год было зафиксировано более 34,8 миллионов предотвращенных атак, но 1,17 миллиона операций оказались успешными для мошенников. Атаки на банковские API, такие как Man-in-the-Middle, стали одной из главных угроз. В 2025 году эксперты прогнозируют рост числа атак на мобильные банковские приложения, так как более 70% россиян используют их для повседневных операций.

Ситуация в России.

Финансовое мошенничество в России продолжает набирать масштабы, демонстрируя тревожный рост как в абсолютных цифрах, так и в количестве зарегистрированных случаев. Рассмотрим ключевые статистические данные за 2024 год и начало 2025 года (рис.1,2):

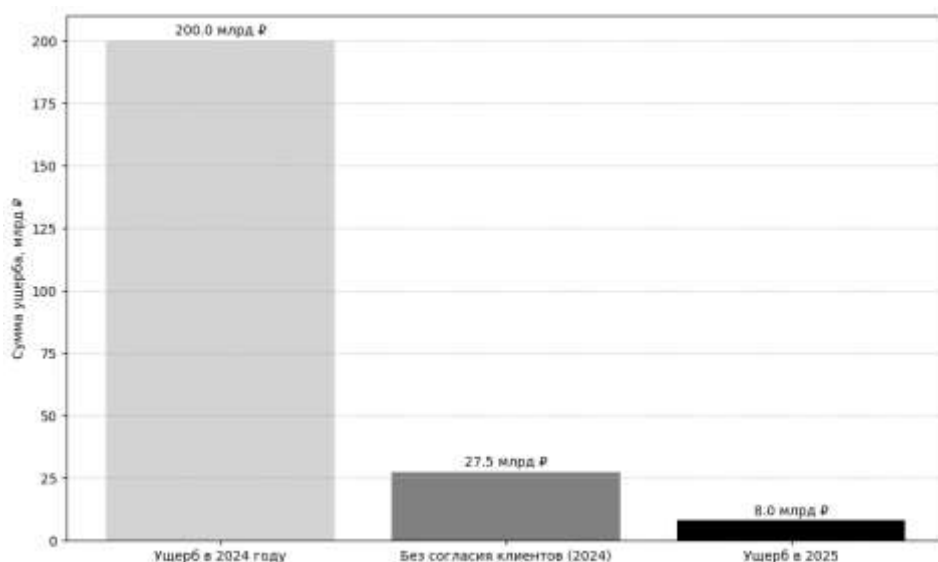


Рис. 1. Ущерб от мошенничества с платежными картами 2024 г. – начало 2025 г.

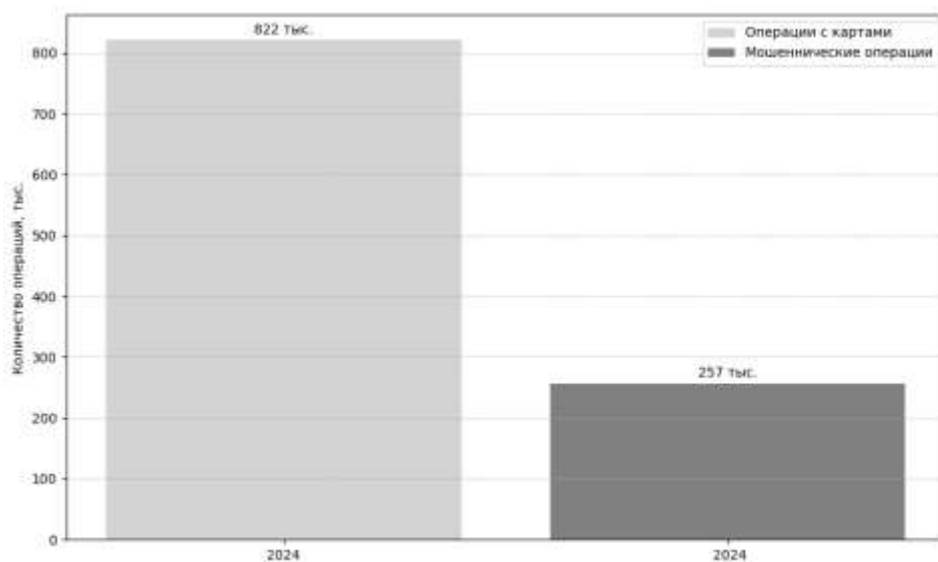


Рис. 2. Количество мошеннических операций за 2024 г.

В 2024 году граждане подали 338 тысяч жалоб на финансовые темы, что на 3,9% больше, чем в 2023 году. Из них 60,7% касались банковских операций. А уже первом квартале 2025 года число жалоб достигло 90 тысяч, что указывает на сохранение тенденции роста.

По оценкам экспертов, объем финансового мошенничества в России в 2025 году может превысить показатели 2024 года в 1,5–1,9 раза. Основной драйвер роста — увеличение числа атак с использованием социальной инженерии и новых технологий, таких как генеративные нейросети.

Телефонное мошенничество в России.

Телефонное мошенничество остается самым распространенным видом обмана в России. В 2024 году мошенники совершили более 8 миллионов звонков в день, из которых 85% были связаны с финансовыми схемами. В 2025 году эта тенденция усилилась: в марте было зафиксировано более 10 миллионов звонков за сутки, что связано с использованием AI-ботов, способных имитировать человеческий голос и адаптировать сценарий в реальном времени.

Типичный сценарий: Злоумышленник звонит жертве, представляясь сотрудником банка, и сообщает о "подозрительной операции" по счету. Затем жертву просят перевести деньги на "безопасный счет" или сообщить код из SMS. В 2024 году такие звонки привели к краже 1,2 миллиарда рублей только за первый квартал. В 2025 году добавился новый сценарий: Злоумышленники используют схемы, представляясь сотрудниками Федеральной Службы Безопасности, и обвиняют жертву в финансировании терроризма, требуя перевести деньги для "снятия обвинений". За январь–март 2025 года эта схема принесла мошенникам около 400 миллионов рублей.

Социальная инженерия и новые технологии.

Социальная инженерия остается ключевым инструментом мошенников. В 2024 году 92% атак на частных лиц в России использовали методы социальной инженерии, такие как фишинг, запугивание или ложные обещания быстрого заработка [6]. В 2025 году добавились схемы с использованием генеративных моделей (GANs), которые создают поддельные документы или видеозвонки для обмана жертв. Например, в январе 2025 года мошенники использовали поддельное видео с "директором компании", чтобы убедить сотрудника перевести 20 миллионов рублей. В марте 2025 года появилась схема с фальшивыми видеозвонками от "налоговой службы", что привело к краже 100 миллионов рублей у малого бизнеса.

Реакция банков и государства.

Банки и регуляторы предпринимают меры для борьбы с мошенничеством. В 2024 году вступил в силу Федеральный закон № 369-ФЗ, обязывающий банки проверять переводы и возвращать украденные деньги в течение 30 дней [7]. В 2025 году ЦБ планирует ужесточить требования к antifraud-процедурам при выдаче кредитов, что может снизить число атак, связанных с оформлением займов на подставных лиц.

Современные методы защиты от финансового мошенничества

1. Аутентификация и контроль доступа

1. MFA – использование нескольких факторов (пароль + биометрия + одноразовый код).
2. Биометрическая идентификация – сканирование отпечатков пальцев, радужки глаза, голосовой аутентификации.
3. Аппаратные токены и FIDO2-ключи – защищают от фишинга и перехвата учетных данных.

2. Мониторинг и анализ транзакций

1. FDS – системы, использующие машинное обучение и анализ больших данных для выявления подозрительных транзакций, таких как переводы на аномально крупные суммы или в несвойственные регионы.
2. UEBA – отслеживание поведенческих паттернов пользователей и устройств для выявления аномалий, указывающих на мошеннические действия.
3. Правила и сигнатурный анализ – детектирование известных мошеннических схем по шаблонам.

3. Шифрование и защита данных

1. E2EE – предотвращает перехват конфиденциальных данных, таких как финансовые транзакции, при передаче между клиентом и сервером.
2. Хэширование паролей – защита учетных данных в базах данных.
3. Токенизация – замена критичных данных на токены, снижающие риск утечки.

4. Защита от фишинга и социальной инженерии

1. AI-анализатор фишинговых писем – автоматическое обнаружение подозрительных писем и ссылок.
2. DNS-фильтрация и антифишинговые решения – блокировка вредоносных сайтов.
3. Обучение сотрудников и пользователей – повышение осведомленности о киберугрозах.

5. Защита инфраструктуры

1. WAF – защита веб-приложений от атак, таких как SQL-инъекции и XSS.
2. DLP – системы предотвращения утечек конфиденциальных данных, таких как номера банковских карт и персональная информация клиентов.
3. SIEM – централизованный анализ логов для выявления атак.

6. Блокчейн и децентрализованные технологии

1. Smart Contracts – автоматизированные контракты без посредников, уменьшающие риски подмены данных.
2. DID – безопасный доступ к финансовым сервисам.

7. Краудсорсинг и Threat Intelligence

1. Обмен данными о киберугрозах между банками и организациями.
2. Dark Web мониторинг – отслеживание утечек данных клиентов.
3. SOC – круглосуточный мониторинг атак и мошеннической активности.

8. Биометрия и поведенческий анализ

1. Контекстная аутентификация – анализ геолокации, устройства, IP-адреса при входе в систему.
2. Кейлоггинг-анализ – проверка паттернов набора текста, чтобы обнаружить подмену пользователя.
3. Анализ мышечной памяти (Behavioral Biometrics) – уникальные движения мыши и сенсорного экрана.

9. Обратное проектирование мошеннических схем (Fraud Intelligence)

1. Red Team операции – имитация атак мошенников на системы банка для выявления уязвимостей в процессах аутентификации или мониторинга транзакций.
2. OSINT – сбор разведданных о преступниках в открытых источниках.
3. Deception Technology – создание фальшивых данных и транзакций для отслеживания мошенников.

10. Смарт-контракты и цифровые активы

1. Защита DeFi-платформ – выявление уязвимостей в смарт-контрактах.
2. NFT для финансовых гарантий – использование токенов в банковских системах.

Проблема финансового мошенничества в условиях цифровизации приобретает особую значимость, что подтверждается анализом текущего состояния вопроса:

- Масштабы финансового мошенничества в России и мире демонстрируют устойчивую тенденцию к росту.
- Мошенники становятся все хитрее и умнее. Конечно, существует большое количество способов защиты, но они направлены на уже давно известные угрозы.
- Нормативно-правовая база, несмотря на определенные достижения, имеет существенные недостатки.

Внутренние законы иногда не дают должного эффекта. Например Федеральный закон № 369-ФЗ, обязывающий банки возвращать украденные средства, показал низкую эффективность: В 2024 году кредитные организации возвратили клиентам 9,9% (2 713,58 млн рублей) от всего объема операций по переводу денежных средств, совершенных без добровольного согласия клиентов (в 2023 году данный показатель составил 8,7%, или 1 378,76 млн рублей) [8].

Направление решения вопроса

Можно выделить несколько направлений для повышения эффективности противодействия финансовому мошенничеству:

1. Усовершенствование нормативно правовой базы

1.1. Недостаточная регламентация цифровых форм мошенничества.

Наблюдается отсутствие нормативного закрепления понятий: «цифровое финансовое мошенничество», «технологические схемы обмана», «интернет-мошенничество с применением искусственного интеллекта». Например, статья 272 УК РФ — Неправомерный доступ к компьютерной информации [9] не охватывает случаи, когда пользователь сам передаёт данные по просьбе злоумышленника и статья 159.6 УК РФ — Мошенничество в сфере компьютерной информации [10] не охватывает случаи социальной инженерии. Предлагается внести изменения в Уголовный кодекс РФ, закрепив отдельные составы преступлений, связанных с цифровыми финансовыми аферами, и разработать правовые определения указанных терминов.

1.2. Недостаточная строгость уголовных санкций.

Многие мошеннические действия квалифицируются по статьям 159.1 УК РФ - мошенничество в сфере кредитования [11], предусматривающая ограниченное наказание, особенно при ущербе менее значительного размера. Предусмотрено наказание до двух лет лишения свободы или штраф до 120 тыс. рублей. Редко, когда выносятся наказания так как если мошенничество затрагивало социально уязвимые группы людей, то суд вынужден привести в наказание лишь штраф, а значит мошенник останется на свободе. Предлагается ужесточить и дополнить уже существующие статьи УК РФ.

2. Повышение финансовой грамотности и осведомленности населения.

Социальная инженерия остается главной угрозой, и борьба с ней требует повышения финансовой грамотности населения. Предлагается запустить общероссийские кампании:

2.1. *Геймифицированная мобильная платформа* - разработка интерактивного мобильного приложения в формате обучающей игры, в которой пользователи проходят сценарии реальных мошеннических схем и учатся правильно реагировать на угрозы.

2.2. *Кампания в транспорте и инфраструктуре* - предполагает размещение кратких просветительских видео и инфографики в такси, поездах метро, аэропортах и торговых центрах. Такие материалы могут содержать конкретные признаки мошенничества и советы по защите.

3. *Исследовательские центры для раннего выявления новых угроз.*

Идея заключается в том, что в университетах, научных центрах будут реализованы узкоспециализированные лаборатории по выявлению угроз, связанных с финансовой безопасностью. В таких центрах лаборантами могут быть студенты направлений, связанных с информационной безопасностью. Такие центры позволят анализировать существующие технологии на предмет уязвимостей и передавать данные банкам и регулирующим органам и разрабатывать контрмеры для устранения уязвимостей. Мониторинг поможет обнаружить уязвимости до их эксплуатации мошенниками.

Список литературы

1. Уголовный кодекс Российской Федерации: по состоянию на 1 апр. 2025 г. — М.: Проспект, 2025. — 256 с.
2. О национальной платежной системе: Федеральный закон от 27 июня 2011 г. № 161-ФЗ: в ред. от 1 янв. 2025 г. — М.: Юрайт, 2025. — 48 с.
3. О персональных данных: Федеральный закон от 27 июля 2006 г. № 152-ФЗ: в ред. от 1 янв. 2025 г. — М.: Эксмо, 2025. — 32 с.
4. О порядке взаимодействия банков с клиентами при выявлении мошеннических операций: Указание Банка России от 6 авг. 2020 г. № 5521-У. — М.: Центральный банк Российской Федерации, 2020. — 12 с.
5. Обзор финансовой стабильности за 2024 год [Электронный ресурс]. // cbr.ru. URL: https://cbr.ru/analytics/finstab/ofs/2q_3q_2024/ (дата обращения: 03.04.2025).
6. Актуальные киберугрозы: III квартал 2024 года [Электронный ресурс]. // ptsecurity.com. URL: <https://ptsecurity.com/ru-ru/research/analytics/aktualnye-kiberugrozy-iii-kvartal-2024-goda/#id2> (дата обращения: 03.04.2025).
7. О внесении изменений в отдельные законодательные акты Российской Федерации в целях противодействия мошенничеству: Федеральный закон от 1 июля 2024 г. № 369-ФЗ. — М.: Юридическая литература, 2024. — 20 с.
8. Обзор операций, совершенных без добровольного согласия клиентов финансовых организаций [Электронный ресурс]. // cbr.ru. URL: https://cbr.ru/analytics/ib/operations_survey/2024/ (дата обращения: 09.04.2025)
9. УК РФ Статья 272. Неправомерный доступ к компьютерной информации [Электронный ресурс]. // consultant.ru. URL: https://www.consultant.ru/document/cons_doc_LAW_10699/5c337673c261a026c476d578035ce68a0ae86da0/ (дата обращения: 14.05.2025)

10. УК РФ Статья 159.6. Мошенничество в сфере компьютерной информации [Электронный ресурс]. // consultant.ru. URL: https://www.consultant.ru/document/cons_doc_LAW_10699/51c53d82b60ac8c009745bdea3838d507064c6d3/ (дата обращения: 14.05.2025)

11. УК РФ Статья 159.1. Мошенничество в сфере кредитования [Электронный ресурс]. // consultant.ru. URL: https://www.consultant.ru/document/cons_doc_LAW_10699/823429f3a37857573b519d0b17fd14f96a99bca4/ (дата обращения: 14.05.2025)

PROTECTION AGAINST FINANCIAL FRAUD

E.K. Shkurenko, E.Yu. Nikitina

Perm State University

Abstract. The current state of financial fraud has been analyzed, vulnerable areas in protection systems have been identified, and proposals have been put forward to improve the effectiveness of countering financial fraud. The directions of improvement of legal, technical and educational measures of counteraction to fraud are offered.

Keywords: *financial fraud, social engineering, artificial intelligence, cyber threats, information security.*

ТЕХНИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

Е.О. Шолков, А.Н. Рабчевский

Пермский государственный национальный исследовательский университет

Аннотация. В условиях стремительной цифровизации защита интеллектуальной собственности (ИС) становится критически важной задачей для обеспечения экономической безопасности и стимулирования инноваций. Настоящая статья посвящена анализу современных технических методов защиты ИС на территории Российской Федерации. Рассмотрены ключевые технологии: цифровые водяные знаки (ЦВЗ), системы управления цифровыми правами (DRM) и инструменты на базе искусственного интеллекта (ИИ). Проведена оценка их эффективности, выявлены ограничения, связанные с правоприменительной практикой, стоимостью внедрения и устойчивостью к атакам. Предложены актуальные направления развития, включая биометрическую аутентификацию контента и адаптивные ИИ-системы мониторинга. Результаты демонстрируют необходимость комплексного подхода, сочетающего технологические решения с укреплением правовой базы и развитием экспертного потенциала для эффективной защиты ИС в российских реалиях.

Ключевые слова: *интеллектуальная собственность, цифровые водяные знаки, DRM, искусственный интеллект, защита авторских прав, информационная безопасность, цифровое пиратство.*

Введение

Интеллектуальная собственность (ИС) — ключевой актив в цифровой экономике, охватывающий программное обеспечение, медиаконтент, изобретения и научные разработки [1]. Бурное развитие информационных технологий, с одной стороны, упрощает создание и распространение инноваций, с другой — создает беспрецедентные риски несанкционированного копирования, распространения и модификации объектов ИС. В России, где процессы цифровизации и импортозамещения приобретают стратегическое значение, проблема защиты ИС стоит особенно остро. Уязвимость российского контента (кино, музыка, ПО, литература) перед несанкционированным доступом и распространением наносит значительный экономический ущерб и подрывает конкурентоспособность отечественных правообладателей.

Правовая основа защиты ИС в РФ закреплена в Части IV Гражданского кодекса (ГК РФ), предусматривающей гражданскую, административную (ст. 7.12 КоАП РФ) и уголовную ответственность (ст. 146 УК РФ) за нарушения [1]. Однако правоприменение сталкивается с трудностями: нехватка экспертизы, длительные судебные процедуры и сложность доказывания нарушений в цифровой среде. В этих условиях технические средства защиты ИС становятся необходимым дополнением к правовым механизмам.

Цель данной статьи — рассмотреть современные технические решения для защиты ИС, применяемые или перспективные для применения в России, оценить их эффективность и предложить новые возможные направления развития технических средств для защиты ИС.

Обзор существующих решений

Одним из методов защиты ИС являются цифровые водяные знаки (ЦВЗ) представляют собой технологические маркеры, внедряемые в цифровой контент (изображения, аудио-видеоматериалы, документы) для идентификации правообладателя и отслеживания их дальнейшего распространения [2]. Существуют два основных типа:

- Видимые (открыто размещаемые элементы, например логотипы);
- Невидимые (скрытые метки, которые можно обнаружить при использовании специализированного ПО) [5].

Технология внедрения основана на модификации малозаметных параметров файла (цветовых характеристик, структурных особенностей), но при этом способна сохранять исходное качество контента [5]. В России ЦВЗ применяются:

- Для защиты изображений на онлайн-платформах, предназначенных для покупки и продажи фото контента;
- Верификации подлинности документов;
- Выявления источников утечек корпоративной информации.

Преимущества: низкая стоимость реализации, малая заметность.

Недостатки: уязвимость к сжатию и целенаправленной обработке, ограниченное применение в правовом поле РФ из-за дефицита экспертов и низкой осведомлённости малого бизнеса [3].

Другой метод, это система управления цифровыми правами (DRM) — комплексное решение для контроля доступа к цифровому контенту. Принцип работы этих систем включает в себя:

- Шифрование контента;
- Распределение лицензионных ключей с ограничениями использования;
- Аутентификацию пользователей [4].

В Российской Федерации этот метод применяется в различных сферах:

- Защита от несанкционированного копирования в стриминговых сервисах видео и аудио контента (IVI, Okko, Яндекс музыка);
- Ограничение нелицензированного копирования и распространения книг Электронные библиотеки (ЛитРес);
- Защита собственных разработок от несанкционированного использования путем применения аппаратных DRM систем через программные или USB-ключи.

Преимущества: высокий уровень безопасности.

Недостатки: значительные затраты на внедрение, ограничения для пользователей (онлайн-проверки), возможность технического обхода, частичная зависимость от зарубежных технологий (Widevine, PlayReady) [3,4].

В последнее время для защиты ИС все чаще применяют Искусственный интеллект (ИИ). Он применяется для автоматизации защиты авторских прав через:

- Генерацию цифровых "отпечатков" контента;
- Мониторинг интернет-пространства (соцсети, файлообменники);
- Автоматическое реагирование на нарушения [6].

В РФ технологии ИИ внедряются для обнаружения пиратского контента в закрытых источниках (мессенджеры).

Преимущества: высокая скорость обработки больших объёмов данных.

Ограничения:

- Высокая стоимость разработки;
- Риск ложных срабатываний;
- Недостаток экспертизы в судебной системе;
- Неравномерность технологической инфраструктуры по регионам.

Перспективные направления для защиты ИС

Анализ текущих методов защиты ИС в России показывает, что у каждого технического средства защиты ИС есть свои слабые стороны: ЦВЗ можно обойти, например, применив специальное ПО для сжатия информации, DRM системы требуют значительных денежных вложений со стороны правообладателя ИС, а собственные разработки ИИ-системы для защиты ИС сложны и дороги в создании. Кроме того, сохраняется зависимость от иностранных технологий, а судебная система не всегда готова работать с цифровыми доказательствами. Чтобы усилить защиту, может быть предложено несколько путей развития технологий защиты ИС.

1. Адаптивные цифровые водяные знаки с ИИ

Новым шагом в защите ИС вполне могут стать "умные" водяные знаки, способные самостоятельно восстанавливаться при повреждении. В отличие от обычных меток, эти адаптивные цифровые знаки содержат встроенные нейросетевые алгоритмы, которые анализируют изменения в файле. Если злоумышленник пытается удалить знак через различные технические средства, к которым можно отнести обрезку, сжатие или фильтрацию, система автоматически восстанавливает оригинальную структуру исходного защищаемого файла. Для критических случаев повреждения метка может временно стать видимой, сохраняя связь с правообладателем. Технология демонстрирует высокую устойчивость к большинству известных атак, включая профессиональные инструменты удаления водяных знаков.

2. Биометрическая защита контента

Для особо ценных цифровых активов (например, дорогих корпоративных программ или эксклюзивных фильмов, показ которых осуществляется исключительно в закрытом сообществе) предлагается двухуровневая система доступа, сочетающая традиционные лицензии с биометрической верификацией. Пользователь должен подтвердить личность через отпечаток

пальца или распознавание лица непосредственно в момент использования контента. Данные биометрии обрабатываются только на устройстве. Это гарантирует, что даже при краже файла его невозможно будет открыть без физического присутствия владельца. Технология особенно актуальна для защиты коммерческого ПО, эксклюзивных видео и аудио материалов и корпоративных баз данных.

3. Системы мониторинга поведения пользователей на основе ИИ

Данные системы представляет из себя перспективные направления в области защиты интеллектуальной собственности. Эти решения анализируют действия пользователей в режиме реального времени, используя машинное обучение для создания профилей-паттернов нормальной активности законопослушного пользователя. При отклонениях (несанкционированный доступ к конфиденциальным данным, массовое копирование файлов, попытки обхода защиты) система мгновенно блокирует подозрительные сессии и оповещает службы безопасности. Помимо этого, такие системы также могут применяться для автоматического направления юридических требований об удалении пиратского контента хостинг-провайдерам и владельцам ресурсов, на которых размещена и распространяется информация, полученная путем кражи ИС.

Заключение

Эффективная защита интеллектуальной собственности в России требует развития от разрозненных технических решений к комплексной экосистеме. Предложенные направления, такие как адаптивные ИИ-ЦВЗ, биометрически усиленные DRM и системы мониторинга поведения пользователей на основе ИИ, нацелены на преодоление ключевых недостатков существующих методов: уязвимости, высокой стоимости и медленного реагирования на нарушения. Их реализация, особенно в контексте политики импортозамещения и технологического суверенитета, позволит создать устойчивую среду для развития инноваций и защиты интересов российских правообладателей на цифровом рынке.

Список литературы

1. Гражданский кодекс Российской Федерации (часть четвертая) от 18.12.2006 № 230-ФЗ (ред. от 24.02.2025). (дата обращения 25.03.2025)
2. Грачёва Ю.А. Применение цифровых водяных знаков для защиты цифровых фотографий // Информационные технологии. 2023. № 5. С. 45–52. (дата обращения 25.03.2025)
3. Козлов А.В. Современные методы защиты цифрового контента. СПб.: БХВ-Петербург, 2022. 320 с. (дата обращения 25.03.2025)
4. Морозов И.П. DRM-системы: технологии и перспективы развития // Информационная безопасность. 2023. № 3. С. 78–85. (дата обращения 25.03.2025)
5. Орешкина Е.И. Классификация методов нанесения цифровых водяных знаков // Защита информации. Инсайд. 2022. № 3. С. 28–35. (дата обращения 25.03.2025)

6. Савченко Е.Д. Применение средств искусственного интеллекта для защиты авторских прав // Искусственный интеллект и право. 2023. № 2. С. 89–97. (дата обращения 25.03.2025)

TECHNICAL METHODS OF INTELLECTUAL PROPERTY PROTECTION

E.O. Sholkov, A.N. Rabchevsky

Perm State University

Abstract. In the context of rapid digitalization, the protection of intellectual property (IP) is becoming a critical task for ensuring economic security and stimulating innovation. This article is devoted to the analysis of modern technical methods of IP protection in the territory of the Russian Federation. Key technologies are considered: digital watermarks (digital watermarks), digital rights management systems (DRM) and tools based on artificial intelligence (AI). Their effectiveness was assessed, and limitations related to law enforcement practices, implementation costs, and attack resistance were identified. Current directions of development are proposed, including biometric content authentication and adaptive AI monitoring systems. The results demonstrate the need for an integrated approach combining technological solutions with strengthening the legal framework and developing expert potential for effective IP protection in Russian realities.

Keywords: *intellectual property, digital watermarks, DRM, artificial intelligence, copyright protection, information security, digital piracy.*

Научное издание

Актуальные проблемы информационной безопасности

Сборник статей

Выпуск 1

Статьи публикуются в авторской редакции, авторы несут ответственность за содержание статей, за достоверность приведенных в статье фактов, цитат, статистических и иных данных, имен, названий и прочих сведений.

Издается в авторской редакции
Компьютерная верстка: *Е. Ю. Никитина*

Объем данных 1,56 Мб
Подписано к использованию 24.08.2026

Размещено в открытом доступе
на сайте psu.ru
в разделе НАУКА / Электронные публикации
и в электронной мультимедийной библиотеке ELis

Управление издательской деятельности
Пермского государственного
национального исследовательского университета
614068, г. Пермь, ул. Букирева, 15