НИЯУ МИФИ

Национальный исследовательский ядерный университет «МИФИ»

Третья Всероссийская
научно-техническая конференция

«Кибернетика и информационная безопасность»

КИБ-2025
КИБЕРНЕТИКА
И ИНФОРМАЦИОННАЯ
БЕЗОПАСНОСТЬ

3 – 4 декабря 2025 г.

Сборник научных трудов

Том 2

Москва 2025

Национальный исследовательский ядерный университет «МИФИ»

Третья Всероссийская научно-техническая конференция

«Кибернетика и информационная безопасность»

«КИБ-2025»

Сборник научных трудов

В двух томах

Том 2

3–4 декабря 2025 г., Москва

Москва 2025

УДК 004.056 : 001(06)
ББК 32.973.202
В85

Третья Всероссийская научно-техническая конференция «Кибернетика и информационная безопасность «КИБ-2025». Сборник научных трудов. 3-4 декабря 2025 г., Москва. В 2-х т. Т. 2. М.: НИЯУ МИФИ, 2025. 204 с.

Настоящая книга содержит тезисы научных работ и докладов, предложенных специалистами на конференции «КИБ-2025».

Представленные материалы выполнены преподавателями, научными сотрудниками, молодыми учеными, аспирантами и студентами МИФИ и других вузов, специалистами академических научных и научно-производственных организаций Москвы и России, сотрудничающих с МИФИ. Работы отражают достижения и уровень исследований, тенденции и проблемы в развитии и обеспечении образования и научно-исследовательских работ по актуальным вопросам информационной безопасности, решению задач по защите информации, построения информационных и интеллектуальных систем управления в защищенном исполнении.

Книга предназначена читателям, интересующимся тематикой представленных научных направлений.

Статьи сборника издаются в авторской редакции.

Материалы получены 25.10.2025

ISBN 978-5-7262-3201-0
ISBN 978-5-7262-3200-3 (т. 2)

СОДЕРЖАНИЕ

РАЗРАБОТКА БЕЗОПАСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

ТЕОРЕТИЧЕСКАЯ И ПРАКТИЧЕСКАЯ КРИПТОГРАФИЯ

ИНФОРМАЦИОННО-АНАЛИТИЧЕСКИЕ СИСТЕМЫ БЕЗОПАСНОСТИ

ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СИСТЕМЕ ВЫСШЕЙ ШКОЛЫ

КИБ-2025

КИБЕРНЕТИКА
И ИНФОРМАЦИОННАЯ
БЕЗОПАСНОСТЬ

Направление

Разработка безопасного программного обеспечения

Руководитель секции – ЗАГРЕБАЕВ А.М., д.ф.-м.н.,

заведующий кафедрой №22

УДК 004.056

М.К. ЧОКПАРОВ, А.Е. КАРЕТНИКОВ

ООО «Институт проблем безопасности и анализа информации», Москва

ПРИМЕНЕНИЕ РИСК-ОРИЕНТИРОВАННОГО ПОДХОДА ПРИ РАЗРАБОТКЕ БЕЗОПАСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

В данной статье предлагается применение методологии на основе оценки рисков как стратегии управления безопасностью процессов разработки программного обеспечения, позволяющей эффективно оценивать возможные угрозы, расставлять приоритеты и оптимально планировать реализацию мер по внедрению процессов разработки безопасного программного обеспечения (РБПО), а также в дальнейшем контролировать их выполнение.

Введение

В 2024 г. в силу вступил национальный стандарт Российской Федерации [1], содержащий общие требования к разработчикам программного обеспечения (ПО) по реализации процессов РБПО. В связи с этим, многие компании начали внедрять у себя данные процессы. При первом запуске инструментов статического анализа исходного кода обнаруживается большое количество предупреждений. Отсюда появляется потребность в методологии управления, позволяющей структурировать полученные результаты, выполнять оценку рисков и планировать наиболее оптимальным образом меры по их устранению, согласно существующей модели угроз и вероятной поверхности атаки.

Применение риск-ориентированного подхода

Опыт использования различных инструментов статического анализа, а также существующие обзоры [2] показывают, что наиболее популярные решения сфокусированы на реализации метода поиска уязвимостей. При этом для управления результатами (отчетами) статического анализа существует три основных способа: группировка и сортировка, удаление ненужных результатов, комментарии к результатам работ статического анализатора.

На взгляд авторов данной статьи, приведенные подходы справляются с задачей предоставления результатов анализа кода, но недостаточны для полноценного управления. Для решения этого недостатка предлагается использовать методологию риск-ориентированного подхода, которая зарекомендовала себя в различных сферах государственного управления [3].

Идея реализации данного подхода заключается в расширении обычной группировки результатов анализа и расчете показателей возможных рисков по существующим модулям исследуемого программного обеспечения, учитывая важность и критичность конкретного модуля. Более того, методология дает возможность вводить свои факторы риска и таким образом учитывать различные аспекты, в том числе дополнительные метрики, присваиваемые выявленным предупреждениям различными статическими анализаторами. Всё это позволяет фокусировать ресурсы разработчиков в первую очередь на самых значимых рисках.

По полученным результатам разрабатывается стратегия, далее применяются меры по устранению выявленных недостатков программного обеспечения, а также уменьшению вероятности появления новых. После чего выполняется регламентный мониторинг рассчитываемых показателей, оценка эффективности принятых мер и в случае её недостаточности, производится их пересмотр и корректировка.

Для проверки возможности реализации предлагаемого подхода, а также его эффективности на практике, был разработан прототип на базе аналитических технологий iRule, использующий описанную методологию. В качестве исследуемого ПО используется сама система iRule и результаты анализа её исходного кода.

Заключение

Реализация предлагаемого метода и использование его на практике показали состоятельность предлагаемого метода, облегчив внедрение процессов РБПО в существующий цикл разработки программного продукта.

Список литературы

1. ГОСТ Р 56939-2024. Национальный стандарт Российской Федерации. Защита информации. Разработка безопасного программного обеспечения. Общие требования (утв. и введен в действие Приказом Росстандарта от 24.10.2024 N 1504-ст).

2. Марков А.С., Антипов И.С., Арустамян С.С., Магакелова Н.А. Сравнительный анализ и выбор статических анализаторов безопасности кода // Вопросы кибербезопасности, 2024. – № 5(63). – С. 79–88, 2024. DOI: 10.21681/2311-3456-2024-5-79-88.

3. Короткий Ю.Ф. Управление рисками в сфере противодействия отмыванию преступных доходов и финансированию терроризма. Вопросы методологии: учебное пособие. Москва: МУМЦФМ, 2020. – 102 с. ISBN 978-5-6044180-7-9.

УДК 004.056

М.К. ЧОКПАРОВ, А.Е. КАРЕТНИКОВ

ООО «Институт проблем безопасности и анализа информации», Москва

ПРОГРАММНЫЙ КОМПЛЕКС «УПРАВЛЕНИЕ РБПО». СПЕЦИАЛЬНЫЕ АНАЛИТИЧЕСКИЕ ТЕХНОЛОГИИ IRULE

В данной статье рассматриваются вопросы применения риск-ориентированного подхода для построения информационно-аналитических систем безопасности. Приведен пример практического использования в этих целях отечественных технологий iRule, отвечающих требованиям и рекомендациям стандартов анализа информации в сфере безопасности.

Программный комплекс «Управление РБПО» (ПК) построен на основе методологии управления рисками, которая детально проработана в рамках проектного управления [1], широко используется по линии финансовых разведок [2, 3], а также в сфере госуправления [4].

В соответствии с основными принципами построения аналитических систем в сфере безопасности ПК охватывает все компоненты аналитического процесса (т.н. Intelligence Cycle): Сбор данных - Оценка и предобработка данных – Систематизация данных в соответствии с аналитической моделью – Анализ данных – Подготовка отчетов, выводов и заключений.

На примере статического анализа уязвимостей разрабатываемого программного продукта (ПП) представлен фрагмент панели управления РБПО в виде свертки (рис. 1), на которой в режиме реального времени отображаются уровни рисков (критичность) для каждой из выявленных уязвимостей, а также соответствующие рейтинги оценок РБПО для каждого из компонентов ПП и для ПП в целом.

Использование простого механизма фильтрации позволяет свертывать панель управления по различным показателям, например, анализировать результаты работы каждого из исполнителей. Таким образом, ПК используется не только в интересах руководства, но и в повседневной работе самими исполнителями, что практически исключает “разночтения” при широком обсуждении результатов РБПО. Кроме того, важно отметить, что с учетом наличия шаблонов для регламентных аналитических материалов проекты отчетных документов и заключений могут формироваться в авторежиме.

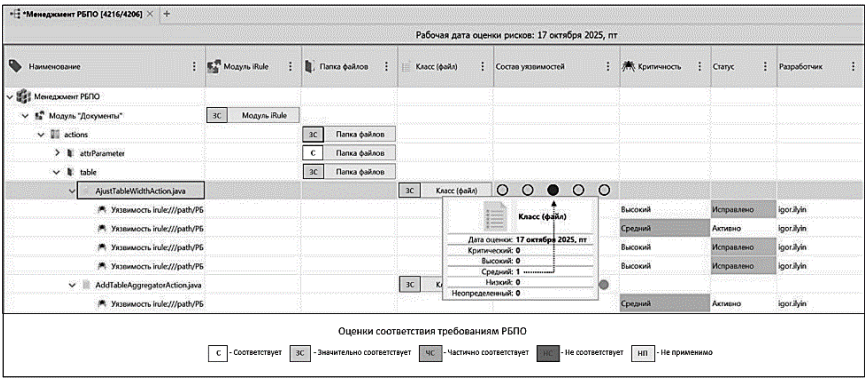


Рис. 1. Фрагмент панели управления РБПО

Реализация ПК выполнена на базе аналитических технологий iRule (Росреестр, номер 3242) и iRule BigData (Росреестр, 5033). Сопоставительный анализ технологий iRule и основных зарубежных аналогов, используемых за рубежом в качестве стандарта «де-факто» для построения аналитических систем в сфере безопасности (i2.group; Raytheon Visual Analytics, Palantir) показывает, что технологии iRule соответствуют требованиям, предъявляемым к базовым аналитическим технологиям, охватывают все этапы аналитического процесса (Intelligence Cycle) и обеспечивают их «бесшовную» интеграцию.

Список литературы

1. Руководство к своду знаний по управлению проектами (Руководство PMBOK®). Шестое издание, Newtown Square, PA: Project Management Institute, 2017 – Перевод на русский язык, издание, оформление издательство «Олимп–Бизнес», 2018. – 1166с. ISBN 9781628251845.

2. Methodology for assessing technical compliance with the FATF recommendations and the effectiveness of aml/cft/cpf systems, February 2022. 251 p. – URL: https://www.fatf-gafi.org/content/dam/fatf-gafi/methodology/FATF-Assessment-Methodology-2022.pdf.coredownload.inline.pdf.

3. Короткий Ю.Ф. Управление рисками в сфере ПОД/ФТ. Вопросы методологии. М.: МУМЦФМ, 2020. – 102 с. ISBN 978-5-6044180-7-9.

4. Integrity Risk Assesment Methodology for Institutions of Central Government, December 2019. 78 p. – URL: https://idmalbania.org/wp-content/uploads/dlm_uploads/2024/03/Integrity-Plan-Methodology-C-Institutions-2020-ENG-002.pdf.

УДК 004.424

М.А. СИМАНОВСКИЙ

Национальный исследовательский ядерный университет «МИФИ», Москва

ПРИМЕНЕНИЕ ПАРАДИГМЫ МЕТАПРОГРАММИРОВАНИЯ ДЛЯ ПОВЫШЕНИЯ БЕЗОПАСНОСТИ НАУКОЕМКОГО ПО

Анализируются общие подходы к разработке научного программного обеспечения. Предлагаются некоторые способы повышения безопасности типов в таком ПО, основанные на принципах утиной типизации и возможностях метапрограммирования современного C++. Обосновывается необходимость использования абстракций времени компиляции в научном программном обеспечении, где традиционно в угоду производительности избегались классические высокоуровневые конструкции, основанные на динамической диспетчеризации.

Современные исследования немыслимы без математического и программного обеспечения, которое стало инструментом, столь же значимым, что и лабораторное оборудование. Проведение компьютерного аналитического и имитационного моделирования и вычислительных экспериментов дают возможности апробации гипотез с существенно меньшими издержками и рисками [1].

Традиционно подходы при создании ПО для бизнеса и науки значительно отличаются. Перспективы долгосрочной поддержки, гибкости, переиспользуемости и читаемости кода, за исключением небольшого числа проектов, отходят на второй план, уступая место скорости разработки и скорости выполнения [2].

Классический полиморфизм в C++ и многих других объектно-ориентированных языках требует использования таблиц виртуальных функций. Работы [3, 4] демонстрируют, как динамическая диспетчеризация способна замедлить выполнение программы по сравнению с более многословными неполиморфными аналогами из-за дополнительных инструкций, кэш-промахов и усложнению предсказаний переходов. Долгосрочная поддержка мономорфных конструкций, создаваемых вручную, при этом в значительной степени усложняется.

В третьей редакции языка C++ вводится механизм для автоматической мономорфизации: шаблоны. Благодаря этому единожды написанный блок кода, параметризованный типом, мог на этапе компиляции быть повторен для каждого используемого типа явно, что позволяет избегать работу с таблицей виртуальных функций во время выполнения программы.

С другой стороны, при использовании шаблонов возникают противоречия с концепцией интерфейсов, которые реализуются обычно как классы из чисто виртуальных функций, а создание виртуальных шаблонных функций вовсе запрещено. При этом все равно остается необходимость описания контрактов для явного определения требований к поведению объектов.

Поведение контрактов может быть воссоздано с помощью шаблонных ограничений, введенных со стандартом C++20, похожих по своей сути на синтез классических интерфейсов и утиной типизации. Вместо явного описания типа с перечислением сигнатур виртуальных методов возможно описать концепт: набор синтаксических правил, предъявляемых к типу, проверяемых на этапе компиляции. При этом не возникает никаких дополнительных отношений наследования, как это происходит в случае с абстрактными классами: тип реализует концепт, если и только если отвечает всем его требованиям, и мономорфизация шаблона нужным типом произойдет лишь в случае удовлетворения ограничений. Использование концептов позволяет формулировать и проверять инварианты непосредственно в исходном коде, частично реализуя методологию корректности по построению [5] и устраняя классы потенциальных ошибок еще до его запуска.

Таким образом, применение метапрограммирования шаблонов с ограничениями и концептами предоставляет не только эффективный механизм создания гибкого программного обеспечения с высоким уровнем абстракции, обеспечивая нулевые накладные расходы времени выполнения, но и существенно снизить риски получения некорректного поведения за счет проверок времени компиляции.

Список литературы

1. Нечаевский А.В. История развития компьютерного имитационного моделирования. Системный анализ в науке и образовании. 2021, 2, с. 103–117.

2. Connolly A., Hellerstein J., Alterman N., Beck D., Fatland R., Lazowska E., Mandava V., & Stone S. Software Engineering Practices in Academia: Promoting the 3Rs—Readability, Resilience, and Reuse. Harvard Data Science Review, 2023, 5(2). doi: 10.1162/99608f92.018bf012

3. Driesen K., Hölzle U. The direct cost of virtual function calls in C++. SIGPLAN. 1996, 31(10), pp. 306–323. https://doi.org/10.1145/236338.236369.

4. Arnold M., Grove D. Collecting and exploiting high-accuracy call graph profiles in virtual machines. International Symposium on Code Generation and Optimization, San Jose, CA, USA, 2005, pp. 51-62, doi: 10.1109/CGO.2005.9.

5. Bordis T., Runge T. & Schaefer I. Correctness-by-construction for feature-oriented software product lines. In Proceedings of the 19th ACM SIGPLAN International Conference on Generative Programming: Concepts and Experiences (GPCE 2020). Association for Computing Machinery, New York, NY, USA, 2020. 22–34 .doi:10.1145/3425898.3426959.

УДК 004.056

В.В. ВОХМИНОВА, Р.О. САДЫКОВА

МИРЭА – Российский технологический университет, Москва

СПОСОБ ПРОТИВОДЕЙСТВИЯ СОСТЯЗАТЕЛЬНЫМ АТАКАМ НА НЕЙРОСЕТЕВЫЕ МОДЕЛИ

В статье рассматриваются современные способы противодействия состязательным (adversarial) атакам на нейросетевые модели, которые представляют собой одну из основных угроз безопасности интеллектуальных систем. Представлены особенности и ограничения каждого метода, а также обоснована необходимость комплексного применения нескольких техник для повышения устойчивости моделей.

Современные нейросетевые модели нашли широкое применение в разнообразных областях, включая компьютерное зрение, обработку естественного языка и системы кибербезопасности. Однако с ростом их популярности возросла и активность атакующих, использующих так называемые состязательные (adversarial) атаки – методы, при которых входные данные намеренно искажаются минимальными, но направленными изменениями для обмана модели [1]. Устойчивость к этим атакам является одной из ключевых задач в обеспечении безопасности и надёжности нейросетевых систем.

Состязательные атаки направлены на создание слегка модифицированных входных данных, которые не заметны человеку, но приводят модель к ошибочной классификации или неверным выводам. Эти атаки могут иметь существенные последствия в критически важных приложениях, таких как автономные транспортные системы и системы биометрической идентификации. Поэтому разработка эффективных методов противодействия этим атакам приобретает первостепенное значение.

Состязательное обучение. Одним из наиболее распространённых методов защиты является состязательное обучение (adversarial training). Метод заключается в расширении тренировочного датасета за счёт генерации и включения в него атакующих примеров с правильными метками [2]. Данный подход позволяет научиться устойчивости к атакам.

Оборонительная дистилляция. Другим перспективным подходом является оборонительная дистилляция. Эта методика основана на концепции дистилляции знаний в машинном обучении, где более сложная модель передаёт информацию более простой [2].

Объяснимый искусственный интеллект и обнаружение атак. Использование методов объяснимого ИИ (XAI) помогает выявлять уязвимые места моделей и анализировать поведение при обработке входных данных [3].

Генеративные методы защиты. Использование генеративных состязательных сетей (например, Defense-GAN) позволяет восстанавливать и очищать входные данные от возможных искажений до их подачи в основную модель, что предотвращает отрицательное влияние атакующих возмущений [4].

Технические меры и укрепление модели. Регуляризация, спектральная нормализация весов, а также оптимизация архитектуры модели и алгоритмов обучения служат дополнительными средствами повышения устойчивости к разнообразным видам атак.

Заключение

В условиях постоянного развития и усложнения атакующих методов необходим комплексный и адаптивный подход к защите нейросетевых моделей. Сочетание таких методов, как состязательное обучение, оборонительная дистилляция, объяснимый ИИ и генеративные подходы, позволяет повысить надёжность и безопасность систем искусственного интеллекта. Однако даже комплексное применение существующих методов не гарантирует абсолютной защиты, поскольку постоянно появляются новые виды атак, что требует непрерывных исследований и разработки адаптивных систем безопасности.

Таким образом, выбор и внедрение эффективных способов противодействия состязательным атакам является основой для обеспечения безопасной эксплуатации нейросетевых моделей в различных сферах человеческой деятельности.

Список литературы

1. Петров В.А., Иванов С.К. Методы защиты искусственного интеллекта от атак: Вестник кибербезопасности. – 2024. – № 12. – С. 45–53.

2. Смирнова Е.В. Состязательные атаки и методы их предотвращения в системах машинного обучения: Информационная безопасность. – 2025. м Т. 18, № 3. – С. 112–121.

3. Козлов Д.П. Оборонительная дистилляция: принципы и применение: Журнал современных технологий. – 2023. – Т. 7, № 4. – С. 33–41.

4. Иванова М.Н. Современные методы защиты интеллектуальных систем: Информационные технологии и безопасность. – 2025. – Т. 10, № 1. – С. 24–30

5. Вероятностный подход к оценке защищённости информации от угроз / М.Ю. Титов, П.И. Карасев, П.Ю. Пушкин, М.М. Титова // Национальная Ассоциация Ученых. – 2021. – № 74-1. – С. 59-61. – DOI 10.31618/NAS.2413-5291.2021.1.74.515. – EDN WSTQMZ.

УДК 004.056

Е.В. СМОЛЕНЧУК

Национальный исследовательский ядерный университет «МИФИ», Москва

РАЗРАБОТКА СИСТЕМЫ АНАЛИЗА ТОНАЛЬНОСТИ КОММЕНТАРИЕВ НА САЙТЕ HABR.COM С ВИЗУАЛИЗАЦИЕЙ В РЕАЛЬНОМ ВРЕМЕНИ

Работа посвящена проектированию решения, позволяющего автоматически определять эмоциональную окраску пользовательских комментариев на технических платформах. Рассмотрены существующие подходы к анализу тональности и выделены их ограничения, а также предложена архитектура системы, сочетающая инструменты сбора, обработки и визуализации данных в едином аналитическом пространстве.

Стремительное развитие информационных технологий и рост популярности интернета привели к кардинальным изменениям в способах обмена информацией. Интернет-пространство наполнено не только публикациями и статьями, но и пользовательским контентом, среди которого особое место занимают комментарии. Активно это можно наблюдать на специализированных платформах, таких как Хабр [1], Hacker News [2] и другие. В отличие от обыденных социальных сетей, комментарии на такого рода платформах насыщены большим количеством специализированной лексики, поэтому не всегда предоставляется возможным понять отношение пользователей к тому или иному новостному событию.

В таких условиях задача автоматизированного анализа комментариев приобретает особую актуальность. Ожидания и потребности аудитории, своевременное реагирование на возникающие проблемы позволяют оперативно выявлять негативное или же позитивное настроение пользователей.

По данным выборочного обследования населения по вопросам использования ИКТ на конец 2023 г. 94,1% населения Российской Федерации пользуются Интернетом, а 84,6% делают это каждый или почти каждый день [3].

В настоящее время существует множество подходов и инструментов для анализа тональности текстов, как в англоязычном, так и в русскоязычном сегменте. Существующие готовые платформенные решения, примером которых является Yandex DataSphere [4], имеют ряд ограничений пользования бесплатной версией, а также зарубежные

аналоги, как NLP Cloud [5], не позволяют использовать расширенную версию на территории Российской Федерации. Таким образом, для анализа комментариев, характеризующихся насыщенностью профессиональной терминологией и специфическим стилем общения, представленные решения не являются оптимальными.

Помимо промышленных решений и платформ, существует значительное количество академических и частных исследований, направленных на поиск эффективных методов анализа тональности. Одно из последних – работа В.В. Васильева «Компьютерный анализ тональности региональных СМИ» [6]. В центре рассмотрения – анализ тональности новостей региональных порталов с целью выявления ключевых тем, эмоциональной окраски и языкового портрета медийных текстов. Автор использует инструменты собственных алгоритмов фильтрации и лемматизации для выявления именованных сущностей и оценки полярности. Особое внимание уделяется сложности передачи тональности при машинном и ручном переводе. Работа подчёркивает ограниченность существующих методов в улавливании коммуникативных оттенков текста и предлагает пути их совершенствования.

Таким образом, реализуя такого рода систему, требуется выбрать эффективные технологии, обеспечивающие высокую точность анализа и скорость обработки данных, а также их безопасность. Архитектура должна включать необходимый минимум компонентов на этапах разработки: сбор данных, обработка текста и обучение моделей, безопасное хранение, серверная часть и визуализация.

Список литературы

1. Хабр — платформа коллективных блогов. [Электронный ресурс]. – URL: https://habr.com/ru/ – (дата обращения: 21.09.2025).

2. Hacker News – социальная новостная площадка для обсуждения IT-тем и стартапов. [Электронный ресурс]. – URL: https://news.ycombinator.com/ – (дата обращения: 21.09.2025).

3. Регионы России. Социально-экономические показатели. 2024 [Электронный ресурс]. – URL: https://rosstat.gov.ru/storage/mediabank/Region_Pokaz_2024.pdf – (дата обращения: 21.09.2025).

4. Яндекс DataSphere. [Электронный ресурс]. – URL: https://datasphere.yandex.cloud – (дата обращения: 21.09.2025).

5. Google Cloud Natural Language API. [Электронный ресурс]. – URL: https://cloud.google.com/natural-language – (дата обращения: 21.09.2025).

6. Васильев В.В. Компьютерный анализ тональности региональных СМИ // Теория и практика современной науки. – 2025. – №1(115). – URL: https://cyberleninka.ru/article/n/kompyuternyy-analiz-tonalnosti-regionalnyh-smi – (дата обращения: 28.09.2025).

УДК 004.056

М.Д. АВЕРЧЕНКО, И.А. ТКАЛИЧ, Е.Е. ПОНЯЕВ

Национальный исследовательский ядерный университет «МИФИ», Москва

РАЗРАБОТКА БЕЗОПАСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ С ИСПОЛЬЗОВАНИЕМ МЕТОДОВ СТАТИЧЕСКОГО АНАЛИЗА КОДА

Рассматриваются методы повышения безопасности программного обеспечения с использованием инструментов статического анализа кода. Приводится краткая характеристика подходов и типовых уязвимостей, а также результаты сравнительного анализа SonarQube, PVS-Studio и CodeQL. Комбинированное применение анализаторов повышает полноту выявления уязвимостей более чем на 25%. Отмечаются перспективы развития отечественных решений и использование машинного обучения для автоматизации анализа.

Введение

Рост числа инцидентов информационной безопасности требует внедрения мер защиты уже на этапе разработки ПО [1]. Подход *Security by Design* ориентирован на предотвращение уязвимостей, а не их устранение. Важным инструментом такого подхода является статический анализ кода, позволяющий выявлять ошибки до компиляции программы.

Интеграция анализа в процессы DevSecOps обеспечивает постоянную проверку кода в CI/CD и формирует культуру безопасной разработки [2].

1. Методы и типовые уязвимости

Статический анализ – исследование исходного кода без его выполнения. Основные методы:

- синтаксический и семантический анализ (проверка структуры и типов данных);
- межпроцедурный анализ (взаимосвязи между функциями);
- абстрактная интерпретация (моделирование поведения программы) [3];
- поиск по шаблонам уязвимостей.

Инструменты анализа позволяют выявлять переполнение буфера, SQL-инъекции, ошибки обработки исключений и нарушения доступа. По данным OWASP, до 70 % критических уязвимостей обнаруживаются на уровне исходного кода.

2. Практическое исследование

Для оценки эффективности проведено сравнение инструментов SonarQube, PVS-Studio и CodeQL на двух открытых проектах: веб-

приложении на Python (Django) и библиотеке на C++. Измерялись три показателя – количество уязвимостей, ложные срабатывания и время анализа (табл. 1).

Таблица 1. Результаты анализа

Инструмент	Найдено уязвимостей	Ложные срабатывания	Время (мин)
SonarQube	36	5	4
PVS-Studio	48	8	6
CodeQL	42	4	9

PVS-Studio показал наибольшую полноту, CodeQL – лучшую точность, SonarQube – оптимальную скорость и простоту интеграции. Совместное использование SonarQube и CodeQL повысило полноту обнаружения на 28% и снизило ложные срабатывания на 15%.

3. Интеграция и перспективы

Внедрение статического анализа в CI/CD обеспечивает автоматическую проверку при каждом коммите и контроль устранения дефектов через системы Jira и GitLab. Отечественные решения – *Svace*, *Kaspersky Static Analyzer*, *CodeSealer* – соответствуют требованиям ФСТЭК и ГОСТ Р 56939–2016 [4].

Перспективные направления – объединение SAST и DAST, а также использование машинного обучения для интеллектуального поиска уязвимостей.

Заключение

Статический анализ кода является эффективным инструментом повышения безопасности программного обеспечения. Применение нескольких анализаторов обеспечивает оптимальный баланс между точностью и полнотой. Интеграция анализа в DevSecOps-процессы формирует непрерывный контроль качества кода и способствует развитию культуры безопасной разработки.

Список литературы

1. McGraw, G. *Software Security: Building Security In.* Addison-Wesley, 2006.
2. Shostack, A. *Threat Modeling: Designing for Security.* Wiley, 2014.
3. Chess, B., & West, J. *Secure Programming with Static Analysis.* Addison-Wesley, 2007.
4. Касперский, Е. *Методы автоматизированного анализа кода: отечественные решения.* // Информационная безопасность, № 3, 2024.

УДК 004.056

К.Г. ГАВДАН

Обнинский институт атомной энергетики филиал НИЯУ МИФИ

РЕШЕНИЯ СУЩЕСТВУЮЩИХ ПРОБЛЕМ РАЗРАБОТКИ БЕЗОПАСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

В работе представлены результаты системного анализа современных подходов и методов обеспечения безопасности программного обеспечения (ПО) на этапе разработки. Исследование сфокусировано на процессах создания защищенного ПО в условиях меняющихся киберугроз. На основе анализа научных публикаций и практик IT-компаний выявлены и систематизированы ключевые проблемы в области разработки безопасного ПО. Полученная классификация актуальных вызовов и нерешенных задач создает основу для дальнейшего совершенствования методологий безопасности и определения перспективных направлений исследований в области защиты программного обеспечения.

Введение

Продолжающийся рост количества и сложности целенаправленных кибератак обусловливает повышенные требования к безопасности программного обеспечения (ПО) на всех этапах его жизненного цикла. Несмотря на усилия IT-сообщества, проблема создания защищенного ПО остается нерешенной, что подтверждается устойчивой динамикой финансовых потерь организаций от инцидентов информационной безопасности [1]. В этих условиях разработка эффективных подходов к обеспечению безопасности на этапе создания ПО становится критически важной задачей [2].

Особую сложность в Российской Федерации придает нормативно-правовой контекст. Согласно постановлению Правительства РФ №608, в стране действуют три регулятора в области информационной безопасности (ИБ): Министерство обороны РФ, ФСБ России и ФСТЭК России. Каждый из регуляторов организует самостоятельную систему лицензирования и сертификации средств защиты информации (СЗИ) по требованиям безопасности информации (ТБИ) [1]. На практике это приводит к тому, что требования к безопасному ПО в разных системах сертификации имеют существенные, а подчас и принципиальные особенности, что усложняет процесс разработки. Таким образом, процесс создания безопасного ПО сталкивается с комплексом проблем [1] к ужесточающимся регуляторным требованиям. Настоящее исследование направлено на анализ существующих проблем и методов их решения в области разработки безопасного ПО, что и определяет его актуальность.

Подходы и методы решения существующих проблем

Как с описанными выше проблемами предлагается бороться?

а) внедрение культуры безопасности (Security Culture):

– обучение и повышение осведомленности разработчиков;

– введение роли Security Champion в командах;

б) интеграция безопасности в жизненный цикл разработки (SDLC):

– Модель DevSecOps: «Сдвиг безопасности влево»;

– Практики: статический и динамический анализ, анализ зависимостей;

в) следование стандартам и лучшим практикам:

– Принципы безопасного проектирования: например, Defense in Depth;

– Использование проверенных фреймворков и шаблонов.

Заключение

Установлено, что разработка БПО является не набором разрозненных мер, а целостным, системным и целенаправленным процессом, который должен быть интегрирован во все этапы жизненного цикла ПО – от проектирования до эксплуатации. Ключевым фактором успешности этого процесса является преодоление кадрового дефицита: эффективность методологий БПО критически зависит от уровня компетенции и осведомленности сотрудников в данной предметной области.

В качестве перспективных направлений для повышения гарантий безопасности необходимо выбрать: внедрение инструментов статического и динамического анализа для автоматизированного поиска уязвимостей; применение методов формальной верификации для математически строгого доказательства отсутствия дефектов в критически важных модулях; развитие процессов DevSecOps для обеспечения непрерывности контроля безопасности. Таким образом, достижение высокого уровня защищенности ПО возможно лишь при сочетании системного подхода, постоянного развития компетенций персонала и интеграции передовых инструментальных средств в процесс разработки.

Список литературы

1. Арустамян, САС С.; Вареница, Виталий В.; Марков, Алексей С.. методические и реализационные аспекты внедрения процессов разработки безопасного программного обеспечения. Безопасность информационных технологий, [S.l.], v. 30, n. 2, p. 23-37, мая 2023. ISSN 2074-7136. Доступно на: <https://bit.spels.ru/index.php/bit/article/view/1499>. Дата доступа: 23 окт. 2025. doi:http://dx.doi.org/10.26583/bit.2023.2.01. (дата обращения: 10.09.2025).

2. Как избежать ошибки при безопасной разработке программного обеспечения / В.В. Вареница, В.Л. Цирлов и др.; под ред. д-ра техн. наук А.С. Маркова – М.: Квант-медиа, 2025. – 334 с.: ил. 89-97.ISBN 978-5-6053386-1-1 (дата обращения: 14.09.2025).

УДК 004.056

А.П. КИМ, И.М. ЕФРЕМОВ, И.И. ЗОЛОТОВ

МИРЭА – Российский технологический университет, Москва

РАЗРАБОТКА СИСТЕМЫ АНАЛИЗА БЕЗОПАСНОСТИ ИСХОДНОГО КОДА НА ЯЗЫКЕ PYTHON С ГРАФИЧЕСКИМ ИНТЕРФЕЙСОМ

В настоящее время наблюдается значительное количество случаев взломов и атак в информационном пространстве. Современные системы подвергаются различным угрозам, и поэтому важно проводить анализ его исходного кода на предмет возможных уязвимостей. Цель данной работы – предоставить разработчикам инструмент для выявления уязвимостей на ранних этапах разработки. Разработанная система выявляет распространённые уязвимости и формирует отчет с указанием их расположения в коде.

На фоне существующих решений (Bandit – мощные AST-правила; Semgrep – кросс-языковые паттерны; Gitleaks – сканирование секретов), наш подход делает акцент на объяснимости: каждое срабатывание сопровождается сниппетом, правилом и уровнем критичности. Мы формализуем набор минимально необходимых практик: запрет yaml.load без безопасного загрузчика, детект subprocess.*(shell=True), фиксация requests (…, verify-False), предупреждение о hashlib.md5/sha1, поиск ключей и JWT-токенов. Эта основа для дальнейшего развития, а также включения анализа потоков данных и обучения правил на эмпирике баг-репортов. Исходный код, реализованного ПО, расположен на GitHub [1].

Архитектура системы

Система анализа безопасности состоит из нескольких основных компонентов:

1) В основе модуля анализа лежит разбор абстрактного синтаксического дерева (AST) исходного кода Python. С помощью модуля выполняется парсинг кода в древовидную структуру, отражающую синтаксис программы. Анализ на уровне AST предоставляет инструменту структурированное представление кода, позволяя распознавать элементы программы без потери контекста [2]. Это существенно повышает точность обнаружения уязвимых конструкций по сравнению с поиском по сырым текстовым шаблонам.

2) Поиск по регулярным выражениям. Помимо AST-анализа, в системе применяются регулярные выражения для поиска конкретных

небезопасных шаблонов, которые проще выявить на уровне текста исходного кода. Комбинация семантического разбора и синтаксического поиска повышает покрытие анализа: AST обеспечивает понимание структур кода, а regex позволяет быстро находить простые характерные фрагменты [3].

3) Графический интерфейс пользователя (GUI). Для удобства пользователей реализован графический интерфейс с помощью стандартной библиотеки Tkinter. GUI предоставляет форму для выбора файлов или проектов на Python, настройки параметров анализа и запуска проверки через нажатие кнопки.

4) Отчётность. Пользователь может сортировать и просматривать детали каждой найденной проблемы. Система показывает уязвимости с уровнями риска (HIGH, MEDIUM, LOW, INFO), указывая файл, строку, тип и фрагмент кода. Каждый результат включает информацию о файле, строке, колонке, типе уязвимости и найденном фрагменте кода.

Заключение

Предложенная система демонстрирует, что гибрид AST+regex при компактном наборе правил способен покрыть критичные классы уязвимостей в Python с хорошей объяснимостью результатов. К сильным сторонам относим: контекстный анализ вызовов, единое ядро для GUI/CLI, встроенный отчёт и сниппеты, локальность и независимость от облака. По сравнению с аналогами: Bandit обеспечивает больше правил и зрелость экосистемы, но лишён встроенного GUI; Semgrep даёт кросс-языковую систему и гибкие паттерны, но требует длительного обучения и нередко шире класс правил, чем нужно начинающей команде; секрет-сканеры (Gitleaks) точные в своих задачах, но не анализируют семантику кода.

Список литературы

1. GitHub. SecScanPY – система анализа безопасности исходного кода на Python [Электронный ресурс]. – Режим доступа: https://github.com/Forman75/SecScanPY (дата обращения 08.10.2025).

2. Python Software Foundation. Модуль ast – абстрактные синтаксические деревья [Электронный ресурс]. – Документация Python 2024. – Режим доступа: https://docs.python.org/3/library/ast.html (дата обращения 06.10.2025).

3. Bhargav A. Semgrep: The Easiest SAST Tool For Developers [Электронный ресурс]. – AppSecEngineer Blog, 21.06.2024. – Режим доступа: https://www.appsecengineer.com/blog/semgrep-the-easiest-sast-tool-for-developers-and-everyone-else (дата обращения: 06.10.2025).

УДК 681.5.01:681.5.015.44

А.А. КОРМУХИН, С.В. КТИТРОВ

Национальный исследовательский ядерный университет «МИФИ», Москва

МОДИФИКАЦИЯ ФИЛЬТРА КАЛМАНА ДЛЯ ПОВЫШЕНИЯ БЕЗОПАСНОСТИ РАБОЧИХ РЕЖИМОВ КУСОЧНО-ЛИНЕЙНЫХ СИСТЕМ УПРАВЛЕНИЯ

Рассматривается эффективность методов Калмановской фильтрации в задаче борьбы с воздействиями шумов обратной связи в кусочно-линейных системах управления для обеспечения успешного подавления автоколебаний. На примере моделирования системы третьего порядка применимость фильтра Калмана (ФК), моделирующего синусоиду, многоканального (многомодельного) классического ФК и расширенного ФК.

Автоколебания – незатухающие колебания, свойственные нелинейным системам, возникновение и параметры которых определяются внутренними свойствами системы и не зависят от начального её состояния. Наличие автоколебаний в системе способно привести к различным нежелательным эффектам, от понижения стабильности и быстродействия системы, до непредсказуемости её поведения, в результате чего возрастают риски отказов и поломок оборудования, возникновения потенциально опасных ситуаций. Подавление автоколебаний – важная задача, решение которой затрудняется наличием шумов в сигнале, борьба с которыми требует применения различных алгоритмов фильтрации, таких как фильтр Калмана.

В общем случае, рассматриваемая система может быть описана структурной схемой, приведенной на рис. 1.

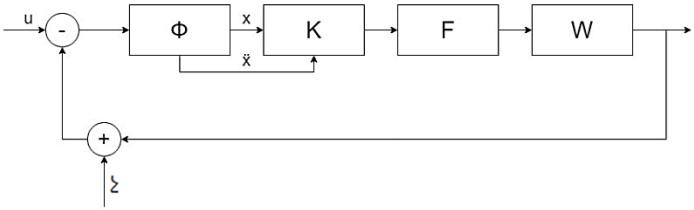


Рис. 1. Схема кусочно-линейной системы

На рис. 1 обозначены: W – передаточная функция системы, F – кусочно-линейная функция, K – однородное управление, задаваемое формулой

ниже, зависящее от параметра ω, который должен быть строго меньше частоты автоколебаний системы:

$$K(x,\dot{x}) = x + 0.5(|x - |\frac{\dot{x}}{\omega}|| - |x + |\frac{\dot{x}}{\omega}||), \quad (1)$$

Ф – фильтрующий элемент, в данном случае фильтр Калмана, ξ – шум.

Классический фильтр Калмана [1, 2], рассчитанный на линейные системы, в явном виде не может быть применен к данной системе. Было рассмотрено два подхода для адаптации классического ФК под данную систему. Первый подход – использование линейного ФК, построенного на основе модели линейных синусоидальных колебаний с частотой автоколебательной системы, не обеспечил решение задачи. Второй – многомодельный подход, заключающийся в построении модели динамики системы для каждого линейного участка кусочно-линейной функции F.

Также был использован расширенный фильтр Калмана [3, 4], являющийся широко используемой во многих инженерных областях модификацией классического фильтра Калмана, предназначенной для работы с нелинейными системами.

Проведено моделирование динамики системы с кусочно-линейной функцией F типа ограничение, и передаточной функцией W, заданной формулой:

$$W(p) = \frac{K}{p(T_1 p+1)(T_2 p+1)}. \quad (2)$$

Предложенный метод формирования фильтра Калмана на основе участков линейности кусочно-линейной системы в составной форме позволяет применять результирующий составной (многомодельный) фильтр для решения задачи фильтрации в нелинейной системе. При моделировании применение составного фильтра Калмана, процедура синтеза которого является более простой, и расширенного фильтра Калмана дало стабильные, хорошие результаты, сопоставимые по качеству друг с другом, что говорит о работоспособности предложенного подхода.

Список литературы

1. Kalman R.E. A New Approach to Linear Filtering and Prediction Problems // Transactions of the ASME (American Society of Mechanical Engineers). Journal of Basic Engineering. 1960. Vol. 82 (1). P. 35–45.

2. Alex Becker. Kalman filter from the ground up – 2-nd edition. https://www.kalmanfilter.net/ (дата обращения 03.03.2025)

3. Leonard A. McGee, Stanley F. Schmidt. Discovery of the Kalman Filter as a Practical Tool for Aerospace Industry. 1985. NASA Technical Memorandum 86847.

4. Einicke G.A. Smoothing, Filtering and Prediction. Estimating the Past, Present and Future 2-nd Edition. – Prime publishing – Amazon.com, 2019.

УДК 004.056

М.А. ЛАПИНА, А.Р. БАГАУТДИНОВА,
Р.В. РЫСЬКОВ, В.Г. ЛАПИН

Северо-Кавказский федеральный университет, Ставрополь

ИССЛЕДОВАНИЕ МЕТОДОВ МАШИННОГО ОБУЧЕНИЯ ДЛЯ ОБНАРУЖЕНИЯ ВРЕДОНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ В ОПЕРАЦИОННОЙ СИСТЕМЕ ANDROID

Проведен сравнительный анализ различных алгоритмов машинного обучения, таких как дерево решений, случайный лес, деревья градиентного бустинга, ансамбль деревьев, логистическая регрессия, нечеткие правила и устойчивый многослойный перцептрон с обратным распространением. Оценена их эффективность на реальном наборе данных вредоносных и безопасных приложений. Наилучшей моделью оказался многослойный перцептрон с обратным распространением с F-мерой 0,942.

Актуальность

С развитием технологий смартфоны стали неотъемлемой частью нашей жизни. Однако с ростом их популярности, возросло количество вредоносного ПО, нацеленного на пользователей мобильных устройств, в частности операционной системы (ОС) Android [1]. Вредоносные приложения крадут личные данные, подписывают пользователей на платные сервисы и выполняют другие действия без его ведома.

Традиционные методы обнаружения вредоносного ПО, такие как сигнатурный, эвристический анализ не всегда эффективны из-за постоянного усовершенствования атак, вредоносных приложений и появления новых способов обхода защитных механизмов. Альтернативой традиционных методов является использование машинного обучения для автоматического выявления вредоносного ПО [2]. Инструментом, который предоставляет удобную платформу для работы с такими моделями, является KNIME.

Методология исследования

Исследование проведено с использованием платформы KNIME на реальном наборе данных "Dataset malware/beningn permissions Android", содержащем информацию о разрешениях, запрашиваемых приложениями. Набор данных включает 331 колонку (330 разрешений и целевая колонка "type"). Далее был выполнен отбор данных, в результате чего осталось 57 наиболее значимых разрешений [3].

Анализируемые модели

Были исследованы следующие алгоритмы машинного обучения: дерево решений, случайный лес, деревья градиентного бустинга, ансамбль деревьев, логистическая регрессия, нечеткие правила, вероятностная нейронная сеть, устойчивый многослойный перцептрон с обратным распространением и k-ближайших соседей [2]. Для уменьшения размерности признаков использовался метод главных компонент (PCA).

Результаты исследования

По результатам анализа PCA с использованием F-меры в качестве метрики были выделены пять лучших моделей: логистическая регрессия (F-мера 0,937), устойчивый многослойный перцептрон с обратным распространением (F-мера 0,935), ансамбль деревьев (F-мера 0,929), k-ближайших соседей (F-мера 0,921) и случайный лес (F-мера 0,921). После дополнительной настройки гиперпараметров наилучший результат показал устойчивый многослойный перцептрон с обратным распространением с F-мерой 0,942.

Заключение

Наилучшей моделью для обнаружения вредоносного программного обеспечения в операционной системе Android оказался устойчивый многослойный перцептрон с обратным распространением. Исследование подтвердило эффективность методов машинного обучения для автоматического выявления вредоносных приложений на основе анализа запрашиваемых разрешений с использованием платформы KNIME.

Список литературы

1. Yerima S.Y. et al. A new android malware detection approach using bayesian classification //2013 IEEE 27th international conference on advanced information networking and applications (AINA). – IEEE, 2013. – С. 121–128.

2. S.Y. Yerima, S. Sezer, G. McWilliams. “Analysis of Bayesian Classification Based Approaches for Android Malware Detection” IET Information Security, Volume 8, Issue 1, January 2014, p. 25–36, Print ISSN 1751-8709, Online ISSN 1751-8717. DOI: 10.1049/iet-ifs.2013.0095.

3. Dataset malware/beningn permissions Android // kaggle URL: https://www.kaggle.com/datasets/xwolf12/datasetandroidpermissions.

УДК 004.056

А.С. ВИРЯСОВ, А.П. СЛУЧЕВСКАЯ

МИРЭА – Российский технологический университет, Москва

ПРЕДОТВРАЩЕНИЕ И БОРЬБА С АТАКАМИ ТИПА ОТКАЗ В ОБСЛУЖИВАНИИ НА ОСНОВЕ ПРОФИЛИРОВАНИЯ В ИНТЕРПРЕТИРУЕМЫХ ЯЗЫКАХ ПРОГРАММИРОВАНИЯ

Работа посвящёна оценке эффективности алгоритмических решений и влияния особенностей интерпретируемых языков на возникновение отказов в обслуживании. Рассматриваются методы профилирования программного кода, включая оценку алгоритмической сложности с помощью о-символики (Big O notation), а также практические подходы к решению выявленных проблем.

Введение

Современное программное обеспечение становится всё более сложным и функциональным, что требует внимательного анализа и оптимизации кода для обеспечения стабильности работы [1].

Особое значение при этом приобретает взаимодействие с компилятором и средой выполнения. В ходе исследования была разработана программа для оценки сложности алгоритмов на разных языках программирования.

Было выявлено, что время выполнения алгоритма на языке C# существенно зависит не только от самого кода, но и от таких факторов среды, как сборщик мусора и интерпретатор, что может привести к ухудшению производительности даже при теоретически оптимальной сложности.

Борьба с атаками типа отказ в обслуживании на основе профилирования в интерпретируемых языках программирования

Для предотвращения подобных проблем важным инструментом является профилирование – процесс анализа производительности, позволяющий выявлять узкие места в коде и повышать его эффективность. Профилирование включает три этапа: сбор данных о работе программы (время, число вызовов, память), анализ полученных показателей и оптимизацию на основе результатов [2]. При этом используются специализированные средства, адаптированные под конкретные языки программирования.

Методология анализа сложности алгоритмов с помощью о-символики (Big O notation) позволяет оценить асимптотическое поведение времени

выполнения или использования памяти в зависимости от объёма входных данных.

Существуют различные классы сложности, от самых эффективных к наименее эффективным:

- Константная O(1) – самое быстрое время выполнения
- Экспоненциальное $O(2^n)$ – самое медленное время выполнения

Время выполнения функции пропорционально количеству базовых операций (сложение, присваивание и т.д.), которые она выполняет. Количество этих операций зависит от размера задачи (например, количества элементов в массиве).

При оценке сложности нас обычно не интересует точное число операций. Вместо этого мы анализируем, как это число растет относительно размера задачи.

Основное внимание уделяется пониманию прироста операций при увеличении размера задачи, чаще всего в худшем сценарии.

Заключение

Таким образом, для построения отказоустойчивых программных систем, способных противостоять современным угрозам отказа в обслуживании, особо важной вещью представляется внедрение комплексного и многоуровневого подхода.

Данный подход должен сочетать в себе теоретический анализ, включая в себя оценку вычислительной сложности и асимптотического поведения алгоритмов. Особое внимание при этом необходимо уделять специфике исполнения кода в интерпретируемых средах, которые могут давать дополнительную вычислительную нагрузку. Такой подход поможет создать комплексую защиту от атаки типа отказ в обслуживании [3].

Список литературы

1. Чернов Д. DDoS-атаки в 2022 и методы защиты от них [Электронный ресурс] // Habr. – URL: https://habr.com/ru/companies/slurm/articles/674218/ (дата обращения: 08.10.2025).

2. Скородумов А. Защита от DDoS-атак. Опыт и практика [Электронный ресурс] // SecuTeck.ru. – 17.11.2022. – URL: https://www.secuteck.ru/articles/zashchita-ot-ddos-atak-opyt-i-praktika (дата обращения: 08.10.2025).

3. Кадыров Р.Р. Методы обнаружения и предотвращения DDOS-атак [Электронный ресурс] // Политехнический молодежный журнал. – 2019. – № 07. – URL: https://ptsj.ru/articles/507/507.pdf (дата обращения: 08.10.2025).

УДК 004.056

А.Е. ПЕРВЫХ, А.В. ПОЛЯКОВА

МИРЭА – Российский технологический университет, Москва

ОБЗОР СОВРЕМЕННЫХ ТЕХНОЛОГИЙ ГЕНЕРАТИВНОГО ИСКУССТВЕННОГО ИНТЕЛЛЕКТА И ЯЗЫКОВЫХ МОДЕЛЕЙ

В статье представлен обзор современных направлений развития генеративного искусственного интеллекта (ИИ) и больших языковых моделей. Описаны принципы их архитектуры, механизмы обучения и адаптации, а также особенности применения в задачах программирования. Проведён сравнительный анализ наиболее известных моделей, таких как GPT-4, Gemini, Claude, LLaMA и DeepSeek. Отмечены тенденции к мультимодальности, повышению эффективности и созданию автономных ИИ-агентов. Сделаны выводы о перспективах дальнейшего развития технологий генеративного ИИ.

Введение

Генеративный искусственный интеллект (Generative AI) представляет собой класс моделей машинного обучения, способных создавать новые данные, статистически схожие с обучающими примерами. В основе большинства современных решений лежит архитектура трансформера, предложенная в работе [1], которая позволила эффективно обучать модели на огромных объёмах текстов и кодов. Большие языковые модели (LLM) стали центральным элементом этой технологии. Они обучаются на триллионах токенов, охватывающих естественный язык, программный код, документацию и даже мультимодальные данные. В результате модели, такие как GPT-4, Claude, Gemini или DeepSeek, способны не только обрабатывать текст, но и писать программы, анализировать изображения, понимать схемы и решать задачи логического характера.

Обзор современных технологий генеративного искусственного интеллекта и языковых моделей

Современные языковые модели различаются по степени открытости и специализации. Открытые решения, такие как Meta LLaMA 3 или DeepSeek Coder, позволяют исследователям адаптировать модели под собственные нужды, модифицировать архитектуру и дообучать их на специфичных данных [2]. Проприетарные системы, например OpenAI GPT-4, Google Gemini или Anthropic Claude, предоставляют доступ через API, предлагая высокую точность и готовую инфраструктуру, но ограничивая возможности кастомизации. Современные архитектуры

активно развиваются в сторону повышения эффективности. Модели на основе Mixture-of-Experts (MoE) позволяют включать только часть параметров при обработке конкретного запроса, снижая вычислительные затраты. Параллельно растёт интерес к методам параметро-эффективного дообучения (PEFT), таким как LoRA и Prompt Tuning, которые делают адаптацию больших моделей доступной для исследователей и компаний среднего уровня. В перспективе ожидается появление более лёгких и энергоэффективных моделей, которые смогут работать локально без подключения к облаку [3]. Также активно развиваются технологии создания автономных ИИ-агентов, способных самостоятельно выполнять многошаговые задачи: писать и тестировать код, и оптимизировать процессы разработки. Такие агенты уже начинают интегрироваться в корпоративные системы, формируя основу для нового поколения интеллектуальных инструментов [4].

Заключение

Таким образом, генеративный искусственный интеллект переживает этап стремительного развития. Большие языковые модели становятся универсальными инструментами, способными решать широкий спектр задач — от автоматизации кодирования до поддержки принятия решений. Их дальнейшее совершенствование, связанное с безопасностью, персонализацией и снижением ошибок, определит будущее программной инженерии и цифровых технологий в целом. В ближайшие годы можно ожидать не только улучшения качества генерации, но и более глубокой интеграции ИИ в инфраструктуру разработки, что сделает взаимодействие человека и машины ещё более продуктивным и естественным.

Список литературы

1. Савельев А.В., Глухова И.О. Развитие отечественных генеративных моделей искусственного интеллекта: состояние и перспективы. Информационные технологии и вычислительные системы, 2024, № 2(98), с. 7–18. DOI: http://dx.doi.org/10.21455/itvs.2024.2.1.

2. Белов Р.С., Князева Л.А. Архитектура и обучение больших языковых моделей: анализ современных решений. Труды Института системного программирования РАН, 2023, т. 35, № 4, с. 42–56. DOI: http://dx.doi.org/10.15514/ISPRAS-2023-35(4)-03.

3. Дьячков П.Н., Орлова Е.В. Использование языковых моделей в задачах автоматизации программирования. Вестник Московского государственного технического университета им. Н.Э. Баумана. Сер. Информатика и системы управления, 2023, № 5, с. 29–41. DOI: http://dx.doi.org/10.18698/0236-3933-2023-5-29-41.

4. Синицын В.А., Руденко Д.С. Методы повышения эффективности генеративных языковых моделей на отечественных вычислительных платформах. Научно-технический вестник информационных технологий, механики и оптики, 2024, т. 24, № 2, с. 63–72. DOI: http://dx.doi.org/10.17586/2226-1494-2024-24-2-63-72.

УДК 004.891.2

А.Д. ЧЕРНЯВСКИЙ, В.С. КИРЕЕВ
Национальный исследовательский ядерный университет «МИФИ», Москва

ОЦЕНКА ТОЧНОСТИ РАБОТЫ ВОПРОСНО-ОТВЕТНОЙ СИСТЕМЫ ДЛЯ ПОДДЕРЖКИ УЧЕБНОГО ПРОЦЕССА

За последние годы в системе образования произошли серьёзные перемены, вызванные в первую очередь развитием технологий. Так, данные с сайта Яндекс Вордстат [1] показывают устойчивую тенденцию к популяризации самообучения за последние 5 лет. В связи с этим, целью работы является усовершенствование вопросно-ответной системы, а именно – создание программных компонентов для определения корректности ее ответов.

Были поставлены задачи, выполнение которых позволит достичь цели работы. Так, первой задачей являлось проведение сравнительного анализа существующих вопросно-ответных систем (результаты анализа представлены в табл. 1).

Таблица 1. Сравнительная характеристика существующих решений (вопросно-ответных систем)

Решение	Пользовательский интерфейс	Источники информации	Ключевая особенность
Разрабатываемое решение	У приложения присутствует Telegram-бот, вопросы можно задавать через него	База знаний определенного курса, реализованная в виде графа с использованием Neo4j	Использована технология GraphRAG, за счет чего уменьшается время ответа на вопрос и повышается точность
CQACD	Есть (вопросы можно задать через диалоговую систему на платформе) [3]	Основной – BCKO (Basic Computer Knowledge Ontology) и дополнительный – WordNet	Наличие библиотеки шаблонов для ввода вопросов
MCQA	Есть (диалоговая система на платформе)	Платформа MOOC (Massive Open Online Courses)	Есть алгоритм разделения «профессиональных» вопросов и «пустых»

Второй задачей был разбор возможных подходов к оценке точности. Был сделан вывод, что надежная стратегия оценки не опирается на один подход, а использует сравнительную и последовательную структуру: офлайн-тестирование для первоначального отбора алгоритмов, пользовательские исследования для уточнения пользовательского опыта и окончательную валидацию посредством контролируемых онлайн экспериментов для подтверждения эффективности и ценности в реальных условиях [2]

Далее, на основании результатов данного анализа был выбран собственный подход для оценки точности разработанной вопросно-ответной системы. Этот подход основан на технологии «LLM as a judge», который предполагает оценку достоверности и релевантности ответов нейросетевой модели системы рядом других нейросетевых моделей с некоторыми предварительными операциями.

Далее было проведено моделирование работы всей системы и работы функции оценки точности (диаграмма прецедентов, диаграмма состояний, диаграмма деятельности). В частности, на диаграмме прецедентов были указаны возможные сценарии взаимодействия пользователей с вопросно-ответной системой в зависимости от роли пользователя (учащийся, преподаватель, администратор).

Следующей задачей был анализ и выбор программных инструментов для доработки приложения (а именно, языков программирования, фреймворков, IDE и т.д.). Финальной задачей была программная реализация функции оценки точности приложения вопросно-ответной системы (написание программного кода).

Список литературы

1. 3456-2023-1-2-12. Яндекс Вордстат. Официальный сайт [Электронный ресурс]. URL: https://wordstat.yandex.ru/ (дата обращения: 10.07.2025).

2. Vu T., Moschitti A. AVA: an automatic evaluation approach to question answering systems //arXiv preprint arXiv:2005.00705. – 2020.

3. Wen Y., Zhu X., Zhang L. CQACD: A concept question-answering system for intelligent tutoring using a domain ontology with rich semantics //Ieee Access. – 2022. – Т. 10. – С. 67247–67261.

УДК 004.056

Н.Е. ПЕТРОВ

МИРЭА – Российский технологический университет, Москва

СОВРЕМЕННЫЕ ТРЕНДЫ ПОВЫШЕНИЯ УРОВНЯ БЕЗОПАСНОСТИ БАЗ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

В статье рассматриваются современные тренды и подходы к повышению уровня безопасности баз данных в информационных системах в 2025 году. Описывается роль искусственного интеллекта и автоматизации в обеспечении проактивной защиты от киберугроз, а также внедрение модели безопасности Zero Trust, предполагающей постоянную проверку подлинности и минимизацию прав доступа. Полученные результаты подчеркивают необходимость интеграции многоуровневого подхода и использования передовых технологий для обеспечения надежной и гибкой защиты баз данных в условиях возрастающих киберугроз.

Введение

В условиях стремительного роста объёмов и значимости данных в информационных системах критически возрастает роль безопасности баз данных. К 2025 г. наблюдается формирование новых тенденций и подходов, направленных на повышение устойчивости и защиты данных от многочисленных киберугроз. Данная статья посвящена обзору основных современных трендов безопасности баз данных, раскрывающих интеграцию передовых технологий и стратегий защиты информации.

Искусственный интеллект и автоматизация

Одним из ключевых трендов является применение искусственного интеллекта (ИИ) и автоматизированных систем для обеспечения безопасности баз данных. Современные решения используют алгоритмы машинного обучения и анализа поведения для выявления аномалий в режиме реального времени, что позволяет оперативно обнаруживать и нейтрализовать попытки несанкционированного доступа и внутренние угрозы. Автоматизация процессов реагирования на инциденты с использованием платформ SOAR (Security Orchestration, Automation and Response) и XDR (Extended Detection and Response) способствует снижению времени реакции и повышению эффективности защиты данных.

Архитектура Zero Trust: новая парадигма безопасности

Вторая значимая тенденция – повсеместное внедрение модели Zero Trust, основанной на принципе «никому и ничему не доверять по

умолчанию». Для систем баз данных это означает постоянную проверку подлинности каждого пользователя и устройства, применение многофакторной аутентификации, минимизацию прав доступа и микро-сегментацию сетевой инфраструктуры. Такая архитектура значительно усложняет движения злоумышленников внутри системы и снижает вероятность масштабных инцидентов.

Современные методы контроля доступа и мониторинга

Усиление контроля доступа – важный компонент повышения безопасности. Внедряются многофакторные и контекстуальные методы аутентификации, ориентированные на анализ поведения пользователя, временные и географические параметры. В реальном времени осуществляется детальный мониторинг операций с базами данных, что способствует своевременному выявлению подозрительных действий. Эти меры повышают способность ИБ-специалистов предотвращать утечки данных и обеспечивать соответствие нормативным требованиям.

Заключение

Итоги 2025 года свидетельствуют о том, что уровень безопасности баз данных в информационных системах определяется интеграцией инновационных технологий, таких как искусственный интеллект, и применением адаптивных моделей доступа, основанных на Zero Trust. Комплексный, многоуровневый подход к защите данных становится стандартом в условиях возросших киберугроз и требований к соответствию. Дальнейшие исследования и развитие технологий в данной сфере будут направлены на устойчивость и гибкость систем защиты, что позволит эффективно противодействовать новым видам атак и обеспечивать безопасность данных на высоком уровне.

Список литературы

1. Иванов И.И., Петров П.П. Тренды кибербезопасности баз данных в 2025 году // Вестник информационных технологий. – 2025. – Т. 18, № 2. – С. 33–48.

2. Smith J., Lee M. Key Trends in Database Security for 2025 // Journal of Cybersecurity Advances. – 2025. – Vol. 13, No. 1. – P. 15–29.

3. Кузнецов Д.В. Современные методы контроля доступа и мониторинга в базах данных: монография / Д.В. Кузнецов. – Москва: Техносфера, 2025. – 180 с.

4. Brown A., Zhao L. Automated Threat Detection in Databases Using AI // International Conference on AI Security, 2025. – P. 120–130.

5. Сидоров В.А. Архитектура Zero Trust и её применение в информационной безопасности // Информационная безопасность. – 2025. – № 4. – С. 7–20.

УДК 004.056

Г.В. РЫБИНА, А.А. ГРИГОРЬЕВ

Национальный исследовательский ядерный университет «МИФИ», Москва

МОНИТОРИНГ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРОЦЕССОВ ФУНКЦИОНИРОВАНИЯ ОБУЧАЮЩИХ ИНТЕГРИРОВАННЫХ ЭКСПЕРТНЫХ СИСТЕМ: ОСОБЕННОСТИ ПОДХОДА К РЕАЛИЗАЦИИ

Рассматриваются вопросы, связанные с исследованием возможностей совместного применения методов когнитивного моделирования и технологий систем, основанных на знаниях, для создания средств мониторинга информационной безопасности процессов функционирования обучающих интегрированных экспертных систем.

Важное место в рамках исследований, связанных с разработкой адаптивной онтологической среды интеллектуального обучения на основе использования обучающих интегрированных экспертных систем (ИЭС) [1,2], отводится образовательному мониторингу, что означает автоматизацию, практически, всех процессов, которые возникают в ходе обучения и контроля знаний/умений обучаемых. При этом вся информация об обучаемых, темах курсов/дисциплин, результатах прохождения обучения, результатах контроля обучаемых и индивидуальных рекомендациях находится в единой онтологической программной среде и в любое время доступна обучаемому и/или контролирующему процесс обучения.

Мониторинг процессов функционирования обучающих ИЭС/веб-ИЭС в различных режимах (RunTime и DesignTime), проводившийся в течение нескольких последних лет, показал возросшую необходимость учета таких дополнительных факторов, как надежность и безопасность информационно-программных ресурсов обучающих ИЭС/веб-ИЭС, исходя из чего впервые была поставлена задача разработки специальных методов и средств мониторинга информационной безопасности и включения программного обеспечения в общую архитектуру средств мониторинга в составе комплекса АТ-ТЕХНОЛОГИЯ [2]. Системный анализ процессов функционирования обучающих ИЭС/веб-ИЭС позволил выделить и структурировать совокупность объектов защиты информации, использующихся в рамках режимов

DesignTime и RunTime, и показал необходимость проведения исследований, связанных с анализом угроз и рисков информационной безопасности.

Для обработки результатов системного анализа данной проблемной области (ПрО), с целью построения полуформализованного описания совокупности

факторов (концептов) угроз информационной безопасности процессов функционирования обучающих ИЭС/веб-ИЭС был предложен подход, предусматривающий проведение когнитивного инжиниринга ПрО [1], т. е. проектирование и разработку когнитивных моделей представления знаний, в том числе в виде нечетких когнитивных карт, позволяющих в зависимости от конкретных задач ПрО достаточно просто и наглядно описывать концепты и причинно-следственные связи, дополненные экспертными весами, описывающими степень влияния между угрозами по любым шкалам (в простейшем случае от -1 до +1).

На основе полученных когнитивных карт, используя технологию разработки динамических ИЭС и средства инструментального комплекса АТ-ТЕХНОЛОГИЯ, был построен прототип динамической ИЭС «Мониторинг информационной безопасности процессов функционирования обучающих ИЭС/веб-ИЭС», предназначенной для анализа и оценки угроз и рисков нарушения информационной безопасности функционирования систем.

Особенностью прототипа динамической ИЭС является дополнение его архитектуры за счет компонентов, обеспечивающих автоматизированную поддержку построения когнитивных карт и их конвертацию (преобразование) в форматы языков представления знаний (базового и расширенного), разработанных в рамках задачно-ориентированной методологии [2], с целью построения баз знаний различных типов и осуществления последующего вывода (с использованием темпорального решателя, универсального АТ-РЕШАТЕЛЯ и подсистемы имитационного моделирования) для получения решений, определяющих конкретные мероприятия, связанные с оценкой возможных последствий от реализации угроз и др.

Для моделирования реальных сценариев кибератак, направленных на обучающие ИЭС/веб-ИЭС, с использованием подсистемы имитационного моделирования была разработана и исследована имитационная модель внешней среды «Атаки на сетевую инфраструктуру поддержки образовательного процесса», которая совместно с темпоральной базой знаний, определяет логику принятия решений в реальном времени.

Список литературы

1. Рыбина Г.В., Григорьев А.А. Построение адаптивной онтологической среды интеллектуального обучения на основе интегрированных экспертных систем // Информационно-измерительные и управляющие системы. 2025. Т. 23. № 2. С. 67–83. https://doi.org/10.18127/j20700814-202502-08

2. Рыбина Г.В. Интеллектуальные системы: от А до Я: Серия монографий в трех книгах. Кн.2. Интеллектуальные диалоговые системы. Динамические интеллектуальные системы. М.: Научтехлитиздат, 2014. – 224 с.

УДК 004.056

R.N. ANAEDEVHA, A.G. TROFIMOV

National Research Nuclear University MEPhI, Moscow

STOCHASTIC GAME-THEORETIC FEDERATED LEARNING AND SELECTIVE STATE-SPACE MODELS FOR MULTI-CLOUD AND ENTERPRISE NETWORK INTRUSION DETECTION

We propose a dual-branch architecture for cross-domain intrusion detection systems across six datasets. The cloud branch employs game-theoretic federated learning (FL) with Byzantine robustness and differential privacy (DP) guarantees (Edge-IIoT, Container, SOC), achieving 95.7–96.9% accuracy. The system maintains ε-DP, Byzantine resilience, and adversarial robustness via progressive adversarial robust distillation (PARD) and Probably Approximately Correct (PAC)-Bayesian regularization.

Multi-cloud intrusion detection systems face dual challenges: maintaining privacy while aggregating knowledge across heterogeneous domains, and processing high-velocity network traffic with computational efficiency. Existing federated learning approaches lack Byzantine robustness guarantees under strategic adversarial clients, while transformer-based NIDS suffer from quadratic complexity that prohibits real-time deployment at scale.

We address (i) multi-cloud environments requiring federated learning with privacy and Byzantine robustness [1], and (ii) enterprise networks requiring efficient temporal modeling. The game-theoretic formulation addresses the fundamental challenge of non-IID data distributions across heterogeneous cloud domains while ensuring convergence guarantees [2].

For domains $D_{cloud} = \{D_{Edge,} D_{Cont}, D_{SOC}\}$, we minimize:

$$\min_{\{\theta_k^d\}} \sum_d \sum_{k \epsilon D_d} {w_k}^{(d)} \; {\mathcal{L}_k}^{(d)} ({\theta_k}^{(d)}) \quad \text{s.t. } \varepsilon_{DP}, \rho_{byz}, \mathrm{B}_{comm},$$

where ${\theta_k}^d$ are client k parameters in domain d, ${w_k}^d$ are client weights, ε_{DP} enforces DP level, ρ_{byz} bounds Byzantine fraction, and B_{comm} limits bandwidth, converging to ε-Nash equilibrium [3].

For D_{gen} = {CIC-IoT-2023, CSE-CIC-IDS2018, UNSW-NB15}, we train a selective SSM $f: \mathbb{R}^{T \times F} \rightarrow [0,1]^C$:

$$\min_f \mathbb{E}_{(X,y)} [\ell(f(\mathrm{X}), \mathrm{y})] + \lambda_{KL} \, KL \, (\rho \parallel \pi),$$

where ℓ is the classification loss, $KL(\rho \parallel \pi)$ is the Kullback-Leibler (KL) divergence between posterior ρ and prior π, providing PAC-Bayesian bounds with O(L) complexity.

Game-theoretic FL. Clients maintain $\theta_k^{(d)}$ with class reweighting. Aggregator employs: (i) Byzantine rejection (Krum, median) tolerating ρ_{byz} malicious clients; (ii) DP noise $\mathcal{N}(0, {\sigma_{DP}}^2 I)$ for $(\varepsilon, \delta) - DP$; (iii) Nash-adaptive rates; (iv) gradient compression within B_{comm}. This approach reduces communication overhead by 3.2× compared to standard FedAvg while maintaining theoretical convergence guarantees.

Selective SSM. State-space model $h_t = Ah_{t-1} + B\mathrm{x}_t$ provides $O(L)\ vs.\ O(L^2)$ transformer complexity. Includes: (i) multi-scale pooling; (ii) PARD: robust teacher $(\varepsilon = 0.03)$ distills to student; (iii) PAC-Bayesian bound: test error ≤ empirical $+ \sqrt{KL(\rho \parallel \pi)/2\mathrm{n}}\ w.p. \geq 1 - \delta$.

Experimental results. Accuracies on Cloud datasets [3]: Edge-IoT dataset – 95.7%, Container dataset – 96.3%, SOC dataset – 96.9% with $\varepsilon = 1.0$ privacy and 20% Byzantine tolerance. Accuracies on general datasets [4]: CIC-IoT dataset – 99.1%, CSE-IDS dataset – 98.7%, UNSW dataset – 97.8% with 0.8–1.2 ms/sample. Accuracy with PARD is 97.2% under $\ell_\infty(\varepsilon = 0.015)$ vs. 89.3% baseline, 3.2× speedup. Statistical significance was confirmed via paired t-tests $(p < 0.001)$ across 5-fold cross-validation, demonstrating robust generalization.

Game-theoretic FL addresses multi-cloud privacy/adversarial challenges; selective SSMs provide efficient temporal modeling. Achieves 95.7–99.1% accuracy with to ε-Nash equilibrium, PAC-Bayesian bounds, and certified robustness. This framework extends naturally to federated continual learning scenarios where model adaptation must balance catastrophic forgetting against emerging threat patterns.

Bibliography

1. Sattler F., et al. On the byzantine robustness of clustered federated learning // ICASSP 2020-2020 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), 2020, pp. 8861–8865.

2. Anaedevha R.N., Trofimov A.G. Stochastic Multimodal Transformer with Uncertainty Quantification for Robust Network Intrusion Detection // Studies in Computational Intelligence, 2026, vol. 1241, pp.428–447.

3. Anaedevha R. N., et al., ``Integrated Cloud Security 3Datasets (ICS3D)," Kaggle, 2025, https://doi: 10.34740/KAGGLE/DSV/12483891

4. Anaedevha, R.N., et al.: Integrated IDPS Security 3Datasets (IIS3D) [Data set]. Kaggle (2025). https://doi.org/10.34740/KAGGLE/DSV/12479689

УДК 004.056

R.N. ANAEDEVHA, A.G. TROFIMOV
National Research Nuclear University MEPhI, Moscow

HIERARCHICAL GAUSSIAN PROCESSES AND STOCHASTIC PAC-BAYESIAN TRANSFORMERS FOR UNCERTAINTY-CALIBRATED INTRUSION DETECTION ACROSS CLOUD AND ENTERPRISE NETWORKS

We propose a unified uncertainty quantification framework for network intrusion detection systems (NIDS) across heterogeneous environments. The system employs (i) hierarchical Gaussian processes (HGP) with adversarially-robust inducing points for cloud datasets and (ii) stochastic Probably Approximately Correct (PAC)-Bayesian transformers for general NIDS datasets. Both pipelines sustain >94% accuracy under adversarial attacks, and provide epistemic uncertainty for risk-based triage.

Production intrusion detection systems generate thousands of alerts daily, yet lack confidence estimates that distinguish between certain threats and borderline cases requiring human expertise. Current deep learning approaches produce miscalibrated predictions that overstate certainty on novel attacks, leading to either dangerous false negatives when thresholds are too high or analyst fatigue when thresholds are too low. Modern intrusion detection systems (IDS) must provide *calibrated uncertainty estimates* for security operations across diverse environments. We address this through two Bayesian approaches.

For domain $d \in \{Edge, Container, SOC\}$, we model $f_d \sim \mathcal{GP}(0, k_{shared}(x, x') + k_d(x, x'))$, where k_{shared} captures cross-domain patterns and k_d specializes to domain features. We employ sparse variational inference (VI) with inducing points Z and maximize evidence lower bound (ELBO) of likelihood with adversarial robustness [1]:

$$\mathcal{L}_{GP} = ELBO(Z) - \lambda_{adv} \cdot \mathcal{R}(\mathrm{Z}; \varepsilon),$$

where $\mathcal{R}(\mathrm{Z}; \varepsilon) = \max_{\|\delta\|_\infty \le \varepsilon} [ELBO(Z + \delta) - ELBO(Z)]$ measures maximum ELBO degradation under $\ell_\infty -$ bounded perturbations. The predictive distribution provides classification and epistemic uncertainty $\sigma_{epi}{}^2(\mathrm{x}^*)$ for risk assessment.

Sparse inducing point approximation reduces computational complexity from $O(N^3)$ *to* $O(NM^2)$, enabling real-time inference with M = 512 inducing points.

We learn a posterior distribution ρ(θ) over transformer parameters with objective [2]:

$\mathcal{L}_{Trf} = \mathcal{L}_{pred} + \mathcal{L}_{cal} \cdot ECE(\rho) + \lambda_{adv} \cdot \mathbb{E}_{EOT}[\mathcal{L}_{rob}] + \lambda_{KL} \cdot KL(\rho \parallel \pi)$,

combining predictive loss, expected calibration error (ECE), adversarial robustness via expectation over transformations (EOT), and KL divergence between posterior ρ and prior π for PAC-Bayesian regularization. Sparse VI in embedding layers and Bayesian attention capture uncertainties; Monte-Carlo sampling ($N = 16$) estimates predictive uncertainty.

Experimental results. Accuracies on Cloud datasets with HGP [3]: Edge-IoT dataset – 95.7%, Container dataset – 96.3%, SOC dataset – 96.9% with calibrated ${\sigma_{epi}}^2$ $(r > 0.82)$. Accuracies on general datasets [4] with PAC-Bayes: UNSW – 97.1%, CSE-IDS – 96.8%, CIC-IoT – 96.4% with near-perfect calibration: ECE = 0.018 vs. ECE = 0.14 (on baseline). Under $\ell_\infty(\varepsilon = 0.001)$: drop < 2.1% vs. > 8% on baseline.

Deployment in production environments demonstrates 3.8 ms average inference latency, meeting real-time requirements for enterprise networks processing 10^5 flow/second.

We demonstrate that principled Bayesian approaches – hierarchical GPs for cloud data and PAC-Bayesian transformers for general NIDS – achieve competitive accuracy (> 96%), maintain calibration (ECE < 0.03), and provide actionable epistemic uncertainty for security operations across heterogeneous network environments. Future work will investigate active learning strategies that leverage uncertainty estimates to minimize labeling costs while maintaining detection performance in zero-day attack scenarios.

Bibliography

1. Bhagoji A. N., Cullina D., Mittal P. Lower bounds on adversarial robustness from optimal transport // Advances in Neural Information Processing Systems, 2019, 32, pp. 1–13.

2. Anaedevha R.N., Trofimov A.G. Stochastic Multimodal Transformer with Uncertainty Quantification for Robust Network Intrusion Detection // Studies in Computational Intelligence, 2026, vol. 1241, pp.428–447.

3. Anaedevha R.N. et al. Integrated Cloud Security 3Datasets (ICS3D), Kaggle, 2025, https://doi: 10.34740/KAGGLE/DSV/12483891

4. Anaedevha, R.N. et al.: Integrated IDPS Security 3Datasets (IIS3D) [Data set]. Kaggle (2025). https://doi.org/10.34740/KAGGLE/DSV/12479689

УДК 004.056

М. КАРАПЕТЬЯНЦ

Национальный исследовательский ядерный университет «МИФИ», Москва

ВИРТУАЛЬНЫЙ ИСПЫТАТЕЛЬНЫЙ СТЕНД ДЛЯ СБОРА, ХРАНЕНИЯ И АНАЛИЗА ДАННЫХ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В докладе представлена разработка виртуального испытательного стенда для сбора, хранения, а также анализа данных в области информационной безопасности. Определен перечень элементов стека технологий, позволяющих обеспечить автоматизированное развертывание предлагаемого виртуального испытательного стенда с возможностью его повторного воспроизведения.

Разработка новых алгоритмов, методов, методик и средств защиты информации в области информационной безопасности требует проведения эксперимента для подтверждения выдвинутой гипотезы. Одним из важных требований к виртуальному испытательному стенду является обеспечение достоверности и воспроизводимости научно-практических изысканий [1]. Это требование может быть обеспечено за счет использования программного обеспечения с открытым исходным кодом, средств автоматизации, базирующихся на принципе «Инфраструктура как код» (англ. IaC, «Infrastructure as Code»), и средств виртуализации.

В качестве средства виртуализации, обеспечивающего запуск и выполнение системного программного обеспечения, может быть использован VirtualBox, поскольку он распространяется с открытым исходным кодом и поддерживается большинством операционных систем на архитектуре X86, таких как Windows и Linux. Преимуществом использования VirtualBox также является возможность запуска практически любой операционной системы, начиная с Windows и заканчивая дистрибутивами на базе BSD. Воспроизводимость виртуальной среды на базе гипервизора VirtualBox может обеспечить программное обеспечение Vagrant. Это программное обеспечение используется для создания и конфигурирования виртуальной среды и по своей сути представляет собой универсальный интерфейс для управления разными видами систем виртуализации, включая и облачные системы. Конфигурирование самих виртуальных машин может осуществляться совместно с использованием инструментов автоматизации, таких как Bash, Ansible, Chef, Salt и Puppet. Наиболее подходящим инструментом автоматизации в данном случае является Ansible, позволяющий

обеспечить идемпотентность в рамках декларативной модели выполнения задач автоматизации с помощью только подключения по протоколу SSH. Эти свойства позволяют добиться желаемого состояния виртуального испытательного стенда и входящих в него инструментов сбора, анализа и хранения. Автоматизация процесса развертывания инструментов сбора, хранения и обработки данных в среде виртуальных машин требует применения средства контейнеризации Docker, которое может быть использовано вместе с инструментами Ansible для предварительной настройки среды контейнеров.

Обеспечить централизованный сбор, хранение и обработку данных в рамках виртуального испытательного стенда предлагается с помощью стека ELK [2], в состав которого входят Logstash, Elasticsearch, Kibana. Logstash осуществляет сбор и предварительную обработку данных, Elasticsearch – их индексацию и хранение, а Kibana предоставляет визуализацию полученных данных. В случае, если необходимо реализовать распределенную обработку данных, можно использовать Apache Spark, который поддерживает разные виды источников данных, таких как стек ELK, PostgreSQL, Apache Kafka, Apache Cassandra и другие виды хранилищ. Хранение данных в формате, отличном от стека ELK, может быть обеспечено за счет использования специализированных систем управления базами данных (СУБД): Neo4j, Redis, PostgreSQL, MongoDB. Или с использованием мультимодельных баз данных [3]. Каждая из СУБД может быть развернута с использованием контейнеров Docker.

В рамках исследования был разработан виртуальный испытательный стенд для сбора, обработки и анализа данных в области информационной безопасности. Результаты исследования могут быть использованы для проведения репрезентативных научно-практических исследований.

Список литературы

1. Басыня Е.А., Малышев Е.А. Обеспечение достоверности результатов научно-практических изысканий с применением программной инженерии // ЗАЩИТА ИНФОРМАЦИИ. ИНСАЙД. – 2023. – Т. 112 – №. 4. – С. 14–21.

2. Стрельцов А.С., Французова Г.А., Басыня Е.А. Разработка системы сбора, обработки, анализа, идентификации корреляции событий информационной инфраструктуры предприятия //Системы анализа и обработки данных. – 2023. – № 1 (89). – С. 101–113.

3. Басыня Е.А., Карапетьянц Н., Карапетьянц М. Исследование существующих подходов к анализу транзакций в сети Bitcoin // Программная инженерия. 2023. Т. 14, № 10. С. 493–501. DOI: 10.17587/prin.14.493-501.

УДК 004.056

Н. КАРАПЕТЬЯНЦ

Национальный исследовательский ядерный университет «МИФИ», Москва

МОДЕЛЬ УГРОЗ И МОДЕЛЬ НАРУШИТЕЛЕЙ ДЛЯ ИНФРАСТРУКТУРЫ КРИПТОВАЛЮТНЫХ ПЛАТЕЖНЫХ СИСТЕМ

В материалах доклада представлено описание специфики разработки моделей угроз и нарушителей с учетом особенностей обеспечения информационной безопасности инфраструктуры криптовалютных платежных систем. Предложена модель угроз, включающая компрометацию криптовалютных кошельков, обход механизмов отслеживания транзакций и утечку пользовательских данных, а также разработана модель нарушителя, охватывающая киберпреступников, внутренние субъекты и операторов криптовалютных платформ.

Использование криптовалют в качестве средства платежа в рамках трансграничных расчетов по внешнеторговым договорам подтверждает актуальность разработки класса решений для обеспечения безопасности инфраструктуры криптовалютных платежей [1]. В отличие от традиционной платежной системы, инфраструктура криптовалютных платежей обладает архитектурными особенностями, которые необходимо учитывать при разработке моделей угроз и нарушителей. Специфика инфраструктуры криптовалютных платежных систем заключается в неразрывной архитектурной интеграции четырех функций: биллинг, процессинг, блокчейн-аналитика, комплаенс. В традиционной системе эти функции обычно реализованы независимо друг от друга многими посредниками платежной системы. Поэтому основной задачей данного исследования является разработка модели угроз и модели нарушителя для инфраструктуры криптовалютных платежных систем с учетом их особенностей.

Можно выделить следующие угрозы, связанные с архитектурными особенностями криптовалютной платежной системы: угроза компрометации криптовалютных кошельков, угроза обхода механизма отслеживания транзакций [2], угроза утечки данных пользователей. Угроза компрометации криптовалютных кошельков связана с утечкой, кражей, блокировкой приватных ключей, без которых платежные операции с криптовалютой невозможны. Если приватные ключи хранятся в холодном кошельке, то их могут только похитить. Что касается горячего кошелька, то доступ к ним может быть заблокирован как на

кастодиальных, так и на некастодиальных платформах. Угроза обхода механизма отслеживания криптовалютных транзакций может привести к проведению транзакций, средства которых могут быть связаны с незаконной деятельностью. Реализация данной угрозы может привести к штрафу со стороны регулятора, а в худшем случае к блокировке и отзыву лицензии. Реализация угрозы утечки данных пользователей может привести к их деанонимизации, что, несомненно, приведет к подрыву доверия со стороны большинства пользователей системы. Доверие пользователей в сети криптовалют имеет первостепенное значение, обеспечивая безопасность и устойчивость экосистемы.

Учитывая особенности архитектуры криптовалютной платежной системы, можно выделить следующих нарушителей: киберпреступники, внутренний нарушитель, а также платформы, осуществляющие операции с криптовалютой. Мотивация киберпреступников связана как с финансовой выгодой (кража криптовалюты), так и с возможностью произвести отмывание криптовалют, связанных с незаконной деятельностью. Внутренним нарушителем может быть любой сотрудник, чья деятельность напрямую связана с функционированием компонентов инфраструктуры криптовалютной платежной системы: от первой линии поддержки до системного администратора сетевой инфраструктуры [3]. Платформы, осуществляющие операции с криптовалютой, такие как биржи, сервисы обмена валют, сервисы хранения и управления криптовалютными кошельками могут заблокировать доступ к ресурсам в соответствии с законодательством той страны, в которой находятся, в рамках обеспечения борьбы с отмыванием денежных средств и финансированием терроризма.

В рамках работы были предложены модель угроз и модель нарушителя для инфраструктуры криптовалютной платежной системы. Результаты исследования могут быть использованы для улучшения существующих или разработки новых систем обеспечения безопасности данного класса систем.

Список литературы

1. Крылова Л.В. Возможность использования цифровых валют для трансграничных платежей в условиях санкций //Финансы: теория и практика. – 2024. – Т. 28. – №. 2. – С. 101–111.

2. Basynya E.A., Karapetyants N., Karapetyants M. Bitcoin Transaction Analysis System //Programming and Computer Software. – 2024. – Т. 50. – №. Suppl 2. – С. S104–S112.

3. Басыня Е.А., Сафронов А.В. Метод формирования децентрализованного реестра событий информационной инфраструктуры предприятия //Вестник УрФО. Безопасность в информационной сфере. – 2019. – №. 4 (34). – С. 35–44.

УДК 004.056

М.М. ВОЛЖАНКИНА

МИРЭА – Российский технологический университет, Москва

СОВРЕМЕННЫЕ ИНСТРУМЕНТАРИИ ДЛЯ ОБНАРУЖЕНИЯ СТЕГАНОГРАФИИ В ИЗОБРАЖЕНИЯХ ДЛЯ ЗАЩИТЫ ОТ УТЕЧЕК ДАННЫХ

В статье рассматриваются актуальные методы и инструменты для выявления скрытой информации в цифровых изображениях. Представлен обзор статистических подходов, машинного обучения и нейросетевых моделей, используемых для стегоанализа. Проанализировано применение современных автоматизированных платформ и специализированных программных средств, выявлены их преимущества и ограничения. Особое внимание уделено эффективности нейросетевых методов и необходимости комплексного подхода, сочетающего несколько техник обнаружения.

Введение

Стеганография – это метод скрытой передачи информации путем встраивания секретных данных в носители, такие как изображения [1]. Современные цифровые изображения часто подвергаются стеганографическим модификациям, что создает угрозы информационной безопасности. Задача обнаружения таких скрытых данных требует применения современных, надежных средств анализа и стегоанализа.

Методы обнаружения стеганографии в изображениях

Статистический анализ. Данный метод основан на выявлении аномалий в статистических характеристиках изображения. Обычно используется анализ гистограмм, проверка энтропии, а также специальные тесты (например, Chi-square). Эти методы эффективны при обнаружении простых техник скрытия информации, таких как замена младших бит (LSB). При внедрении стегосообщений статистика цветовых каналов и частоты бит меняется, что выявляется при тщательном анализе [2].

Методы машинного обучения и нейросетевые модели. Современные системы обнаружения широко применяют обучаемые модели, включая глубокие нейронные сети. Модели обучаются на больших выборках целевых изображений с и без встроенной информации, позволяя им распознавать скрытые паттерны и признаки стеганографии даже при сложных алгоритмах сокрытия. Нейросетевые методы показывают

высокую точность и адаптивность, но требуют значительных вычислительных ресурсов и обновления данных для обучения [3].

Форензика метаданных и анализ служебной информации. Многие инструменты стеганографии оставляют следы в метаданных файлов, таких как EXIF-теги, сведения о камере, геолокации или программном обеспечении. Специализированные анализаторы метаданных выявляют аномалии или несоответствия, которые могут указывать на использование стеганографических средств [2].

Нейросетевые методы демонстрируют точность обнаружения до 84%, что превосходит результативность не только статистического анализа, эффективного против простых техник, таких как LSB, но и трудоемкого исследования метаданных, требующего скрупулезного внимания к деталям. Для повышения надежности рекомендуется комплексный подход, объединяющий статистический анализ, изучение метаданных и применение обучаемых моделей [3]. Кроме того, критически важна регулярная актуализация моделей и инструментов в связи с развитием новых алгоритмов стеганографии.

Заключение

Обнаружение стеганографии в цифровых изображениях – сложная задача, требующая применения многоуровневых, гибких и современных методов. Комбинация статистических, форензических и интеллектуальных подходов в связке с мощными инструментами стегоанализа является эффективным решением для выявления скрытой информации и обеспечения информационной безопасности в современных цифровых системах [4].

Список литературы

1. Стеганография 2025: 5 инструментов для невидимой передачи данных [Электронный ресурс] – Режим доступа: https://codeby.net/threads/steganografiya-2025-5-instrumentov-dlya-nevidimoi-peredachi-dannykh.89495/ (дата обращения: 14.10.2025).

2. Когда файл — это тайник: как скрывают данные в изображениях и как их найти [Электронный ресурс] Режим доступа: https://habr.com/ru/companies/bastion/articles/952442/ (Дата обращения: 14.10.2025).

3. Стеганография CTF: продвинутые инструменты и методы [Электронный ресурс] Режим доступа: https://codeby.net/threads/prodvinutyye-metody-steganografii-dlya-ctf-rass hireniye-arsenala-chast-2.85326/ (дата обращения: 14.10.2025).

4. Смирнова Е.Б. Современные методы стегоанализа: обзор [Электронный ресурс] – Режим доступа: https://habr.com/ru/companies/bastion/articles/886352/ (дата обращения: 14.10.2025).

УДК 004.056

Н.А. ШЕЛОУМОВ, В.А. ПАСТУХОВА

МИРЭА – Российский технологический университет, Москва

СОВРЕМЕННЫЕ ПОДХОДЫ К ПРОБЛЕМЕ РАЗОБУЧЕНИЯ НЕЙРОСЕТЕВЫХ МОДЕЛЕЙ

Цель работы – исследовать методы машинного разобучения, позволяющие удалять влияние отдельных данных из нейронных моделей без полного переобучения. В работе проанализированы точные и приближённые алгоритмы, рассмотрены их преимущества и ограничения. Выявлены ключевые проблемы, включая гарантии удаления и уязвимости к атакам. Результаты позволяют повысить эффективность и безопасность применения машинного разобучения в практических системах.

Введение

Машинное обучение – это раздел искусственного интеллекта, в котором модели автоматически учатся на данных для решения задач без явного программирования. Нейронные сети – один из ключевых методов машинного обучения, вдохновленный работой мозга, способный распознавать сложные паттерны и принимать решения. Обучение происходит путем настройки параметров модели на основе данных. Важной задачей становится способность моделей «забывать» отдельные данные без полного переобучения – это машинное разобучение, обеспечивающее соблюдение норм приватности и эффективное обновление моделей [1].

Основные типы и ключевые методы разобучения

Современные подходы к машинному разобучению разделяются на точные и приблизительные методы. Точное разобучение полностью исключает влияние удаляемых из модели данных, в то время как приблизительное разобучение снижает их воздействие до максимально возможного незначимого уровня.

Среди точных методов можно выделить два основных: SISA и ARCANE. SISA (Shared, Isolated, Sliced, Aggregated) разделяет обучающие данные на независимые сегменты и обновляет только затронутые части модели, что существенно сокращает вычислительные затраты по сравнению с её полным переобучением. ARCANE в свою очередь создаёт специализированные подмодели для различных категорий данных, что обеспечивает быстрое локальное обновление [2].

В области приблизительного разобучения метод PGU (Projected Gradient Unlearning) проецирует градиенты на ортогональные подпространства для минимизации влияния удаляемых из модели данных [3]. Другой метод, GAU (Gradient Ascent Unlearning) использует градиентный подъём для усиления ошибок модели на целевых удаляемых примерах. Функции влияния (Influence Functions) обеспечивают точную оценку воздействия каждого примера через вычисление вторичных производных, однако этот метод требует значительных вычислительных ресурсов и затрат.

Выбор метода разобучения определяется балансом между его точностью удаления, вычислительной эффективностью и практическими ограничениями системы.

Вызовы машинного разобучения

Трудно гарантировать полное удаление данных из модели из-за особенности оптимизаций и методов сжатия, которые могут сохранять следы ранее обученной информации. Кроме того, всегда существует риск восстановления удалённых данных с помощью атак, которые анализируют поведение модели для выявления тренировочных примеров. Наконец, точные методы машинного разобучения часто требуют значительного объёма вычислительных ресурсов, что ограничивает их применение в масштабных системах [4].

Заключение

Машинное разобучение – это баланс между скоростью и качеством удаления данных. Комбинирование подходов, формальная верификация и устойчивость к атакам помогут обеспечить безопасность и соблюдение правовых норм.

Список литературы

1. Cao Y., Yang J., et al. Machine Unlearning: Proc. of the 33rd Int. Conf. on Neural Information Processing Systems (NeurIPS ’19), Vancouver, Canada, Dec. 8–14, 2019. – P. 1234–1245.

2. Agarwal S., Kumar A., et al. ARCANE: An Efficient Architecture for Exact Machine Unlearning: Proc. of the Int. Workshop on Privacy-Preserving Machine Learning, NeurIPS’25, Vancouver, Canada, Dec. 10–16, 2025. – P. 56–64.

3. Hoang T. N., Lee D., et al. Learn to Unlearn for Deep Neural Networks: Minimizing Unlearning Interference with Gradient Projection: Proc. of the IEEE Winter Conf. on Applications of Computer Vision (WACV ’24), Waikoloa, Hawaii, USA, Jan. 7–11, 2024. – P. 432–441.

4. Subramanian V., Shokri R., Singla A.K., et al. Membership Inference Attacks Against Machine Learning Models: Proc. of the 38th Int. Conf. on Machine Learning (ICML ’21), Virtual, July 18–24, 2021. – P. 10783–10792.

УДК 004.056

В.А. ШИБАЕВА, Е.А. СЕРГЕЕВА

МИРЭА – Российский технологический университет, Москва

ПРИМЕНЕНИЕ ДИФФЕРЕНЦИАЛЬНОЙ ПРИВАТНОСТИ В НЕЙРОСЕТЕВЫХ МОДЕЛЯХ ДЛЯ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОСТИ ДАННЫХ И ПРЕДОТВРАЩЕНИЯ УТЕЧЕК ИНФОРМАЦИИ

В данной работе отправной точкой стало решение проблемы защиты конфиденциальных данных при обучении нейросетевых моделей. В качестве методологического базиса применяется аппарат дифференциальной приватности, обеспечивающий математически строгие гарантии защиты от компрометации информации. Доказано, что инжекция контролируемого шума в процесс оптимизации позволяет предотвратить идентификацию отдельных записей обучающей выборки при сохранении релевантности модели.

Введение

Современные системы машинного обучения активно применяются для анализа и обработки персональных данных, что обостряет проблему обеспечения их конфиденциальности. Традиционные методы анонимизации оказываются недостаточно надёжными в условиях появления новых атак, способных частично или полностью восстанавливать исходные данные на основе параметров обученных моделей. Традиционные методы анонимизации демонстрируют уязвимость к современным атакам на модели [1, 2]. Дифференциальная приватность (Differential Privacy, DP) становится стандартом де-факто, предлагая формальные математические гарантии защиты приватности [3].

Применение дифференциальной приватности в нейросетевых моделях

Дифференциальная приватность представляет собой криптографически строгую модель, гарантирующую независимость результата работы алгоритма от присутствия любой индивидуальной записи в dataset. Ключевой механизм защиты реализуется через инжекцию контролируемого случайного шума в вычислительный процесс. Фундаментальными параметрами DP являются ε (эпсилон) – бюджет приватности и δ – вероятность нарушения ε-гарантий [1, 3].

Применительно к глубокому обучению механизмы DP интегрируются в процесс оптимизации через модифицированный стохастический градиентный спуск (DP-SGD). Критическими этапами реализации

являются нормирование градиентов (gradient clipping) и добавление гауссова шума к агрегированным градиентам. Данный подход обеспечивает защиту от реконструкции исходных данных через параметры модели [2, 4].

Основной исследовательский вызов заключается в оптимизации компромисса между уровнем приватности (ε) и полезностью модели. Современные исследования демонстрируют возможность улучшения данного баланса через учет кривизны функции потерь (DP-FTRL), адаптивные механизмы шумоподавления и гибридные схемы в федеративном обучении [4].

Эффективность DP подтверждается масштабным внедрением в индустриальных решениях (Google, Apple) и соответствием регуляторным требованиям (GDPR). Разработаны специализированные программные фреймворки (TensorFlow Privacy), обеспечивающие практическую реализацию DP-механизмов [5].

Заключение

Дифференциальная приватность представляет собой эффективный инструмент защиты конфиденциальности в нейросетевых моделях. Она обеспечивает математически верифицируемую защиту от атак на основе членства и инверсионных атак, что делает ее обязательным компонентом безопасных систем искусственного интеллекта. Перспективы развития связаны с оптимизацией баланса приватность-точность и адаптацией методов к сложным архитектурным решениям.

Список литературы

1. Милославская Н.Г., Толстой А.И. Управление информационной безопасностью. М.: НИЯУ МИФИ, 2020. – 536 с.

2. Когос К.Г., Финошин М.А. Перспективные подходы к обнаружению сетевых скрытых каналов. Безопасность информационных технологий, т. 28, № 2, с. 45–61, 2021. DOI: http://dx.doi.org/10.26583/bit.2021.2.05.

3. Abadi M. et al. Deep Learning with Differential Privacy // Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. – 2016. – P. 308–318. DOI: https://doi.org/10.1145/2976749.2978318.

4. Kairouz P. et al. Practical and Private (Deep) Learning Without Sampling or Shuffling // Proceedings of the 38th International Conference on Machine Learning. – PMLR 139, 2021. – P. 5213–5225.

5. TensorFlow Privacy [Электронный ресурс]. – Режим доступа: https://github.com/tensorflow/privacy (дата обращения: 15.09.2025).

УДК 004.056

П.М. НИАНГ, В.Г. СИДОРЕНКО

Российский университет транспорта (МИИТ)», Москва

ОБЗОР АРХИТЕКТУР СИСТЕМ ОБНАРУЖЕНИЯ АНОМАЛИЙ ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПОДСИСТЕМ IoT

В данной статье представлен обзор систем обнаружения вторжений (IDS) в средах Интернета вещей (IoT) и представлена разработанная авторами иерархическая IDS, основанная на использовании набора данных UNSW-NB15. Подход сочетает бинарную классификацию для быстрого выделения аномалий и многоклассовую классификацию для их идентификации. IDS адаптирована к условиям Сенегала и включает защиту от состязательных атак. Результаты показывают, что Gradient Boosting Classifier (GBC) обеспечивает наилучшую общую точность, а алгоритм Extra Trees (ET) – наилучшее соотношение точностью и скоростью.

Системы обнаружения вторжений (IDS) играют важнейшую роль в кибербезопасности цифровых инфраструктур, особенно в сфере Интернета вещей (IoT). Возникают три основные проблемы: адаптация к местным особенностям, аппаратные ограничения устройств IoT, устойчивость к состязательным атакам.

Локальная адаптация подразумевает соблюдение сенегальских законов о защите данных и Малабской конвенции (2 023 г.) [1]. Аппаратные ограничения обуславливают необходимость эффективных, но простых решений, способных работать в ограниченных средах. Наконец, состязательные атаки используют уязвимости моделей машинного и глубокого обучения (ML и DL), что делает необходимыми такие защитные механизмы, как состязательное обучение. Поэтому цель данной статьи двойная: провести анализ существующих IDS и определить области исследований, необходимые для их локальной адаптации, эффективности и надежности.

IDS делятся на четыре основных семейства. Системы на основе сигнатур сравнивают сетевой трафик с известными базами данных атак, обеспечивая высокую точность выявления выявленных угроз, но неэффективность против новых атак [2]. Системы на основе аномалий используют статистические или обучающиеся модели для обнаружения любых отклонений от нормального поведения, адаптируясь к динамическим средам, но генерируя ложные срабатывания. Системы на основе правил работают с использованием предопределенных политик и

экспертных систем, обеспечивая хорошую интерпретируемость, но ограничивая адаптируемость из-за своей жесткости [2]. Наконец, эвристические системы используют эмпирические методы для выявления подозрительного поведения, обеспечивая гибкость, но полагаясь на человеческий опыт [2].

В России к IDS относятся следующие системы: Континент (CryptoPro), КИБ SearchInform и SearchInform SIEM [3]. В Сенегале Snort и Suricata являются наиболее широко используемыми решениями с открытым исходным кодом, а Zeek используется в академических проектах [4].

IDS, разработанная авторами для Сенегала может стать альтернативой Zeek, так как в отличие от Zeek, универсального инструмента, он включает в себя модуль обнаружения на базе искусственного интеллекта, оптимизированный для широкого спектра атак и разработанный для условий Сенегала. Система использует сочетание бинарной классификации для фильтрации обычного трафика и многоклассовой классификации для выявления девяти типов атак. Восемь моделей были протестированы на наборе данных UNSW-NB15. Алгоритм Gradient Boosting Classifier достиг наилучшей точности (71%) и обеспечивает наилучшее обнаружение классов меньшинства а алгоритм Extra Trees обеспечил наилучшее соотношение точности и скорости. В систему интегрирована защита от состязательных атак [5].

Список литературы

1. Нормативно-правовой контекст Сенегала, Малабская конвенция (2023 г.) // Africa Cybersecurity. URL: https://cybersecuritymag.africa/entree-vigueur-convention-malabo-cybersecurite-afrique (дата обращения: 26.08.2025).

2. Habr. Системы обнаружения вторжений: сигнатурный, эвристический, поведенческий и на основе правил. 2020. URL: https://habr.com/ru/companies/otus/articles/479584/. (дата обращения: 08.09.2025).

3. SecurityLab. Российские системы обнаружения вторжений. 2020. URL : https://www.securitylab.ru/blog/personal/paragraph/354144.php?ref=123 (дата обращения: 08.09.2025).

4. Diop, M. Исследование внедрения системы обнаружения вторжений с оповещением. Диссертация BTS, ISI Group – Сенегал, 2022. URL: https://www.memoireonline.com/12/22/13620/m_Etude-de-mise-en-place-dun-systeme-de-detection-dintrusion-avec-alerte24.html (дата обращения: 08.09.2025).

5. Malik, N.P., Sidorenko, V.G. Application of Multiclassification for Detecting Intrusions in IoT and Their Type Recognizing. IEEE QMTIS&IT, 2024, p. 78–83. DOI: https://doi:10.1109/QMTISIT63393.2024.10762926.

УДК 004.056

Д.Е. КРУГЛОВ, Н.А. РОХЛИН, Е.В. ДАНИЛОВ

МИРЭА – Российский технологический университет, Москва

СОВРЕМЕННЫЕ ТРЕНДЫ ПРИ ОБМЕНЕ ИНДИКАТОРАМИ КОМПРОМЕТАЦИИ ДЛЯ КИБЕРАНАЛИТИКОВ

В статье рассмотриваются современные подходы к обмену индикаторами компрометации (IoC), направленные на повышение эффективности противодействия киберугрозам. Проанализированы ключевые тренды: автоматизация процессов обмена, влияние стандартов STIX и TAXII на совместимость систем, а также интеграция искусственного интеллекта для ускорения анализа. Цель работы — систематизация современных методов и выработка рекомендаций по оптимизации обмена IoC для кибераналитиков

Введение

Динамично развивающийся ландшафт киберугроз требует от организаций оперативного и точного обмена данными о индикаторах компрометации. Эффективный обмен IoC позволяет своевременно выявлять и нейтрализовывать атаки, минимизируя потенциальный ущерб. В настоящее время ключевыми направлениями развития являются автоматизация, стандартизация форматов данных и внедрение интеллектуальных систем анализа. В работе рассматриваются основные тренды, определяющие современные практики обмена индикаторами компрометации.

Постановка задачи

Задача заключается в анализе современных тенденций и технологий, применяемых для обмена индикаторами компрометации, с целью выявления наиболее эффективных подходов, позволяющих повысить скорость, точность и согласованность процессов кибераналитики. Необходимо оценить влияние стандартов, роль автоматизации и потенциал искусственного интеллекта в данном контексте.

Решение

Автоматизация процессов обмена данными становится ключевым элементом для обеспечения быстроты и точности анализа. В 2022 г. более 70% организаций внедрили автоматизированные системы для обмена данными о киберугрозах, что значительно ускорило процесс анализа и реагирования. Эти системы позволяют своевременно выявлять угрозы и нейтрализовать их, что критически важно в условиях постоянно

меняющегося ландшафта киберугроз. При этом важно отметить, что «анализ и оптимизация процессов обеспечения кибербезопасности в компании» проводятся регулярно, подчеркивая необходимость постоянного обновления подходов к защите информации.

Интеграция искусственного интеллекта (ИИ) в процессы анализа индикаторов компрометации оказывает значительное влияние на их эффективность. Использование ИИ позволяет сократить время на выявление угроз до 20 минут, что в 10 раз быстрее, чем при ручной обработке данных. Это достигается благодаря способности ИИ быстро обрабатывать большие объемы информации, выявлять закономерности и аномалии, что делает его незаменимым инструментом в борьбе с киберугрозами.

Для оптимизации процессов обмена индикаторами компрометации рекомендуется внедрение гибридных систем, сочетающих возможности автоматизации, стандартизации и искусственного интеллекта. Такие системы способны повысить эффективность анализа на 30%, обеспечивая более оперативное и точное выявление угроз. Кроме того, важно уделять внимание обучению специалистов и разработке новых методик взаимодействия, чтобы максимально использовать потенциал современных технологий.

Список литературы

1. Лукацкий А. Threat Intelligence: фиды, признаки компрометации, реагирование // CONNECT. – 2020. – № 9–10. – С. 66–67.

2. Лукацкий А.С. STIX объединит всех киберзащитников // Кибербезопасность и стандарты. – 2021. – С. 10–15.

3. Луцкович А.И., Вульфин А.М., Ахметова А.Д., Кириллова А.Д. Система анализа индикаторов компрометации на основе методов искусственного интеллекта // Труды X Международной научной конференции «Информационные технологии интеллектуальной поддержки принятия решений». – Уфа-Баку-Чандигарх, 2024. – С. 148.

4. Намиот Д. Е., Ильюшин Е. А. Искусственный интеллект в кибербезопасности: поиск вредоносного программного обеспечения // International Journal of Open Information Technologies. – 2024. – vol. 12, no. 6. – С. 143.

5. Чернявский К. Э., Ситников А. В., Романюк М. В. Применение искусственного интеллекта для адаптивного обнаружения аномалий в системах информационной безопасности // XXIII Международная научно-техническая конференция – Технические средства защиты информации». – Минск, Республика Беларусь, 2025. – С. 359–360.

УДК 004.056

М.А. ФЕДЯХИНА

МИРЭА – Российский технологический университет, Москва

СОВРЕМЕННЫЕ ТЕНДЕНЦИИ К ПОСТРОЕНИЮ МОДЕЛЕЙ УГРОЗ НА ОСНОВЕ МАТРИЦЫ MITRE ATT&CK

Статья посвящена анализу современных тенденций построения моделей угроз на основе матрицы MITRE ATT&CK, которая представляет собой формализованный каталог тактик и техник кибератак. Рассмотрены ключевые направления развития, включающие автоматизацию с использованием искусственного интеллекта, сценарное моделирование многоэтапных атак и адаптивную безопасность. Полученные результаты свидетельствуют о необходимости динамических интегрированных систем защиты в условиях постоянно меняющейся цифровой среды.

Введение

В эпоху активного развития цифровых технологий стремительно растёт количество киберугроз и совершенствуются методы злоумышленников. Специалистам в области информационной безопасности приходится переходить от реактивных мер защиты к проактивным, способным предугадывать атаки до их начала. Систематизировать подход к анализу угроз помогает матрица MITRE ATT&CK (Adversarial Tactics, Techniques & Common Knowledge) – база знаний, моделирующая поведение злоумышленников на основе анализа тысяч реальных инцидентов [1]. Матрица представляет собой формализованное пособие тактико-технических характеристик кибератак, систематизированное под матричную структуру. В отличие от традиционных классификаторов угроз, эта модель реализует процессно-ориентированный подход, декомпозирующий атаку на последовательность элементарных действий злоумышленника.

Современные тенденции к построению моделей угроз на основе матрицы MITRE ATT&CK

MITRE ATT&CK — открытый проект [1], анализирующий реальные инциденты и регулярно обновляемый новыми техниками. Его матричная структура отражает весь цикл атаки: тактики расположены по этапам компрометации, техники и подтехники – по методам реализации намерений злоумышленников. Ключевые тенденции этого года включают автоматизацию анализа угроз с применением ИИ, сценарное моделирование многоэтапных атак, адаптивную безопасность и усиление

внимания к рискам облачных сред и цепочек поставок. Современная защита требует применения динамических моделей, интеграции данных из разных источников, цифрового моделирования и строгого документирования по стандартам ФСТЭК, ISO и NIST.

Среди новых вызовов – использование ИИ в атаках, квантовые угрозы, скрытные механизмы обхода защиты и эксплуатация легитимных инструментов. Несмотря на рост их эффективности, инициативу сохраняют специалисты ИБ, развивающие проактивные модели защиты.

От теоретической части, в которой мы разобрали современные тактико-технические методы борьбы, перейдём к практическому применению матрицы MITRE ATT&CK, которое требует особых методик. Эти передовые практики позволяют трансформировать абстрактный каталог тактик в работающую систему управления киберрисками, значительно повышая скорость и точность реагирования на угрозы.

Пример применения MITRE ATT&CK – анализ атаки на Colonial Pipeline [2]: злоумышленники получили доступ через скомпрометированный VPN-пароль, перемещались по сети, отключали защитные системы и вывели данные перед шифрованием, вынудив компанию выплатить выкуп. Инцидент показал важность проактивной защиты критической инфраструктуры и необходимости постоянного обновления моделей угроз.

Заключение

Будущее кибербезопасности зависит от динамичных интегрированных систем, в основе которых – такие инструменты, как MITRE ATT&CK, применение которых обеспечивает устойчивость к атакам в условиях меняющейся цифровой среды. Несмотря на растущую сложность угроз, как например, от атак с применением ИИ, инициатива всё так же остаётся в руках ИБ-специалистов. Будущая информационная безопасность зависит от динамических и интегрированных систем защиты, где матрица-классификатор MITRE ATT&CK послужит главным помощником для описания, прогнозирования и предотвращения кибератак. Такой комплексный подход позволит обеспечить реальную киберустойчивость в условиях постоянно меняющейся цифровой среды.

Список литературы

1. MITRE ATT&CK: база знаний по тактикам и техникам кибератак [Электронный ресурс]. – Режим доступа: https://attack.mitre.org/ (дата обращения: 13.10.2025).

2. Understanding the MITRE ATT&CK Framework» [Электронный ресурс]. – Режим доступа: https://evontech.com/component/easyblog/understanding-the-mitre-att-ck-framework.html?Itemid=159 (дата обращения: 13.10.2025).

УДК 004.056

С.М. КУРИЛЕНКО

Московский физико-технический институт (национальный исследовательский университет), Московская область, Долгопрудный

ПРИВАТНЫЙ СЕМАНТИЧЕСКИЙ ПОИСК С ИСПОЛЬЗОВАНИЕМ ГОМОМОРФНОГО ШИФРОВАНИЯ

Рассматривается защищённый семантический поиск в архитектурах RAG при недоверенном сервере. Мы предлагаем новую практическую схему, сочетающую PIR-навигацию по HNSW-графу с последующим гомоморфным пересчётом метрик сходства. Схема обеспечивает формальные криптографические гарантии конфиденциальности запроса, остаётся совместимой с промышленными индексами ближайших соседей.

В практических RAG-сценариях ИИ-поиска запрос пользователя часто содержит чувствительные сведения (медицинские симптомы, юридическую тактику, корпоративные планы).

Для защиты данных в таких системах имеется два естественных подхода:

1. Ciphertext-ciphertext (ct-ct): зашифровать всё (и базу, и запрос) и проводить расчеты полностью гомоморфно. Так обеспечивается максимум приватности ценой роста вычислительных и коммуникационных затрат.
2. Ciphertext-plaintext (ct-pt): зашифровать только запрос, оставить базу открытой. Это существенно быстрее, если допустимо хранить базу в открытом виде на стороне сервера и цель – скрыть содержание запроса.

Корпус документов может быть публичным или организационно допустимым для хранения на стороне сервера. В такой конфигурации естественна схема ct-pt: мы шифруем только вектор запроса, а для защиты базы можем применить маскирование эмбеддингов.

Задача работы – разработать практические схемы реализации защищенного поиска для обоих подходов и провести серию вычислительных экспериментов, которые покажут, какой прирост производительности дает использование схемы ct-pt по сравнению с ct-ct.

При этом важно обеспечить масштабируемость для множественных клиентов без дублирования индексов, сохранение точности ранжирования результатов поиска, интерактивную скорость ответа (менее 1 с).

Базовая схема ct-pt пайплайна:

- Получение эмбеддинга запроса на стороне клиента.
- Сокращение размерности до 256 с помощью PCA для снижения HE-стоимости.
- Шифрование эмбеддинга.
- Отправка шифрованного эмбеддинга на сервер.
- Шифрованные вычисления сходства со всеми элементами базы.
- Возврат ответа на сервер.

База документов хранится в виде маскированных эмбеддингов, где A – секретная ортогональная/перестановочная матрица (глобальная или по-кластерная). Для схемы ct-ct выполняются те же шаги, но векторы документов в базе зашифрованы.

Очевидно, такая схема не обеспечивает масштабируемости, поскольку время обработки линейно растет с увеличением корпуса документов.

Для решения этой проблемы мы реализовали двухступенчатый вариант схемы, при котором поиск подходящих элементов выполняется двухступенчато:

1. PIR-навигация по HNSW-графу, при котором доверенная сторона управляет обходом индекса, не раскрывая запрос серверу: соседства берутся через PIR, а навигация выполняется в публичном кодовом пространстве многозначных SRP-проекций с квантизацией до четырёх уровней и сравнением по L1.
2. HE-переранжирование кандидатов.

Для проведения экспериментов мы использовали полное гомоморфное шифрование CKSS из библиотеки TeanSEAL в режимах ct-ct и ct-cp, а также частичное гомоморфное шифрование Paillier из библиотеки phe в режиме ct-cp.

Эксперименты на русскоязычных эмбеддингах (RuBERT) показали, что при одинаковой точности (100%) ct-pt на базе CKKS быстрее ct-ct на 85% и обеспечивает время отклика менее 1 с.. Вариант с шифрованием Paillier показал время на ответ более 5 ск., что не обеспечивает интерактивной скорости обработки.

Список литературы

1. Chang, Yijia; Li, Songze. Arbitrary-threshold fully homomorphic encryption with lower complexity // Proceedings of the 34th USENIX Conference on Security Symposium. – USA: USENIX Association, 2025. – P. 431–450. – ISBN 978-1-939133-52-6.
2. Zhao, D. A Note on Efficient Privacy-Preserving Similarity Search for Encrypted Vectors // arXiv:2502.14291. 2025.

УДК 004.056

А.Д. ДОМАШКИН, Л.Н. ЛОГИНОВА

Российский университет транспорта (МИИТ)», Москва

АНАЛИЗ АЛГОРИТМОВ МАШИННОГО ОБУЧЕНИЯ ДЛЯ ДЕТЕКТИРОВАНИЯ АНОМАЛИЙ

Цель исследования: анализ алгоритмов машинного обучения (МО) для детектирования аномалий в высоконагруженных информационных системах (ВИС), используемых в интеллектуальных транспортных системах (ИТС), с применением методов контролируемого и неконтролируемого обучения. В результате исследованы пять алгоритмов МО на наборе данных NF-UQ-NIDS и установлены различия в эффективности алгоритмов, обусловленные их архитектурными особенностями и вычислительной сложностью, что позволяет определить применимость методов для детектирования аномалий.

Одной из важнейших задач обеспечения информационной безопасности (ИБ) ИТС является детектирования аномалий в ВИС. С развитием ИТС требуется внедрение современных подходов обеспечения ИБ, включая применение алгоритмов МО для детектирования аномалий [1], поэтому особое внимание уделяется методам МО, способным выявлять аномальные отклонения как на основе размеченных, так и на основе неразмеченных данных.

Для проведения исследования были выбраны 5 самых популярных алгоритма МО и так же рассмотрены наборы данных (датасет) такие как: CICIDS2017, UNSW-NB15, KDD CUP 99 / NSL-KDD, CSE-CIC-IDS2018, BoT-IoT, ToN-IoT, NF-UQ-NIDS.

Анализ перечисленных наборов данных демонстрирует различия по ключевым характеристикам. Классический набор данных KDD CUP 99 содержит около 5 млн записей, однако характеризуется избыточностью данных и устаревшими типами атак, не отражающими актуальный ландшафт угроз. Его модифицированная версия NSL-KDD устраняет проблему дублирования записей, сокращая объём до 148 тыс. экземпляров, но сохраняет ограничения в актуальности векторов атак. Датасет UNSW-NB15 предоставляет 2.5 млн записей с 49 признаками и девятью категориями современных атак, включая анализ, бэкдоры и эксплойты. CICIDS2017 охватывает семь категорий атак на основе реалистичного фонового трафика с 83 признаками и более чем 2.8 млн записей. Крупномасштабный датасет CSE-CIC-IDS2018 содержит более 16 млн записей с 80 признаками, собранными в инфраструктуре с

420 машинами-жертвами. Специализированные наборы данных BoT-IoT и ToN-IoT содержат 72 млн и 42 млн записей, сконцентрированные на атаках в контексте Интернета вещей и промышленных IoT-систем. Унифицированный набор данных NF-UQ-NIDS [2] агрегирует данные из множественных источников в формате NetFlow версии 9, объединяя преимущества UNSW-NB15, BoT-IoT, CSE-CIC-IDS2018 и ToN-IoT, и содержит около 76 млн записей с 43 признаками, охватывающими временной период с 2015 по 2020 год.

Для проведения тестирования был выбран NF-UQ-NIDS [2], так как он содержит в себе наибольшее количество данных, типов аномалий и является универсальным набором данных, что подходит для общей оценки способностей алгоритмов МО.

Проведённый анализ алгоритмов МО на наборе данных NF-UQ-NIDS выявил различия как в показателях качества детектирования аномалий, так и в вычислительной эффективности. Наиболее высокие результаты по точности и F1-мере показал алгоритм K-ближайших соседей, однако его время предсказания ограничивает применение в системах с высокими скоростями обработки трафика. LDA и Isolation Forest предлагают сбалансированные решения с точки зрения скорости и качества, тогда как One-Class SVM и K-средних оказываются менее эффективны при данном наборе данных. На основе проведенного анализа можно сделать вывод, что выбор конкретного алгоритма должен учитывать требования к вычислительной мощности, характер данных и специфику приложения систем детектирования аномалий. На основе проведенного анализа можно сделать вывод, что выбор конкретного алгоритма должен учитывать требования к вычислительной мощности, характер данных и специфику приложения систем детектирования аномалий. Для ВИС, применяемых в ИТС, наиболее актуальными являются алгоритмы LDA и Isolation Forest, так как являются быстродействующими при сохранения качества и точности детектирования аномалий.

Список литературы

1. Баранов Л.А., Сафронов А.И., Сидоренко В.Г. Развитие интеллектуальных систем управления электрическим транспортом // Автоматика, связь, информатика. 2025. № 10. С. 30–32. DOI: 10.62994/AT.2025.10.10.007.

2. Luay M., Layeghy S., Hosseininoorbin S., Faraji H., Sarhan M., Moustafa N., Portmann M. Temporal Analysis of NetFlow Datasets for Network Intrusion Detection Systems // arXiv preprint arXiv:2503.04404. 2025. DOI:10.48550/arXiv.2503.04404.

УДК 004.056

А.Д. ШЕВЕЙКО, Н.А. ЧУРЮМОВ, Д.Н. ШУРШИКОВ

МИРЭА – Российский технологический университет, Москва

КОМПЛЕКСНЫЙ АНАЛИЗ МЕХАНИЗМОВ БЕЗОПАСНОСТИ COOKIE-ФАЙЛОВ В БРАУЗЕРАХ НА БАЗЕ CHROMIUM И ОСОБЕННОСТИ РЕАЛИЗАЦИИ АТРИБУТА SAMESITE

В статье представлен комплексный анализ механизмов безопасности cookie-файлов в браузерах, построенных на платформе Chromium, с акцентом на практическую реализацию атрибута SameSite. Авторами рассмотрено поведение политик Strict, Lax и None в условиях реальной эксплуатации и выявлен дополнительный режим – неявно заданный Lax, возникающий при отсутствии явного указания атрибута. Результаты исследования имеют практическое значение для разработчиков и специалистов по информационной безопасности, занимающихся защитой клиентской стороны веб-систем.

Введение

В рамках проведенного исследования был выполнен комплексный анализ работы механизмов безопасности cookie-файлов в современных браузерах на базе платформы Chromium. Особое внимание уделялось изучению практической реализации атрибута SameSite и его влияния на общую архитектуру веб-безопасности [1]. В процессе тестирования рассматривались различные аспекты функционирования политик Strict, Lax и None в условиях реальной эксплуатации.А также был найден четвертый тип поведения, отличающийся от стандартных.

Виды SameSite

Атрибут SameSite является характеристикой cookie файлов, определяющей, следует ли отправлять cookie файлы при межсайтовых запросах. Этот механизм предназначен для защиты от CSRF-атак (Cross-Site Request Forgery - межсайтовая подделка запросов), а также других клиентских атак и утечки данных. Механизм Lax ограничивает отправку cookie файлов в большинстве межсайтовых запросов (например, в AJAX-запросах или при загрузке изображений). Тем не менее, cookie файлы передаются при использовании безопасных HTTP-методов (GET, HEAD, OPTIONS, TRACE) в процессе навигации по ссылкам. Механизм Strict предусматривает передачу cookie файлов только в случае, если пользователь находится на сайте, которому принадлежит файл cookie. Передача в иных ситуациях невозможна. Выявлен тип поведения неявно

заданный режим Lax. В случае, если разработчик не указывает значение атрибута SameSite для его файлов cookie, установленное значение не принимает значение None, а принимает положение Lax с особенностями реализации. Данная особенность может привести к уязвимостям, включая возможность реализации CSRF-атак, несмотря на активированный механизм защиты. Кроме того, данный параметр используется для авторизации через OAuth и социальные сети, когда пользователь входит на один сайт через учетную запись другого сервиса [3]. Важным условием является обязательная передача таких cookie файлов только по защищенному соединению. Значение SameSite, установленное как Lax, является стандартной настройкой для большинства сессионных cookie файлов в современных браузерах. Значение SameSite, установленное как Strict, обеспечивает максимальный уровень безопасности и применяется для критически важных операций.

Заключение

Выбор политики SameSite представляет собой компромисс между уровнем безопасности и удобством пользователя. SameSite со значением None обеспечивает кросс-доменную функциональность, необходимую для виджетов и OAuth-авторизации. Значение Lax предлагает сбалансированную защиту для большинства сессий, а Strict гарантирует максимальную безопасность для критических операций, жертвуя комфортом пользователя [4]. В то же время, отсутствие явного указания атрибута SameSite для cookie с режимом Lax создает неопределенное поведение, что делает нежелательным пропуск указания данного параметра.

Список литературы

1. Файлы cookie и локальное хранилище (Microsoft Ignite) [Электронный ресурс]. – Режим доступа: https://learn.microsoft.com/ru-ru/microsoftteams/platform/resources/samesite-cookie-update (дата обращения: 16.10.2025).

2. SameSite cookie HTTP [Электронный ресурс]. – Режим доступа: https://udn. realityripple. com/docs/ Web/HTTP/Headers/Set-Cookie/SameSite (дата обращения: 16.10.2025).

3. Merewood R. Объяснение файлов cookie SameSite [Электронный ресурс]. – Режим доступа: https://web.dev/articles/samesite-cookies-explained?hl=ru (датаобращения: 16.10.2025).

4. Оценка эффективности систем защиты информации и анализ рисков информационной безопасности в организации / Ю.Ю. Громов, П.И. Карасев, Ю.А. Губсков, В.О. Котюкова // Информация и безопасность. – 2022. – Т. 25, № 2. – С. 187-192. – DOI 10.36622/VSTU.2022.25.2.003. – EDN EDRNYF.

УДК 004.056

А.К. ХАЛДИНА

МИРЭА – Российский технологический университет, Москва

ОПЫТ ИСПОЛЬЗОВАНИЯ СОВРЕМЕННЫХ ПРОГРАММНЫХ СРЕДСТВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ С ОТКРЫТЫМ ИСХОДНЫМ КОДОМ

В статье выполнен анализ возможностей современных программных средств защиты информации с открытым исходным кодом. В ходе исследования была опробована комплексная система мониторинга и предотвращения угроз на базе решений Wazuh, Suricata, OSSEC и OpenVAS. Основной результат показал, что интеграция инструментов с открытым исходным кодом не обеспечивает эффективную систему безопасности, сопоставимую по ключевым параметрам с коммерческими аналогами, но значимо уменьшает затраты и обеспечивает базовый уровень защиты.

Введение

Современные коммерческие решения в области информационной безопасности требуют значительных финансовых вложений, что делает их малодоступными для малого и среднего бизнеса, а также для образовательных проектов [1]. В связи с этим актуальной задачей становится оценка эффективности и практическая апробация альтернативных решений с открытым исходным кодом. Необходимо определить, могут ли такие инструменты обеспечить комплексную защиту IT-инфраструктуры, становясь аналоговым, но доступным решением.

Архитектурные особенности и потенциальные риски

Платформа Wazuh [2] – унифицированная платформа SIEM/EDR, осуществляющая мониторинг целостности, агрегацию логов, выявление активности и проверку соответствия стандартам (PCI DSS, GDPR), а также автоматическое реагирование. Платформа требует значительных вычислительных ресурсов при масштабировании и отличается сложной первоначальной настройкой. Пользователи сталкиваются с ограниченными возможностями корреляции событий, а настройка автоматического реагирования требует глубоких технических знаний.

Платформа Suricata [3] – высокопроизводительная сетевая IDS/IPS. Использует мощные правила для глубокой инспекции пакетов (DPI), способна как детектировать, так и активно блокировать трафик, с глубоким пониманием протоколов (HTTP, TLS). Сетевая система создает высокую нагрузку на оборудование при активации полного набора правил.

Разработка собственных сигнатур и тонкая настройка представляют значительную сложность. Эффективность против сложных целевых атак ограничена.

Платформа OSSEC [4] – классическая HIDS (Host-based Intrusion Detection System), которая просматривает системные логи, отслеживает изменения в файлах и ищет признаки вредоносных программ. Но OSSEC имеет устаревшую архитектуру и ограниченную масштабируемость. В системе используются слабые хэш-функции типа SHA-1 для контроля целостности и примитивные методы обнаружения аномалий, что затрудняет интеграцию с современными платформами мониторинга.

Платформа OpenVAS [5] – система сканирования сетевых уязвимостей, использующая базу NVT для автоматической проверки сетевых служб. Сканер демонстрирует длительное время проверки и характеризуется высоким процентом ложных срабатываний. Производительность значительно снижается при сканировании сетей большой емкости. Веб-интерфейс устарел и неудобен, а возможности оценки уязвимостей веб-приложений ограничены.

Заключение

Несмотря на эффективность решений в некоторых определенных областях, они не предоставляют комплексный и надежный подход для полноценного функционирования защиты информации. Решения с открытым исходным кодом являются доступным способом снизить риски и минимально обезопасить свои данные для успешного продолжения деятельности, но не могут быть надежным и долговечным решением.

Список литературы

1. Мальцев П. В. Открытые решения в области информационной безопасности малых предприятий // Информационные технологии и безопасность. – 2023. – № 4. – С. 17–23.

2. Wazuh: The Open Source Security Platform [Электронный ресурс]. – Режим доступа: https://wazuh.com (дата обращения: 22.10.2025).

3. Suricata: Open Source IDS/IPS/NSM Engine [Электронный ресурс]. – Режим доступа: https://suricata.io (дата обращения: 22.10.2025).

4. OSSEC: Open Source HIDS Security [Электронный ресурс]. – Режим доступа: https://www.ossec.net (дата обращения: 22.10.2025).

5. OpenVAS: Open Vulnerability Assessment System [Электронный ресурс]. – Режим доступа: https://www.openvas.org (дата обращения: 22.10.2025).

УДК 004.056

Д.И. НЕСЛУХОВСКИЙ[1,2], В.С. НЕФЕДОВ[1]

[1]МИРЭА – Российский технологический университет, Москва
[2]Акционерное общество «Научно-технический центр «Интеграф», Москва

ОЦЕНКА РАСШИРЕНИЯ ПРОСТРАНСТВА ПРИЗНАКОВ TLS-ОТПЕЧАТКОВ ВЕБ-БРАУЗЕРОВ ВО ВРЕМЕНИ

В работе рассматривается временная динамика расширения пространства множественных признаков TLS-отпечатков веб-браузеров. Предложен подход к количественной оценке динамики появления исследуемых признаков в скользящих временных окнах, позволяющий отслеживать эволюцию TLS-конфигураций как процесс последовательного обогащения признакового пространства.

Введение

С выходом новых версий веб-браузеров возникают ранее неизвестные TLS-параметры, приводящие к расширению пространства признаков, используемых при формировании TLS-отпечатков [1]. Для оценки описанных изменений и их возможных последствий необходим формализованный подход для количественного измерения временной динамики появления новых компонент в конфигурациях TLS.

Накопительная оценка новизны

Рассмотрим множество TLS-отпечатков $\mathcal{D} = \{(y_i, F_i)\}_{i=1}^{n}$, где y_i – год выпуска версии браузера, а $F_i = (C_i, E_i, S_i)$ – совокупность множественных признаков для i-й записи: шифронаборов (C_i, англ. cipher suites), расширений (E_i, англ. extensions) и алгоритмов электронной подписи (S_i, англ. signatures). Каждый компонент $f_i \in F_i$ принадлежит универсальному множеству $\mathcal{U}_f = \bigcup_{i=1}^{n} f_i$ при $f \in \mathcal{F} = \{C, E, S\}$.

Определим объединение признаков для произвольного подмножества записей $A \subseteq \mathcal{D}$ как $U_f(A) = \bigcup_{(y_i, F_i) \in A} f_i$. Для фиксированного начального года s множество элементов признака f, встречавшихся ранее, задаётся как $B_f(s) = U_f(\{i : y_i < s\})$, а множество новых (ранее не встречавшихся) элементов для i-й записи с $y_i \geq s$ как $\Delta_f(i; s) = f_i \setminus B_f(s)$. Запись считается содержащей новые признаки, если выполняется следующее условие:

$$d(i; s) = \begin{cases} 1, & \exists f \in \mathcal{F} : \Delta_f(i; s) \neq \emptyset \\ 0, & \text{иначе} \end{cases}$$

Для пары лет $s \leq e$, где e – конечный год, совокупное число записей с признаками определяется как $R(s; e) = \sum_{i: s \leq y_i \leq e} d(i; s)$, характеризующее накопленный объем признаковой новизны между годами s и e. Множество

всех значений $R(s;e)$ образует верхнетреугольную матрицу $R = [R(s;e)]_{s,e\in\mathcal{Y},e\geq s}$, где $\mathcal{Y} = \{y_i \mid (y_i, F_i) \in D\}$ – множество всех лет.

Для каждого года $y \in \mathcal{Y}$ множество новых элементов определяется как $N_f(y) = U_f(\{i : y_i = y\} \setminus \{i : y_i < y\})$, а их общее количество равно $n_{new}(y) = \sum_{f\in\mathcal{F}} |N_f(y)|$. Таким образом, функция $R(s;e)$ описывает динамику накопления записей с новыми признаками во времени, а $n_{new}(y)$ указывает на годы с появлением новых TLS-параметров.

Экспериментальные данные и результаты вычислений

Для оценки использовалась открытая база TLS-отпечатков JA4DB [2], содержащая в себе свыше 170 тыс. индивидуальных записей для веб-браузеров и иных HTTPS-клиентов. Из неё рассматривалось около 9,3 тыс. уникальных отпечатков с 2009 по 2025 гг., соответствующих конкретным версиям популярных браузеров (Chrome, Firefox, Edge, Safari и Opera). Для каждой записи определен год выпуска версии браузера.

Полученные результаты расчетов представлены на рис. 1. Каждая линия показывает зависимость $R(s;e)$ от конечного года e при фиксированном s, а вертикальные пунктирные линии отмечают годы с $n_{new}(y) > 0$. График демонстрирует периоды интенсивного обновления TLS-параметров и накопление новых элементов в конфигурациях веб-браузеров.

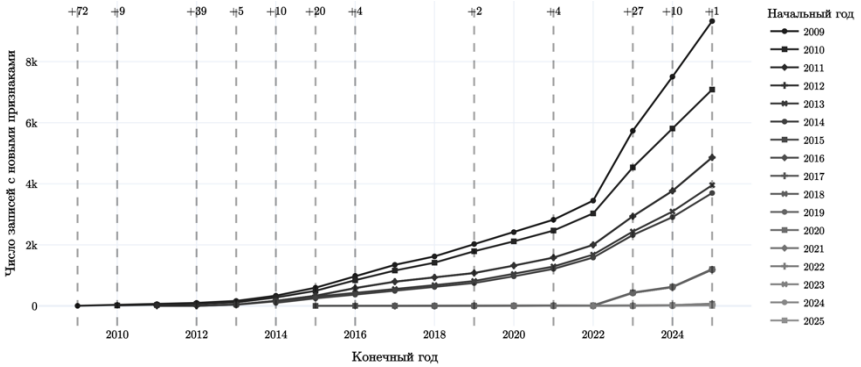


Рис. 1. Число записей с новыми TLS-признаками в скользящих временных окнах

Список литературы

1. Husak M., Cermak M., Jirsik T., Celeda P. HTTPS traffic analysis and client identification using passive SSL/TLS fingerprinting. EURASIP Journal on Information Security, 2016, Vol. 6 (2016), 6 p. DOI: https://doi.org/10.1186/s13635-016-0030-7.

2. JA4+ Database: Community-Maintained Network Fingerprint Repository. URL: https://ja4db.com (дата обращения: 12.09.2025).

УДК 004.056.5

Е.В. ХАРИТОНОВ[1], В.Ю. ЖИВЦОВ[2]

[1]Самарский государственный экономический университет
[2]Самарский государственный медицинский университет

ДЕТЕКТИРОВАНИЕ УЯЗВИМОСТЕЙ НА ОСНОВЕ ГРАФОВЫХ НЕЙРОННЫХ СЕТЕЙ

В работе рассматриваются методы детектирования уязвимостей в программном обеспечении с использованием графовых нейронных сетей. Предложенный подход обеспечивает анализ структурных и контекстных зависимостей в исходном коде, что позволяет выявить потенциально опасные фрагменты. Обученные модели могут формировать основу автономных систем интеллектуального мониторинга.

Современные программно-технические комплексы характеризуются высокой степенью сложности, модульности и взаимосвязанности, что повышает вероятность возникновения уязвимостей в исходном коде и логике взаимодействия компонентов. Классические методы статического анализа обладают ограниченной эффективностью при обнаружении скрытых зависимостей и сложных межмодульных связей, приводя к снижению уровня защищённости информационной инфраструктуры. В целях повышения точности детектирования и минимизации ложноположительных срабатываний перспективным является использование подходов, основанных на машинном обучении и представлении программных структур в виде ориентированных графов.

Программный код может быть представлен в виде вершин, обозначающих различные элементы программы (инструкции, переменные, функции, блоки кода), и рёбер между ними, отражающих логические связи, передачу данных, потоки управления и вызовы функций [1, 2].

Графовые нейронные сети обеспечивают формирование векторного представления признаков с учётом контекстных зависимостей и позволяют выявлять аномальное взаимодействие, указывающее на потенциальные дефекты безопасности. Применение таких моделей способствует автоматизации процессов анализа исходного кода и формированию интеллектуальных систем превентивного обнаружения угроз.

Каждый узел графа обрабатывается с учётом информации, поступающей от его непосредственных соседей в структуре. Такой

механизм обеспечивает учёт контекстных зависимостей, позволяя модели анализировать не только локальные свойства узлов, но и взаимосвязи между ними.

В процессе обновления состояния каждого узла используются обучаемые весовые параметры и смещения, настраиваемые в ходе обучения. После выполнения нескольких последовательных итераций нейронная сеть формирует векторное представление всей графовой структуры, отражающее взаимосвязи и зависимости элементов программного обеспечения [3].

На вход обученной модели подается граф, построенный по исходному коду, результатом является вероятность наличия определённой уязвимости в оцениваемом фрагменте:

$$P = \sigma(w \cdot h + b),$$

где h – полученное векторное представление анализируемого фрагмента исходного кода, w, b – обученные параметры линейного классификатора (веса и смещение соответственно), σ – сигмоидная функция активации, преобразующая выходное значение в диапазон от 0 до 1, интерпретируемые как вероятность наличия уязвимости.

Использование обучаемых представлений позволяет адаптировать модель к различным языкам программирования и архитектурным стилям, сохраняя интерпретируемость результатов [4]. Интеграция графовых нейронных сетей в инструменты обеспечения безопасности программного обеспечения формирует основу для создания автономных систем интеллектуального мониторинга.

Список литературы

1. Chu Z., Wan Y., Li Q., Wu Y., Zhang H., Sui Y., Xu G., Jin H. Graph Neural Networks for Vulnerability Detection: A Counterfactual Explanation // Proceedings of the 33rd ACM SIGSOFT International Symposium on Software Testing and Analysis (ISSTA '24). 2024. URL: https://arxiv.org/abs/2404.15687 (дата обращения: 13.09.2025).

2. Олин Р.А. Методы обеспечения безопасности данных в распределённых системах искусственного интеллекта / Р.А. Олин, В.В. Бондаренко // Актуальные проблемы радиоэлектроники и телекоммуникаций – Самара: ООО «АРТЕЛЬ», 2025. – С. 198–200. – EDN ITHYTA

3. Luo Y., Xu W., Xu D. Detecting Code Vulnerabilities with Heterogeneous GNN Training // arXiv preprint arXiv:2502.16835. 2025. URL: https://arxiv.org/abs/2502.16835 (дата обращения: 19.09.2025).

4. Zhuang Y., Liu Z., Qian P., Liu Q., Wang X., He Q. Smart Contract Vulnerability Detection using Graph Neural Network // Proceedings of the Twenty-Ninth International Joint Conference on Artificial Intelligence (IJCAI-20). 2020. P. 3283–3290. URL: https://www.ijcai.org/proceedings/2020/454 (дата обращения: 29.09.2025).

КИБ-2025

КИБЕРНЕТИКА
И ИНФОРМАЦИОННАЯ
БЕЗОПАСНОСТЬ

Направление

Теоретическая и практическая криптография

Руководитель секции – ПУДОВКИНА М.А.,
д.ф.-м.н., профессор

УДК 519.7

М.А. ПУДОВКИНА

Национальный исследовательский ядерный университет «МИФИ», Москва

О БУМЕРАНГ-МАТРИЦАХ S-БОКСОВ НА ОСНОВЕ ПРЕОБРАЗОВАНИЯ ФЕЙСТЕЛЯ

В связи с исследованием различных групп наложения ключа рассматриваются свойства бумеранг-матрицы S-боксов на основе преобразования Фейстеля над произвольной конечной абелевой группой $(X,+)$. Получены элементы бумеранг-матрицы для 3-раундового преобразования Фейстеля на $(X,+)$. В качестве иллюстрации рассмотрены аддитивные группы кольца вычетов $\mathbb{Z}_{2^n}$ и векторного пространства $V_n(2^m)$ над полем $\mathbb{F}_{2^m}$, которые наиболее часто применяются на практике. Для группы $(V_n(2^m),+)$ в качестве следствия получен известный ранее результат.

Пусть $(X,+)$ – произвольная конечная абелевая группа с нейтральным элементом 0_X, $X^\times = X\backslash\{0_X\}$. Для характеризации криптографических свойств подстановки s на $(X,+)$ относительно разностного метода и его обобщений рассматриваются разностная матрица $p(s) = [\![p_{\varepsilon,\lambda}(s)]\!]$, бумеранг-матрица $b(s) = [\![b_{\varepsilon,\lambda}(s)]\!]$, бумеранг-разностная матрица $b^{(F)}(s) = [\![b^{(F)}_{\varepsilon,\lambda}(s)]\!]$, элементы которых заданы для $\varepsilon,\lambda \in X^\times$ соответственно условиями

$$p_{\varepsilon,\lambda}(s) = |\{\alpha \in X: (\alpha+\varepsilon)^s - \alpha^s = \lambda\}|,$$

$$b_{\varepsilon,\lambda}(s) = \left|\left\{\alpha \in X: ((\alpha+\varepsilon)^s + \lambda)^{s^{-1}} = (\alpha^s+\lambda)^{s^{-1}} + \varepsilon\right\}\right|,$$

$$b^{(F)}_{\varepsilon,\lambda}(s) = |\{\alpha \in X: (\alpha+\varepsilon)^s - \alpha^s = (\alpha+\varepsilon+\lambda)^s - (\alpha+\lambda)^s\}|,$$

где $\beta^s = s(\beta)$ для каждого $\beta \in X$.

Порядком бумеранг-равномерности подстановки s называется число

$$\sigma^{(b)}(s) = \max\left\{b_{\varepsilon,\lambda}(s)\middle|(\varepsilon,\lambda) \in X^\times \times X^\times\right\}.$$

Пусть $d,m,n \in \mathbb{N}$, $d,n \geq 2$, $V_n(2^m)$ – n-мерное векторное пространство над полем $\mathbb{F}_{2^m}$. В [1] для подстановки на основе 3-раундового преобразования Фейстеля над $V_n(2) \times V_d(2)$ показано, что порядок бумеранг-равномерности равен 2^{n+d}, т.е. является максимальным. Обобщим данный результат, в частности, получим элементы бумеранг-матрицы и порядок бумеранг-равномерности 3-раундового

преобразования Фейстеля на произвольной конечной абелевой группе $(X,+)$.

Пусть $S(X)$ – симметрическая группа на X, $\mathrm{ord}(\beta)$ – порядок элемента $\beta \in X$:

$$X^{[2]} = \{\alpha \in X | \mathrm{ord}(\alpha) = 2\}.$$

Теорема 1. *Пусть* $(X,+)$ *– произвольная конечная абелевая группа,* $s_i \in S(X)$, $g_{s_i}: X^2 \to X^2$ *задано условием*

$$g_{s_i}: (\alpha_1, \alpha_2) \mapsto (\alpha_2, \alpha_1 + \alpha_2^{s_i})$$

для каждой пары $(\alpha_1, \alpha_2) \in X^2$, $i = 1,2,3$. *Тогда для всех* $\varepsilon_1, \lambda_2 \in X^{\times}$, $\varepsilon = (\varepsilon_1, 0_X)$, $\lambda = (0_X, \lambda_2)$ *справедливо равенство*

$$b_{\varepsilon,\lambda}\left(g_{s_1} g_{s_2} g_{s_3}\right) = |X| \cdot b^{(F)}_{\lambda_2,\varepsilon_1}(s_2).$$

Кроме того, если $X^{[2]} \neq \emptyset$ *и* $\lambda_2 \in X^{[2]}$, *то*

$$b_{(-\lambda_2,0_X),(0_X,\lambda_2)}\left(g_{s_1} g_{s_2} g_{s_3}\right) = |X| \cdot \sum_{\theta \in X^{[2]} \cup \{0_X\}} p_{\lambda_2,\theta}(s_2).$$

В качестве иллюстрации применения теоремы 1 рассмотрим две группы наложения $(V_n(2^m),+)$, $(\mathbb{Z}_{2^n},+)$, которые чаще всего используются на практике в алгоритмах блочного шифрования.

Следствие 2. *Пусть выполнены условия теоремы 1,* $n, m \in \mathbb{N}, n \geq 2$. *Тогда:*

1) *если* $(X,+) = (V_n(2^m),+)$, *то для каждого* $\lambda_2 \in V_n(2^m)^{\times}$ *справедливо равенство*

$$\sigma^{(b)}\left(g_{s_1} g_{s_2} g_{s_3}\right) = b_{(-\lambda_2,0_X),(0_X,\lambda_2)}\left(g_{s_1} g_{s_2} g_{s_3}\right) = 2^{nm};$$

2) *если* $(X,+) = (\mathbb{Z}_{2^n},+)$, *то*

$$b_{(-\lambda_2,0_X),(0_X,\lambda_2)}\left(g_{s_1} g_{s_2} g_{s_3}\right) = 2^n p_{2^{n-1},2^{n-1}}(s_2),$$

причем $\sigma^{(b)}\left(g_{s_1} g_{s_2} g_{s_3}\right) = 2^{2n}$, *если* 2^{n-1} *– линейный транслятор подстановки* s_2.

Заметим, что при $(X,+) = (V_n(2^m),+)$ в качестве следствия из теоремы 1 получен «классический» результат работы [1].

Список литературы

1. Tian S., Boura C., Perrin L. Boomerang Uniformity of Popular S-box Constructions // Designs Codes and Cryptography, 2020, 88(1), DOI: 10.1007/s10623-020-00785-0

УДК 519.7

Д.А. БУРОВ[1], Д.А. КОНОНОВ[2]

[1]Лаборатория ТВП, Москва
[2]ФСР БИТ, Москва

КЛАССЫ ПОДСТАНОВОК АБЕЛЕВЫХ ГРУПП С ВЫСОКОЙ НЕЛИНЕЙНОСТЬЮ И НИЗКОЙ РАЗНОСТНОЙ δ-РАВНОМЕРНОСТЬЮ, ПОСТРОЕННЫЕ НА ОСНОВЕ ЛОГАРИФМИЧЕСКИХ ПОДСТАНОВОК

Построены классы подстановок мультипликативной группы конечного поля, а также группы $\mathbb{Z}_2 \times \mathbb{Z}_N$ с низкой разностной δ–равномерностью и высокой нелинейностью. Получена оценка нелинейности биективного отображения конечных абелевых групп с помощью дефицита. Получена достижимая граница значений нелинейности логарифмических подстановок.

Представляет интерес построение алгоритмов блочного шифрования, в которых в качестве операции наложения ключа используется эффективно реализуемая операция (например сложение в $\mathbb{Z}_N$), отличная от XOR (группа сдвигов, индуцируемая операцией XOR является весьма структурированной, что может быть использовано в различных методах криптоанализа). Для этого требуются подстановки, нелинейные относительно используемых операций. Построению подстановок на абелевых группах, отличных от аддитивной группы векторного пространства над конечным полем, посвящено существенно меньшее (по сранению со случаем аддитивной группы конечного поля) число работ (см., например, [1–3]). Известно, что для аддитивной группы кольца вычетов оптимальными с точки зрения разностной δ–равномерности и числа нулей в разностной матрице являются так называемые логарифмические подстановки [3].

При сопряжении логарифмических подстановок [3] на $\mathbb{Z}_{q-1}$ изоморфизмом $\xi\colon \mathbb{F}_q^* \to (\mathbb{Z}_{q-1}, +)$ получим подстановки на $\mathbb{F}_{q-1}^*$,

$$f(x) = \begin{cases} ax + b, & \text{если } ax + b \neq 0, \\ b, & \text{если } ax + b = 0, \end{cases} \quad x, a, b \in \mathbb{F}_q^*,$$

которые также будем называть логарифмическими.

Разностной δ–равномерностью отображения $f\colon G \to H$ называется величина $\delta(f) = \max\{\delta_{\alpha,\beta}(f)\colon \alpha \in G^{\times}, \beta \in H\}$, где G, H– абелевы группы, $\delta_{\alpha,\beta}(f) = |\{x\colon f(x +_G \alpha) -_H f(x) = \beta\}|$, $\alpha \in G$, $\beta \in H$. Дефицитом [3]f называют величину $D(f) = |\{(\alpha,\beta) \in G^* \times H\colon \delta_{\alpha,\beta}(f) = 0\}|$. Преобразованием Фурье отображения f при $\alpha \in G$, $\beta \in H$ называется

величина $\hat{f}(\alpha,\beta)=\sum_{x\in G}\chi_\beta(f(x))\overline{\psi_\alpha(x)}$, где χ_β — нетривиальный характер группы H, ψ_α — характер группы G. Линейностью и нелинейностью [4] f называются соответственно величины

$$\mathcal{L}(f)=\max_{\alpha\in G,\beta\in H}\left|\hat{f}(\alpha,\beta)\right|,\ \mathcal{NL}(f)=\left(|G|-\mathcal{L}(f)\right)\cdot|H|^{-1}.$$

Получена нижняя оценка нелинейности биективного отображения абелевых групп с использованием дефицита: $\mathcal{NL}(f)\geqslant 1-\frac{1}{n}\sqrt{2+2D(f)}$. Как следствие усилены нижние оценки нелинейности подстановок с оптимальным дефицитом [3] аддитивных групп конечного поля и циклической группы, полученные в [5].

С использованием аппарата тригонометрических сумм получена верхняя оценка линейности логарифмических подстановок $f\in S(\mathbb{F}_q^*)$ при $q\geq 5$: $\mathcal{L}(f)\leqslant\sqrt{q}+1$.

Аналогично конструкции Z. Zha, L. Hu, S. Sun [6] предложена конструкция подстановок, полученных из логарифмических их изменением на некотором подполе. Установлено, что такие отображения являются биективными и разностно 3-равномерными. Также получены оценки нелинейности таких отображений. Аналогично C. Carlet, D. Tang, X. Tang и Q. Liao [7] предложена конструкция подстановок на группе $\mathbb{Z}_2\times\mathbb{Z}_N$, использующая вместо подстановки обращения логарифмическую подстановку. Установлено, что такие отображения являются биективными и разностно 6-равномерными. Получены достаточные условия, при которых они разностно 5-равномерны. Для одного класса линеаризованных многочленов получена граница разностной δ-равномерности и нижняя граница нелинейности: $n\geqslant 3$, $a,b\in\mathbb{F}_{2^n}^*$, x^3+ax+b не имеет корней в $\mathbb{F}_{2^n}$, $f(x)=x^4+ax^2+bx$. Тогда $f\in S(\mathbb{F}_{2^n}^*)$ и

$$\delta(f)\leqslant 3,\mathcal{NL}(f)\geqslant 1-3\sqrt{2^n}(2^n-1)^{-1}.$$

Список литературы

1. Глухов М.М. О числовых параметрах, связанных с заданием конечных групп системами образующих элементов // Тр. по дискр. матем. 1997. № 1. С. 43–46.
2. Глухов М.М. О матрицах переходов разностей при использовании некоторых модулярных групп // Матем. вопр. криптогр. 2013. № 4. С. 27–47.
3. Panario D., Sakzad A., Stevens B., Wang Q. Two new measures for permutations: ambiguity and deficiency // IEEE Transactions on Information Theory, 2011 57. С. 7648–7657.
4. Drakakis K., Requena V., McGuire G. On the nonlinearity of exponential Welch Costas functions // IEEE Transactions on information theory 2010. № 56. С. 1230–1238.
5. Panario D., Sakzad A., Stevens B., Thomson D., Wang Q. Ambiguity and deficiency of permutations over finite fields with linearized difference map // IEEE transactions on information theory, 2013. № 59. С. 5616–5626.
6. Zha Z., Hu L., Sun S. Constructing new differentially 4-uniform permutations from the inverse function // Finite Fields and Their Applications 2014 № 25. С. 64–78.
7. Carlet C., Tang D., Tang X., Liao Q. New construction of differentially 4-uniform bijections // Proceedings of INSCRYPT 2013, 9th International Conference 2011. Lect. Notes in Comp. Sci. 2014 8567. С. 409.

УДК 519.7

Д.А. БУРОВ[1], С.В. КОСТАРЕВ[2]

[1]Лаборатория ТВП, Москва
[2]ФСР БИТ, Москва

ОБ ИНВОЛЮТИВНОСТИ МАКСИМАЛЬНО РАССЕИВАЮЩИХ МАТРИЦ С НЕТРИВИАЛЬНОЙ ГРУППОЙ АВТОМОРФИЗМОВ

Описаны необходимые и достаточные условия существования инволютивных матриц в классе матриц с нетривиальной регулярной группой автоморфизмов. Доказана теорема о несуществовании максимально рассеивающих матриц с регулярной абелевой группой автоморфизмов, отличной от элементарной абелевой 2-группы.

Линейное преобразование поля $\mathbb{F}_2$ наиболее часто используется в качестве L-слоя XSL-алгоритмов блочного шифрования. Вместе с тем эффективная реализация линейного преобразования является довольно сложной задачей. Выбор в качестве L-слоя инволютивной матрицы потенциально может увеличить эффективность реализации алгоритма. В связи с увеличением стойкости алгоритма блочного шифрования к разностному и линейному методам, матрицу, задающую L-слой, предпочтительнее выбирать с как можно большим коэффициентом рассеивания. Матрицы, имеющие максимальный коэффициент рассеивания (см., например, [1]) называются максимально рассеивающими (MP-) матрицами. Таким образом, актуален вопрос построения инволютивных MP-матриц.

Эффективно строить MP-матрицу удается, например, в классе матриц с нетривиальной группой автоморфизмов (см. [2]). Рассмотрим вопрос построения инволютивных MP-матриц в классах матриц с нетривиальной группой автоморфизмов.

Определим действие на $(\mathbb{F}_{2^r})_{n,n}$: $g=(g_1,g_2)\in S_n^2$ действует на $A=(a_{i,j})\in(\mathbb{F}_{2^r})_{n,n}$ по правилу $A^g=A^{(g_1,g_2)}=(a_{g_1(i),g_2(j)})$.

Определение 1. *Группой автоморфизмов матрицы* $A\in(\mathbb{F}_{2^r})_{n,n}$ *назовем множество* $Aut(A)=\{g\in S_n\times S_n \mid A^g=A\}$.

Через $M_{n,r}(G)$, $G<S_n$, обозначим множество $n\times n$ матриц вида

$$M_{n,r}(G) = \{A \in (\mathbb{F}_{2^r})_{n\times n} \mid Aut(A) = \{(g,g) \mid g \in G\}\}.$$

Далее в случае, когда $G < S_n$ – регулярная группа, ее элементы будут занумерованы следующим образом $G = \{g_1, g_2, \ldots, g_n\}$, где $g_i(1) = i$, $i = 1, \ldots, n.$

Утверждение 1. Пусть $A = (a_{i,j}) \in M_{n,r}(G) \cap GL(n, 2^r)$, $G < S_n$, G – регулярная группа. Тогда и только тогда $A^{-1} = A$, когда выполнена система равенств

$$\begin{cases} \sum_{i=1}^{n} a_{1,i} a_{1,g_i^{-1}(1)} = 1, \\ \sum_{i=1}^{n} a_{1,i} a_{1,g_i^{-1}(k)} = 0, k = 2, \ldots, n. \end{cases}$$

Теорема 2. Пусть $A = (a_{i,j}) \in M_{n,r}(G) \cap GL(n, 2^r)$, $G < S_n$, G – регулярная абелева группа и A является MP-матрицей. Тогда и только тогда $A^{-1} = A$, когда G – элементарная абелева 2-группа и $\sum_{i=1}^{n} a_{1,i} = 1.$

Следствием теоремы 2 является известный факт, что инволютивных MP-циркулянтов не существует [3].

Список литературы

2. Gupta K. C., Pandey S. K., Ray G. I., Samanta S. Cryptographically significant mds matrices over finite fields: A brief survey and some generalized results. Advances in Mathematics of Communications. 2019, № 13(4), pp. 779–843.

3. Буров Д.А., Костарев С.В. Группы автоморфизмов максимально рассеивающих матриц. 14th Workshop on Current Trends in Cryptology (CTCrypt 2025). pp. 131–156.

4. Liu M., Sim S.M. Lightweight MDS generalized circulant matrices. FSE 2016, LNCS, 2016, v. 9783, pp. 101–120.

УДК 519.7

Д.А. БУРОВ[1], Д.А. КОНОНОВ[2]

[1]Лаборатория ТВП, Москва
[2]ФСР БИТ, Москва

О СВЯЗИ НЕЛИНЕЙНОСТИ И РАЗНОСТНОЙ δ-РАВНОМЕРНОСТИ ПОДСТАНОВОК НА АБЕЛЕВЫХ ГРУППАХ С РАССЕИВАНИЕМ ЭЛЕМЕНТОВ ПО СМЕЖНЫМ КЛАССАМ

Работа посвящена исследованию связи параметров отображений $f: G \to H$ конечных абелевых групп G, H, характеризующих нелинейность и разностную δ-равномерность со свойствами по рассеиванию смежных классов группы G. Также рассмотрены свойства транзитивности группы $\langle W^\rho, f\rangle$, где $f \in S(G)$, W^ρ – правое регулярное представление подгруппы $W < G$, действующее на G.

Недостаточная нелинейность функции зашифрования используется во многих методах криптоанализа. Для обеспечения нелинейности выбираются отображения с низкими значениями линейной, разностной и других характеристик. Другим классом криптографически слабых являются отображения, которые переводят набор смежных классов в набор смежных классов. Качество рассеивания определяется матрицей (W, U)-пересечений $P_{W,U}(f) = (p_{\xi,\theta}^{W,U})_{\xi,\theta}$, элементы которой равны $p_{\xi,\theta}^{W,U}(f) = P\{f(x) \in U + \theta | x \in W + \xi\}$ – вероятностям переходов из смежного класса $W + \xi$ группы G в смежный класс $U + \theta$ группы H: чем ближе матрица $P_{W,U}(f)$ к равномерной, тем лучше рассеивание.

В [1] получены оценки линейности и разностной δ-равномерности через вероятности переходов смежных классов отображений двоичных векторных пространств $f: V_n \to V_m$, а также (при $f \in S(V_n)$) изучены свойства транзитивности группы $\langle W^\rho, f\rangle$, $W < V_n$. В настоящей работе обобщены некоторые результаты для отображений $f: G \to H$ произвольных конечных абелевых групп G и H, получена связь транзитивности группы $\langle W^\rho, f\rangle$ с нелинейностью и дефицитом f, получено условие, при котором $\langle W^\rho, f\rangle$ интранзитивна, когда f логарифмическая подстановка.

Через $[G: W]$ обозначим множество представителей смежных классов группы G по подгруппе W. Разностной δ–равномерностью отображения $f: G \to H$ называется величина $\delta(f) = \max\{\delta_{\alpha,\beta}(f): \alpha \in G^\times, \beta \in H\}$, где

$\delta_{\alpha,\beta}(f) = |\{x: f(x+_G\alpha)-_H f(x) = \beta\}|,\ \alpha \in G,\ \beta \in H.$ Преобразованием Фурье отображения f при $\alpha \in G,\ \beta \in H$ называется величина $\hat{f}(\alpha,\beta) = \sum_{x\in G} \chi_\beta(f(x))\overline{\psi_\alpha(x)}$, где χ_β – нетривиальный характер группы H, ψ_α – характер группы G. Линейностью и нелинейностью f называются величины $\mathcal{L}(f) = \max_{\alpha\in G,\beta\in H}\left|\hat{f}(\alpha,\beta)\right|,\quad \mathcal{NL}(f) = |H|^{-1}(|G| - \mathcal{L}(f))$ соответственно.

Теорема 1. *Пусть $f \in S(G)$, G — конечная абелева группа, $W < G$, $\langle W^\rho, f\rangle$ интранзитивна. Тогда $\mathcal{L}(f) \geqslant (|W|^{-1} - |G|^{-1})^{-1}$.*

Известно, что линейность логарифмических подстановок $f \in S(\mathbb{F}_q^*)$ удовлетворяет неравенству $\mathcal{L}(f) \leqslant \sqrt{q} + 1$ при $q \geqslant 5$. Получено условие транзитивности группы $\langle W^\rho, f\rangle$, где $|W| \geqslant (q-1)q^{-1/2}$ при $W < \mathbb{F}_q^*$.

Ранее Д.А. Кононовым оценка линейности подстановок $f \in S(G)$ с использованием величины $D(f) = |\{(\alpha,\beta) \in G^* \times G : \delta_{\alpha,\beta}(f) = 0\}$, называемой дефицитом: $\mathcal{L}(f) \leqslant \sqrt{2 + 2D(f)}$. Показано, что группа $\langle W^\rho, f\rangle$ транзитивна, если справедливо неравенство

$$|W| \geqslant \left(|G|\sqrt{2 + 2D(f)}\right)\left(|G| + \sqrt{2 + 2D(f)}\right)^{-1}.$$

Теорема 2. *Пусть G, H – конечные абелевы группы, $f: G \to H$. Тогда для любых подгрупп $W < G$, $U < H$ выполнены неравенства*

$$\mathcal{L}(f) \geqslant (|W|^{-1} - |G|^{-1})^{-1}|W| \sum_{\xi\in[G:W],\theta\in U} (p_{\xi,\theta}^{W,U}(f)^2 - |H|^{-1}|U|),$$

$$\delta(f) \geqslant |U|^{-1}(|W| - 1)^{-1} \cdot (|G|^{-1}|W|^2 \sum_{\xi\in[G:W],\theta\in U} p_{\xi,\theta}^{W,U}(f)^2 - 1).$$

Также получены похожие оценки снизу для линейности $\mathcal{L}(f)$ сбалансированной функции f и разностной δ-равномерности функции $f \in S(G)$.

Список литературы

1. Буров Д.А. О связи линейной и разностной характеристик отображений двоичных векторных пространств с характеристиками рассеивания по блокам систем импримитивности группы сдвигов двоичного векторного пространства // Дискретная математика. 2023. № 1. С. 3–34.

УДК 519.7

Д.А. БУРОВ[1], Д.А. КОНОНОВ[2]

[1]Лаборатория ТВП, Москва
[2]ФСР БИТ, Москва

ВЫРАЖЕНИЕ НЕКОТОРЫХ КРИПТОГРАФИЧЕСКИХ ХАРАКТЕРИСТИК ПОДСТАНОВОК НА АБЕЛЕВЫХ ГРУППАХ ЧЕРЕЗ РАССЕИВАНИЕ СМЕЖНЫХ КЛАССОВ

Работа посвящена исследованию связи параметров отображений $f: G \to H$ конечных абелевых групп G, H, характеризующих линейность и разностную δ-равномерность, рассеивание групп по смежным классам, а также связи с другими криптографическими характеристиками.

Недостаточная нелинейность функции зашифрования используется во многих методах криптоанализа. Для обеспечения нелинейности выбираются отображения с низкими значениями линейной, разностной, разностно-линейной характеристик и т.д. Другим классом криптографически слабых отображений являются отображения, которые переводят набор смежных классов в набор смежных классов. Качество рассеивания отображением $f: G \to H$, G, H – абелевы группы, определяется матрицей (W, U)-пересечений $P_{W,U}(f) = (p_{\xi,\theta}^{W,U})_{\xi,\theta}$, элементы которой равны $p_{\xi,\theta}^{W,U}(f) = P\{f(x) \in U + \theta | x \in W + \xi\}$ – вероятностям переходов элементов из смежного класса $W + \xi$ группы G в смежный класс $U + \theta$ группы H: чем ближе матрица (W, U)-пересечений к равномерной матрице, тем лучше рассеивание.

В [1] показано, что многие криптографические характеристики отображений $f: V_n \to V_m$ двоичных векторных пространств можно интерпретировать в терминах матрицы (W, U)-пересечений при подходящем выборе подпространств $W < V_n$, $U < V_m$. В настоящей работе некоторые результаты из [1] обобщены на случай отображений произвольных конечных абелевых групп.

Через $[G: W]$ обозначим множество представителей смежных классов группы G по подгруппе W. Разностной δ–равномерностью отображения $f: G \to H$ называется величина $\delta(f) = \max\{\delta_{\alpha,\beta}(f): \alpha \in G^{\times}, \beta \in H\}$, где $\delta_{\alpha,\beta}(f) = |\{x: f(x +_G \alpha) -_H f(x) = \beta\}|$, $\alpha \in G$, $\beta \in H$. Преобразованием Фурье отображения f при $\alpha \in G$, $\beta \in H$ называется величина $\hat{f}(\alpha, \beta) = \sum_{x \in G} \chi_\beta(f(x))\overline{\psi_\alpha(x)}$, где χ_β – нетривиальный характер группы H, ψ_α – характер группы G. Линейностью и нелинейностью f называются величины $\mathcal{L}(f) = \max_{\alpha \in G, \beta \in H} \left|\hat{f}(\alpha, \beta)\right|$, $\mathcal{NL}(f) = |H|^{-1}(|G| - \mathcal{L}(f))$

соответственно.

Пусть G, H – конечные абелевые группы, $W < G$, $U < H$, $f: G \to H$. Доказано, что

$$p^{W,U}_{\xi,\theta}(f) = |U| \cdot |G|^{-1}|H|^{-1} \sum_{\alpha \in W^{\perp}, \beta \in U^{\perp}} \chi_{\xi}(\alpha)\overline{\psi_{\theta}(\beta)}\hat{f}(\alpha,\beta),$$

где $W^{\perp} = \{g \in G: \chi_g(w) = 1 \; \forall w \in W\}$,

$U^{\perp} = \{h \in H: \chi_h(u) = 1 \; \forall u \in U\}$, $\xi \in [G:W]$, $\theta \in [H:U]$.

Также показано, что

$$\delta_{\xi,\theta}(f) = |G|^{-1}|H|^{-1} \sum_{\alpha \in G, \beta \in H} \chi_{\xi}(\alpha)\overline{\psi_{\theta}(\beta)}|\hat{f}(\alpha,\beta)|^2, \quad \xi \in G, \theta \in H.$$

Кроме того, получено выражение для сумм квадратов вероятностей и сумм квадратов преобразований Фурье

$$\sum_{\xi \in [G:W], \theta \in [H:U]} |p^{W,U}_{\xi,\theta}(f)|^2 = |U| \cdot |W| \cdot |G| \cdot |H| \sum_{\alpha \in W^{\perp}, \beta \in U^{\perp}} |\hat{f}(\alpha,\beta)|^2.$$

Показано, что вероятность из метода усеченных разностей $P\{f(x) - f(y) \in U \mid x - y \in W\}$ выражается через элементы матрицы $P_{W,U}(f)$,

$$P\{f(x) - f(y) \in U \mid x - y \in W\} = |G|^{-1} \, |W| \sum_{\xi \in [G:W], \theta \in [H:U]} p^{W,U}_{\xi,\theta}(f)^2.$$

Доказано, что разностно-линейные преобладания $\mathrm{dlc}_{\alpha,\beta}(f) = \sum_{x \in G} \psi_{\beta}(f(x+\alpha) - f(x))$ аналогично случаю двоичных векторных пространств выражаются через преобразования Фурье:

$$\mathrm{dlc}_{\alpha,\beta}(f) = |G|^{-1} \sum_{g \in G} \chi_{\alpha}(g)|\hat{f}(g,\beta)|^2, \quad \alpha \in G, \beta \in H.$$

На стойкость относительно метода бумеранга влияют величины $\mathrm{bc}_{\alpha,\beta}(f) = P\{f(x) - f(y) = \beta, f(x+\alpha) - f(y+\alpha) = \beta\}$, $\alpha \in G, \beta \in H$.

Показано, что для величины $\mathrm{bc}_{\xi,\theta}(f)$, $\xi \in G$, $\theta \in H$, верно равенство

$$\mathrm{bc}_{\xi,\theta}(f) = |G|^{-4}|H|^{-2} \cdot \sum_{\alpha_1,\alpha_2 \in G, \beta_1,\beta_2 \in H} \chi_{\xi}(\alpha_1 + \alpha_2) \cdot$$

$$\cdot \overline{\psi_{\theta}(\beta_1 + \beta_2)}\overline{\hat{f}(\alpha_1,\beta_1)}\hat{f}(\alpha_2,\beta_2)\hat{f}(-\alpha_2,\beta_1)\hat{f}(\alpha_1,-\beta_2).$$

Пусть G, K, H – конечные абелевые группы, $f_1: G \to K$, $f_2: K \to H$, $f = f_1 f_2$. Для любых подгрупп $W < G$, $U < K$ через характеры получено соотношение для $p^{W,U}_{\gamma_1,\gamma_2}(f)$. В качестве следствия из него найдены соотношения для $\delta_{\alpha,\beta}(f)$ и $\mathrm{dlc}_{\alpha,\beta}(f)$ произведения отображений.

Список литературы

1. Буров Д.А. О связи линейной и разностной характеристик отображений двоичных векторных пространств с характеристиками рассеивания по блокам систем импримитивности группы сдвигов двоичного векторного пространства // Дискретная математика. 2023. Т. 35. Вып. 1. С. 3–34.

УДК 519.7

Д.А. БУРОВ[1], С.В. КОСТАРЕВ[2]

[1]*Лаборатория ТВП, Москва*
[2]*ФСР БИТ, Москва*

ОРБИТАЛЬНЫЕ ИНВАРИАНТНЫЕ ПОДПРОСТРАНСТВА МАТРИЦ С НЕТРИВИАЛЬНОЙ ГРУППОЙ АВТОМОРФИЗМОВ

Предлагается подход к описанию инвариантных подпространств матриц с нетривиальной группой автоморфизмов. Описан достаточно большой класс инвариантных подпространств, названных H-орбитальными. Установлена связь между инвариантным подпространством матрицы с нетривиальной группой автоморфизмов и инвариантного H-орбитального подпространства гомоморфного образа матрицы, действующего на пространстве меньшей размерности.

В [1] показано, что в классах матриц с нетривиальной группой автоморфизмов удается эффективно строить максимально рассеивающие (МР) матрицы (см., например, [2]). Однако нетривиальность группы автоморфизмов матрицы вносит дополнительную «структурированность», что может привести к наличию инвариантных смежных классов. Одноименный метод был успешно применен, например, к алгоритмам Khazad, Print, Midori64. В связи с этим актуален вопрос наличия подпространств, инвариантных относительно матриц с нетривиальной группой автоморфизмов.

Определим действие на $(\mathbb{F}_{2^r})_{n,n}$: $g=(g_1,g_2)\in S_n^2$ действует на $A=(a_{i,j})\in(\mathbb{F}_{2^r})_{n,n}$ по правилу $A^g=A^{(g_1,g_2)}=(a_{g_1(i),g_2(j)})$.

Определение 1. *Группой автоморфизмов матрицы* $A\in(\mathbb{F}_{2^r})_{n,n}$ *назовем множество* $Aut(A)=\{g\in S_n\times S_n \mid A^g=A\}$.

Для фиксированного разбиения $\{1,\ldots,n\}=\Gamma_1\cup\ldots\cup\Gamma_k$ определим векторы $e_{\Gamma_k}=\sum_{i\in\Gamma_k}e_i$, $k=1,\ldots,m$. Обозначим через $\Psi=\{\Gamma_i \mid i=1,\ldots,m\}$. Определим пространство $W_\Psi=\langle e_{\Gamma_i},\ldots,e_{\Gamma_m}\rangle$.

Определение 2. *Пусть* $H < S_n$ *и* Ψ *– разбиение на орбиты группы* H. *Тогда подпространство* $W_\Psi < (F_{2^r})^n$ *будем называть* H *– орбитальным и обозначать через* W_H.

Через $M_{n,r}(G)$, $G < S_n$, обозначим множество $n \times n$ матриц вида $M_{n,r}(G) = \{A \in (\mathbb{F}_{2^r})_{n\times n} \mid Aut(A) = \{(g,g) \mid g \in G\}\}$.

Теорема 1. *Пусть* $A \in M_{n,r}(G)$, $G < S_n$. *Тогда любое* H *-орбитальное пространство* W_H, $H < G$, *является инвариантным относительно* A.

Несложно видеть, что имеет место изоморфизм $W_\Psi \overset{\tau_\Psi}{\cong} (\mathbb{F}_{2^r})^m$, где изоморфизм векторных пространств над $\mathbb{F}_{2^r}$ задается по правилу $\tau_\Psi : \sum_{i=1}^{m} v_i e_{\Gamma_i} \mapsto \sum_{i=1}^{m} v_i e_i$. Изоморфизм τ_Ψ индуцирует гомоморфизм групп $\varphi_\Psi : GL(n,2^r)_{\{W_\Psi\}} \to GL(m,2^r)$, где $GL(n,2^r)_{\{W_\Psi\}}$ – стабилизатор множества W_Ψ в группе $GL(n,2^r)$. Если Ψ – разбиение на орбиты группы H, то будем писать φ_H. Также напомним, что любая группа $G < S_n$ изоморфно вкладывается в группу $GL(n,2^r)$ под действием изоморфизма $g \mapsto \hat{g} = (g_{i,j})$, где $g_{i,j} = 1 \Leftrightarrow g(i) = j$, $g \in G$. Изоморфный образ группы $G < S_n$ будем обозначать через $\hat{G} < GL(n,2^r)$.

Теорема 2. *Пусть* $A \in M_{n,r}(G) \cap GL(n,2^r)$, $G < S_n$ *– регулярная группа. Пусть* $H < G$, $Aut(\varphi_H(A)) = \{(t,t) \mid t \in T\}$ *и* $T < S_m$, *где* m *– число орбит группы* H. *Тогда если* $F < T$, *то* F *-орбитальному подпространству* $U_F < (\mathbb{F}_{2^r})^m$ *соответствует подпространство* $\tau_H^{-1}(U_F) < (\mathbb{F}_{2^r})^n$, *инвариантное относительно матрицы* A.

Список литературы

1. Буров Д.А., Костарев С.В. Группы автоморфизмов максимально рассеивающих матриц. 14th Workshop on Current Trends in Cryptology (CTCrypt 2025). pp. 131–156.

2. Gupta K. C., Pandey S. K., Ray G. I., Samanta S. Cryptographically significant mds matrices over finite fields: A brief survey and some generalized results. Advances in Mathematics of Communications. 2019, № 13(4), pp. 779–843.

УДК 519.7

М.В. ПОЛЯКОВ

Национальный исследовательский ядерный университет «МИФИ», Москва

ИСПОЛЬЗОВАНИЕ СКРЫТЫХ ЛИНЕЙНЫХ СООТНОШЕНИЙ ДЛЯ ПОСТРОЕНИЯ КВАНТОВЫХ РАЗЛИЧИТЕЛЕЙ ДЛЯ ШИФРОВ ФЕЙСТЕЛЯ

Работа посвящена построению квантовых различителей на некоторые шифры Фейстеля. В основе различителей лежит квантовый алгоритм поиска скрытых линейных соотношений криптографических отображений. В результате использование данного квантового оракула позволяет построить 3-раундовые различители на алгоритмы «Магма» и КБ-256.

Криптографические отображения с линейной структурой представляют особенный интерес в криптографии, так как наличие линейной структуры является уязвимостью шифрсистемы и позволяет применять атаку на основе метода гомоморфизмов. Кроме того, существование линейной структуры означает наличие разности с вероятностью 1, которую можно использовать, например, в атаке различения. Описанию линейных структур шифрсистем посвящены работы [1–3].

В [4] был представлен алгоритм нахождения скрытой линейной структуры криптографических отображений на квантовом компьютере с полиномиальной сложностью относительно числа запросов к квантовому оракулу. Алгоритм основан на задаче скрытого сдвига [5]. Квантовый алгоритм решения данной задачи часто применяется при построении квантовых различителей на алгоритмы блочного шифрования [6–8].

Введем необходимые обозначения. Пусть V_n – n-мерное векторное пространство над полем $\mathbb{F}_2$, $S(X)$ – симметрическая группа на множестве X; $\langle \alpha, \beta \rangle$ – скалярное произведение векторов $\alpha, \beta \in V_n$. Будем рассматривать функцию $f: V_n \to V_n$, заданную уравнением

$$f(x, \delta) = s(x) + s(x + \alpha) + \delta,$$

где $s \in S(V_n)$ – некоторая подстановка с линейной структурой $(\alpha, \delta) \in V_n \backslash \{0\} \times V_n \backslash \{0\}$. Данная функция скрывает подгруппу $H = \langle \alpha \rangle$. Используя алгоритм из [4], можно найти образующий элемент α за $O(n)$ выполнений квантовой схемы с экспоненциально низким уровнем ошибки.

Предложенный алгоритм можно использовать для построения различителей на шифры Фейстеля. Для этого необходимо построить

квантовый оракул, реализующий периодическую функцию f. Тогда успешное нахождение скрытого периода позволит эффективно различать шифр Фейстеля от случайной подстановки на V_{2n}.

Примеры построенных оракулов:

- для 3-раундового алгоритма «Магма»

$$f(b,x) = g_{k_2}\big(g_{k_1}(a_b) + x\big),$$

где $g_k: V_{32} \to V_{32}$ – раундовая функция;

- для алгоритма КБ-256

$$f(b,x) = b + f_1^{(3)}\big(\alpha^{(3)}, b_0^{(3)}\big) + f_2^{(1)}\big(\alpha^{(1)}, b_1^{(1)}\big) + x,$$

где $f^{(i)}: V_{32} \times V_{32} \to V_{32}$ – i-я раундовая функция.

Кроме того, показано, что для реализации найденных квантовых оракулов в виде квантовой схемы потребуется:

- 320 кубитов и 894 квантовых вентиля для алгоритма «Магма»;
- 352 кубита и 5301 квантовый вентиль для алгоритма КБ-256.

Список литературы

1. Chaum D., Evertse J. Cryptanalysis of DES with a reduce number of rounds sequences of linear factors in block ciphers // LNCS. 1985. V. 218 P. 192–211.
2. Evertse J. Linear structures in block ciphers // LNCS. 1988. V. 304. P. 249–268.
3. Б. А. Погорелов, М. А. Пудовкина, “Факторструктуры преобразований”, Матем. вопр. криптогр., 3:3 (2012), 81–104.
4. М. В. Поляков, М. А. Пудовкина, “Поиск скрытой линейной структуры отображения на квантовом компьютере”, *ПДМ. Приложение*, 2025, № 18, 276–279.
5. Simon D. On the power of quantum computations // Proc. SFCS’94. Santa Fe, NM, USA, 1994. P. 116–123.
6. Kaplan M., Leurent G., Leverrier A., Naya-Plasencia M. Breaking symmetric cryptosystems using quantum period finding. In: Robshaw M., Katz J., eds. Advances in Cryptology - CRYPTO 2016. Lecture Notes in Computer Science, Vol 9815. Berlin: Springer-Verlag, 2016. 207–237.
7. Kuwakado H., Morii M. Quantum distinguisher between the 3-round feistel cipher and the random permutation. In: International symposium on information theory, ISIT 2010. IEEE, 2010. 2682–2685.
8. Dong X., Li Z., Wang X. Quantum cryptanalysis on some generalized Feistel schemes. Science China Information Sciences, 2018, 62(2): 22501.

УДК 519.7

П.А. ПОЛЯКОВА, М.В. ПОЛЯКОВ

Национальный исследовательский ядерный университет «МИФИ», Москва

ОЦЕНКА СТОЙКОСТИ ПРОТОКОЛОВ SIGNCRYPTION В МОДЕЛИ Q2

Работа посвящена оценке стойкости протоколов одновременного шифрования и подписи Signcryption в модели Q2. Данная модель подразумевает наличие у атакующего доступа к квантовому оракулу, реализующему исследуемый криптографический примитив и принимающему на вход запросы в виде суперпозиции входов. Рассматривается модифицированный протокол Signcryption, в котором подпись вычисляется на коммутативных изогениях суперсингулярных эллиптических кривых. Показывается, что для реализации алгоритма Signcryption в виде квантовой схемы потребуется порядка 2^{40} квантовых вентилей и порядка 10^6 кубитов.

В 1997 г. была предложена идея одновременного шифрования и подписи передаваемых сообщений – Signcryption [1]. Основной целью такого механизма было одновременное обеспечение невозможности подделки подписи и нарушения конфиденциальности. Кроме того, по заявлениям авторов, внедрение подобных механизмов сокращает трудоемкость реализуемых преобразований и информационных взаимодействий по сравнению с механизмами Signature-then-encryption. В настоящее время такие схемы можно встретить, например, в мессенджерах [2].

Предлагается рассматривать модифицированный протокол Signcryption, в котором формирование и проверка электронной подписи сообщения выполняются на основе коммутативных изогений суперсингулярных эллиптических кривых (CSI-FiSh [3]):

1. $\mathrm{KeyGen}(1^{\lambda})$ – при заданном уровне стойкости λ возвращает ключевую пару для формирования и проверки подписи;
2. $\mathrm{Sign}(sk, m)$ – вычисляет подпись σ сообщения m на ключе sk алгоритмом CSI-FiSh;
3. $\mathrm{Verify}(pk, \sigma, m)$ – проверяет подпись σ сообщения m с помощью ключа pk алгоритмом CSI-FiSh;
4. $\mathrm{Signcryption}(m, K, sk)$ – алгоритм формирования шифртекста c и подписи σ сообщения m. K – ключ шифрования данных, sk – ключ вычисления подписи;

5. $\mathrm{Unsigncryption}(c, K, pk)$ – алгоритм расшифрования шифртекста c и проверки подписи σ сообщения m. K – ключ шифрования данных, pk – ключ проверки подписи.

Согласно [4], модель стойкости Q2 подразумевает, что у атакующего есть доступ к квантовому оракулу, реализующему все необходимые криптографические преобразования.

Для оценки постквантовой стойкости такого модифицированного протокола требуется реализовать квантовый оракул, в свою очередь реализующий алгоритм $\mathrm{Signcryption}(*,*,*)$. В работах [5, 6, 7] проводились аналогичные исследования для протокола CSIDH-512. Используя подходы из данных статей, можно получить следующие параметры сложности квантовой схемы:

- количество используемых кубитов – порядка 10^6;
- количество T-вентилей, необходимых для реализации умножения – 6.270.628;
- количество T-вентилей, необходимых для вычисления полного группового действия – 0.7×2^{40}.

Список литературы

1. Zheng Y. Digital Signcryption or How to Achieve Cost (Signature & Encryption) ≪ Cost (Signature) + Cost (Encryption) // Advances in Cryptology. – CRYPTO'97. Lecture Notes in Computer Science. – 1997. – № 1294. – С. 165–179.

2. Bellare M., Stepanovs I. Security Under Message-Derived Keys: Signcryption in iMessage // Advances in Cryptology – EUROCRYPT'20. Lecture Notes in Computer Science. – 2020. – № 12107. – С. 507–537.

3. Beullens W., Kleinjung T., Vercauteren F. CSI-FiSh: Efficient Isogeny based Signatures through Class Group Computations // Advances in Cryptology. — ASIACRYPT'19. Lecture Notes in Computer Science. – 2019. – № 11921. – С. 227–247.

4. Kaplan M., Leurent G., Leverrier A., Naya-Plasencia M. Quantum differential and linear cryptanalysis. – IACR Trans. Symm. Cryptol. – 2016. – № 1. – С. 71–94.

5. Bonnetain X., Schrottenloher A. Quantum security analysis of CSIDH and ordinary isogeny-based schemes. – IACR Cryptology ePrint Archive. –2018. – № 537.

6. Bonnetain X., Schrottenloher A. Quantum Security Analysis of CSIDH. // Advances in Cryptology – EUROCRYPT'20. Lecture Notes in Computer Science. – 2020. – № 12106. – С. 493–522.

7. Bernstein D.J., Lange T., Martindale C., Panny L. Quantum Circuits for the CSIDH: Optimizing Quantum Evaluation of Isogenies. // Advances in Cryptology – EUROCRYPT'19. Lecture Notes in Computer Science. – 2019. – № 11477. С. 409–441.

УДК 519.7

М.А. ПУДОВКИНА, А.М. СМИРНОВ

Национальный исследовательский ядерный университет «МИФИ», Москва

АТАКА РАЗЛИЧЕНИЯ НА КЛАСС АЛГОРИТМОВ БЛОЧНОГО ШИФРОВАНИЯ НА ОСНОВЕ ПРЕОБРАЗОВАНИЯ ФЕЙСТЕЛЯ

В работе рассматривается класс алгоритмов блочного шифрования на основе преобразования Фейстеля с XSL – функцией усложнения, у которых линейное преобразование задается подстановочной матрицей. Предложена атака различения, основанная на сохранение разности у композиции преобразований раундовой функции при применении перестановки фиксированных координат пары текстов. Получены оценки трудоемкости атаки и вероятность её успеха.

Рассмотрим класс алгоритмов блочного шифрования на основе преобразования Фейстеля, у которых линейное преобразование функции усложнения задается подстановочной матрицей.

Пусть $n, m \in \mathbb{N}$, $V_d(2^m)$ – d-мерное векторное пространство над полем $\mathbb{F}_{2^m}$, $d \in \mathbb{N}$; $\mathrm{I}(A)$ − индикатор выполнения условия A. Будем обозначать через h линейное преобразование функции усложнения и соответствующую ему подстановочную $(n \times n)$-матрицу в стандартном базисе над полем $\mathbb{F}_{2^m}$, $h = [\![h_{i,j}]\!]$.

Отображение $t: V_{2n}(2^m) \to V_n(2^m)$, подстановка $s = (s_1, \dots, s_n) \in S(\mathbb{F}_{2^m})^n$ и «дополненная» функцию усложнения $f_k: V_{2n}(2^m) \to V_{2n}(2^m)$ на раундовом ключе $k \in V_n(2^m)$ для каждого $\alpha = (\alpha_1, \dots, \alpha_{2n}) \in V_{2n}(2^m)$ задаются соответственно условиями

$$t: (\alpha_1, \dots, \alpha_{2n}) \longmapsto (\alpha_1, \dots, \alpha_n),$$
$$s: (\alpha_1, \dots, \alpha_n) \longmapsto (s_1(\alpha_1), \dots, s_n(\alpha_n)),$$
$$f_k: (\alpha_1, \dots, \alpha_{2n}) \longmapsto (hs(t(\alpha) \oplus k), \alpha_{n+1}, \dots, \alpha_{2n}).$$

Введем также линейные отображения $h_i: V_{2n}(2^m) \to V_{2n}(2^m)$, $i = 1,2$, заданные для каждого $\alpha = (\alpha_1, \dots, \alpha_{2n}) \in V_{2n}(2^m)$ условиями

$$h_1: (\alpha_1, \dots, \alpha_{2n}) \longmapsto (\alpha_{n+1}, \dots, \alpha_{2n}, \alpha_1, \dots, \alpha_n),$$
$$h_2: (\alpha_1, \dots, \alpha_{2n}) \longmapsto (\alpha_1, \dots, \alpha_n, \alpha_1 \oplus \alpha_{n+1}, \dots, \alpha_n \oplus \alpha_{2n}).$$

Пусть $g_k: V_{2n}(2^m) \to V_{2n}(2^m)$ − раундовая функция преобразования Фейстеля с «дополненной» функцией усложнения f_k на ключе $k \in V_n(2^m)$.

Лемма 1. *Для каждого* $k \in V_n(2^m)$ *справедливо равенство*

$$g_k = f_k^{-1} h_2 f_k h_1. \quad (1)$$

Равенство (1), связывающее раундовую функцию g_k и «дополненную» функцию усложнения f_k на ключе $k \in V_n(2^m)$, будет использовано при доказательстве теоремы 1, а тем самым и для построения атаки.

Для всех $\theta=(\theta_1, \dots, \theta_{2n}) \in V_{2n}(2)$, $\alpha^{(j)}=\left(\alpha_1^{(j)}, \dots, \alpha_{2n}^{(j)}\right) \in V_{2n}(2^m)$, $j = 1,2$ зададим отображение $\rho_\theta^{(i)}: V_{2n}(2^m)^2 \to \mathbb{F}_{2^m}$ условием

$$\rho_\theta^{(i)}\left(\alpha^{(1)}, \alpha^{(2)}\right)=\alpha_i^{(1)}\mathrm{I}(\theta_i = 0)+\alpha_i^{(2)}\mathrm{I}(\theta_i = 1) \text{ при } i = 1, \dots, 2n,$$

и положим

$$\rho_\theta\left(\alpha^{(1)}, \alpha^{(2)}\right)=\left(\rho_\theta^{(1)}\left(\alpha^{(1)}, \alpha^{(2)}\right), \dots, \rho_\theta^{(n)}\left(\alpha^{(1)}, \alpha^{(2)}\right)\right).$$

Из [1] вытекает равенство

$$s\left(\alpha^{(1)}\right) \oplus s\left(\alpha^{(2)}\right)=\rho_\theta\left(s(\alpha^{(1)}), s(\alpha^{(2)})\right) \oplus \rho_\theta\left(s(\alpha^{(2)}), s(\alpha^{(1)})\right)$$

для всех $\alpha^{(1)}, \alpha^{(2)} \in V_{2n}(2^m)$.

Подстановочной матрице h соответствует перестановка $\tau \in S(\{1, \dots, n\})$ координат n-мерного вектора из $V_n(2^m)$.

Теорема 1. *Пусть* $l \in \mathbb{N}$, $(k_1, \dots, k_l) \in V_n(2^m)^l$,

$$\tilde{g}_{k_1,\dots,k_l} = g_{k_l} g_{k_{l-1}} \cdots g_{k_1},$$

а τ *при разложении на независимые циклы содержит транспозицию* (r, d). *Тогда для каждой пары* $\left(\alpha^{(1)}, \alpha^{(2)}\right) \in V_n(2^m)^2$ *справедливо равенство*

$$\tilde{g}_{k_1,\dots,k_l}\left(\alpha^{(1)}\right) \oplus \tilde{g}_{k_1,\dots,k_l}\left(\alpha^{(2)}\right)=$$
$$= \tilde{g}_{k_1,\dots,k_l}\left(\rho_\theta\left(\alpha^{(1)}, \alpha^{(2)}\right)\right) \oplus \tilde{g}_{k_1,\dots,k_l}\left(\rho_\theta\left(\alpha^{(2)}, \alpha^{(1)}\right)\right),$$

где $\theta=(\theta_1, \dots, \theta_n)$,

$$\theta_i = \mathrm{I}\left(h_{i-n,d}=1, i>n \text{ или } i=d\right) \text{ при } d < n+1.$$

На основании теоремы 1 предложена атака различения, целью которой является проверка гипотезы, что подстановка $\tilde{g}_{k_1,\dots,k_l}$ не является случайной. Доказано, что трудоемкость атаки составляет 4 операции зашифрования, а вероятность успеха атаки равна 1.

Список литературы

1. Ronjom S., Bardeh N. G., and Helleseth T.Yoyo tricks with AES // ASIACRYPT 2017. Lect. Notes Comput. Sci. 2017. V. 10624. No. 1. P. 217 – 243.

УДК 519.7

К.В. АНТОНОВ[1], А.Р. БЕЛОВ[2], Д.А. ЗАХАРОВ[1], А.В. ЖАРКОВА[3], О.В. КАМЛОВСКИЙ[4], Д.М. КРАПИВЕНЦЕВ[1], А.А. КОЗЛОВ[1], П.Г. КЛЮЧАРЕВ[5], В.Н. КНЯЗЕВ[2], Д.М. МУРИН[2], М.В. ПОЛЯКОВ[1], М.А. ПУДОВКИНА[1], А.М. СМИРНОВ[1], А.В. ТКАЧУК[6], С.С. ТИТОВ[7]

[1]*Национальный исследовательский ядерный университет «МИФИ», Москва*

[2]*Ярославский государственный университет им. П.Г. Демидова*

[3]*Саратовский государственный университет им. Н.Г. Чернышевского*

[4]*Российский технологический университет МИРЭА, Москва*

[5]*Московский государственный технический университет им. Н.Э. Баумана*

[6]*ФГУП "НПП "Гамма", Москва*

[7]*Уральский государственный университет путей сообщения, Екатеринбург*

О ВСЕРОССИЙСКОЙ СТУДЕНЧЕСКОЙ ОЛИМПИАДЕ ПО КРИПТОГРАФИИ И КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ «CRYPTOFOX»

С 2023 г. кафедра криптографии и безопасности компьютерных систем НИЯУ МИФИ проводит студенческую олимпиаду по криптографии и компьютерной безопасности «CryptoFox». Задачи олимпиады связаны с теоретической криптографией, практической криптографией и компьютерной безопасностью. Спецификой олимпиады является наличие нерешенных, а также исследовательских задач. В работе проводится обзор задач олимпиады «CryptoFox» и обсуждаются ее особенностей.

С 2023 г. кафедра криптографии и безопасности компьютерных систем (№ 41) НИЯУ МИФИ проводит студенческую олимпиаду по криптографии и компьютерной безопасности «CryptoFox» с целью популяризации криптографии в России и развитие интереса у начинающих специалистов к разнообразным интересным проблемам, которые возникают в современной теоретической и практической криптографии: от классических ее направлений до появляющихся новых и перспективных, включая постквантовую криптографию. Задачи олимпиады условно делятся на две категории: 1) теоретическая криптография; 2) практическая криптография и компьютерная безопасность. Разнообразные задачи олимпиады возникают при синтезе и анализе криптосистем, а также берутся из современных научно-исследовательских работ, представленных на ведущих криптографических

конференциях. Такие задачи находятся в категории «Теоретическая криптография». Однако на практике специалистам по компьютерной безопасности приходится сталкиваться с необходимостью выполнять реверс-инжиниринг, тестировать корректность реализации криптосистемы по ее программному коду, выявлять закладки в программной реализации, проводить статистический анализ данных, обнаруживать уязвимости и предлагать защиту от них, разрабатывать способы дешифрования сообщений и т.д. Подобные задачи, а также характерные для CTF-соревнований задания относятся к категории «Практическая криптография и компьютерная безопасность». Спецификой олимпиады является наличие исследовательских, а также нерешенных задач.

В 2025 г. к организации олимпиады присоединились кафедры «Информационная безопасность» (ИУ8) МГТУ им Н.Э. Баумана, «Компьютерная безопасность и математические методы обработки информации» ЯрГУ им. П.Г. Демидова. На олимпиаду зарегистрировалось более 250 студентов из различных ведущих вузов от Москвы до Владивостока. Победители и призеры (20 студентов) из НИЯУ МИФИ, ИТМО, МГТУ им. Н.Э. Баумана, ЯрГУ им. П.Г. Демидова, СГУ им Н.Г. Чернышевского, УрГУПС.

Начнем с рассмотрения задач 2023 г. Участникам предлагалась задача, посвященная анализу XSL-алгоритма блочного шифрования в режиме гаммирования, в которой для решения необходимо было заметить наличие линейных соотношений в S-блоке. В задаче «Новая операция сложения с ключом» требовалось описать вероятностные свойства новой бинарной операции Impulsive OR сложения с ключом. В 2024 г. Олимпиада была посвящена 35-летию первого отечественного стандарта шифрования ГОСТ 28147-89. В рамках этого предложена задача, посвященная анализу его модификации GOST-CryptoFox 2024 на основе метода связанных ключей. Идеи задачи взята из [1]. В 2025 г**.** олимпиада была посвящена 130-летию нобелевского лауреата, академика АН СССР, д.ф.-м.н. И.Е. Тамма. В рамках этого предложена исследовательская задача «Странная вселенная», в которой рассматривается вселенная с нелинейным квантовым преобразованием h, а проблема заключается в анализе влияния нелинейности h на стойкость протокола BB84 в этой вселенной.

Список литературы

1. Ko Y., Hong S., Lee W., Lee S., Kang J. S. Related Key Differential Attacks on 27 Rounds of XTEA and Full-Round GOST // FSE 2004. − 2004. – pp. 299–316.

УДК 519.7

Д.А. БИТУС

Научно-производственное предприятие «Гамма», Москва

КОМБИНИРОВАННАЯ АТАКА НА 24 ТАКТА «МАГМЫ»

В данной работе рассматривается применение атаки на 8 тактов «Магмы» методом усечённого дифференциала и сдвиговой атаки на 24 такта «Магмы».

В [1] была предложена комбинированная атака на 24 такта «Магмы», в настоящей работе представлены реализация, уточнение статистик и методы оптимизации данной атаки. Комбинированная атака состоит из двух этапов: на первом происходит сведение сдвиговой атакой полной (почти полной) кодовой книги 24 тактов «Магмы» к небольшой части кодовой книги 8 тактов «Магмы», на втором – извлечение ключа методом усечённого дифференциала.

Рассмотрим атаку методом усечённого дифференциала. В [1] представлен дифференциальный путь и вероятности его переходов. Данный путь реализуем и верен с тем лишь исключением, что вероятность его реализации в операции «сумма с тактовым ключом» будет выше и зависит от тактового ключа. На практике эта вероятность находится в пределах 2^{-9}–2^{-11}, в [1] указано значение $2^{-11{,}5}$, то есть релевантная нижняя граница данной вероятности. Для оптимизации данного этапа атаки можно предложить перебор тактового ключа не целиком, а блоками по 4 бита, с последующим их объединением с учётом возможного бита переноса. Также стоит отметить, что предложенная атака позволяет получить небольшое множество ключей (приблизительно 60), для каждого из которых надо провести атаку на меньшее количество тактов. В настоящей работе атакой на меньшее количество тактов является этот же дифференциальный путь с урезанными первыми тактами. В результате её применения извлечение ключа на реальном вычислителе (ПК с процессором AMD Ryzen 7 5800H) возможно в пределах 5 минут.

Рассмотрим атаку методом сдвига. Представим реализацию 24-тактовой «Магмы» как троекратную реализацию случайной подстановки. В этом случае необходимо решить задачу дискретного логарифмирования на группе подстановок. В [1] берутся циклы длины n не кратной 3, а восстановление изначальной подстановку (8 тактов «Магмы») возможно при помощи алгоритма Евклида путём применения троекратной подстановки ещё некоторое количество раз. Евклида даст

верный ответ только в случае $НОД(n, 3) = 1$. Рассмотрим случайный цикл длины $n > 2^{41}$: $НОД(n, 3) = 3$. В таком случае после троекратного применения подстановки, исходный цикл разобьётся на три цикла. Подводя итоги, для случайного цикла случайной подстановки верно: изначальный цикл восстановим с вероятностью 2/3; изначальный цикл невосстановим, но это неизвестно до применения алгоритма с вероятностью 2/9; изначальный цикл невосстановим, это известно до применения алгоритма с вероятностью 1/9.

В настоящей работе предлагается подход к восстановлению изначального цикла при условии его разбиения на 3 цикла путём их скрепления. Стоит отметить, что при отсутствии дополнительной информации все предполагаемые начальные циклы неотличимы, однако дополнительной информацией является дифференциальный путь. Подход состоит из следующих шагов: 1) найти 3 цикла одинаковой длины, в которые предположительно разделился изначальный цикл; 2) для одного из циклов найти и сохранить в структуру все пары его элементов, удовлетворяющие входной разности дифференциального пути; 3) для двух других циклов проверить выходную разность дифференциального пути на сохранённой структуре для каждого сдвига данных циклов; 4) случай, в котором реализовалась выходная разность максимальное количество раз, есть нужное скрепление циклов. Конец алгоритма. При недостаточности полученной выборки необходимо применить алгоритм для одного из двух оставшихся переходов, иначе на полученной выборке реализовать атаку на 8 тактов «Магмы». В итоге, в статье [1] атака требовала не более 2^{64} операций, но с вероятностью около 2^{-40} не могла свести 24 такта к 8. Предложенный в настоящей работе алгоритм в данном неблагоприятном случае требует не более 2^{80} операций, но вероятность нахождения истинного ключа близится к 1. Единственный вариант, при котором данный алгоритм не сможет свести 24 такта «Магмы» к 8 это случай, когда все циклы 8 тактов «Магмы» не превышают 2^{40}.

В настоящей работе была проверена на практике атака, предложенная в [1], были уточнены некоторые статистики и предложены оптимизации и модификации данной атаки для её ускорения и увеличения вероятности успеха.

Список литературы

1. A. Bar-On, E. Biham, O. Dunkelman and N. Keller. Efficient Slide Attacks. Journal of Cryptology, 2018, с. 641−670.

УДК 519.7

А.В. ГОДОВ, К.В. АНТОНОВ

Национальный исследовательский ядерный университет «МИФИ», Москва

ОБ АЛГЕБРАИЧЕСКОМ КРИПТОАНАЛИЗЕ TRIVIUM-ПОДОБНЫХ АЛГОРИТМОВ ПОТОЧНОГО ШИФРОВАНИЯ

Задача восстановления секретного ключа алгоритма поточного шифрования может быть эффективно сведена к задаче смешанного целочисленного линейного программирования (ЦЛП). В работе предлагается комбинация методов ЦЛП и атак из класса «угадывай и определяй», а именно техники вероятностных лазеек. При помощи указанного подхода производится оценка стойкости Trivium-подобных алгоритмов поточного шифрования в сценарии атаки по подобранным значениям векторов инициализации.

Одной из NP-трудных задач является задача смешанного целочисленного линейного программирования (ЦЛП) – задача оптимизации вещественнозначной линейной функции при условии целочисленности некоторых её аргументов и выполнимости ряда линейных ограничений. Для решения ЦЛП существует множество программных средств (решателей), таких как Gurobi [1], CPLEX [2], SCIP [3].

Описываемые в работе атаки на основе решателей задачи ЦЛП принадлежат к классу «угадывай и определяй». Конкретно, к подходу на основе ЦЛП адаптированы атаки IBS [4], которые используют понятие вероятностных лазеек. Говоря неформально, вероятностной лазейкой в алгебраической задаче называется набор переменных, подстановка значений которых упрощает задачу так, что её можно эффективно решить с ненулевой вероятностью. В работе впервые предлагается применить комбинированный подход в криптоанализе: атаки на основе вероятностных лазеек с применением методов ЦЛП.

Объектом криптоанализа являются Trivium-подобные алгоритмы поточного шифрования, редуцированные по числу шагов инициализации: Trivium [5] и Bivium-A [6]. Схема Trivium построена на основе регистров сдвига, зашифрование происходит путём наложения на открытый текст гаммы, получаемой из секретного ключа и несекретного вектора инициализации. Рассматриваем несколько сценариев атаки:

1) восстановление неизвестного состояния регистров, гамма считается известной;

2) восстановление ключа по известному фрагменту гаммы, значение вектора инициализации известно, но выбирается случайно равновероятно;

3) восстановление ключа по подобранным значениям векторов инициализации: у криптоаналитика имеется возможность получить фрагменты гаммы для искомого секретного ключа и любых выбранных значений векторов инициализации.

В экспериментах использовался решатель SCIP [3]. Поиск оптимальной по трудоёмкости атаки проводился при помощи модифицированного алгоритма 1+1 на вычислительном кластере МИФИ [7]. Для Bivium-A были построены атаки на полную версию алгоритма (708 шагов), у Trivium же в спецификации 1152 шага, и атаки построены на редуцированные версии. Трудоёмкости построенных атак приведены в табл. 1 и 2.

Таблица 1. Трудоёмкость атак на Bivium-A

Сценарий атаки	Вероятность успеха атаки	Трудоёмкость атаки, с.
2	0,05	2^{74}
1	0,57	2^{8}
1	1	2^{29}

Таблица 2. Трудоёмкость атак на Trivium

Сценарий атаки	Число шагов инициализации	Вероятность успеха атаки	Трудоёмкость атаки, с.
1	64	1	2^{74}
1	80	1	2^{77}
1	96	1	2^{80}
3	128	1	2^{74}

Список литературы

1. Gurobi Optimizer. Режим доступа: https://www.gurobi.com/documentation/
2. IBM ILOG CPLEX. https://www.ibm.com/products/ilog-cplex-optimization-studio/
3. SCIP. https://www.scipopt.org/
4. Семёнов А.А. Атаки из класса «угадывай и определяй» и автоматические способы их построения. Прикладная дискретная математика, 2018, с. 81–86.
5. De Cannière C., Preneel B. TRIVIUM Specifications, 2005.
6. Borghoff J., Knudsen L.R., Stolpe M. Bivium as a Mixed-Integer Linear Programming Problem. Cryptography and Coding, 2009, p. 135–152.
7. Вычислительный кластер НИЯУ МИФИ. https://it.mephi.ru/hpc/

УДК 519.7

Д.А. ЗАХАРОВ[1], А.Б. ЧУХНО[2]

[1]Национальный исследовательский ядерный университет «МИФИ», Москва
[2]Московский институт электроники и математики им. А.Н. Тихонова НИУ ВШЭ

О ПРАКТИЧЕСКОЙ ТРУДОЕМКОСТИ АТАКИ НА РЕЖИМ ПОЛНОДИСКОВОГО ШИФРОВАНИЯ XEH

В 2022 г. в качестве более стойкой модификации режима XTS и одновременно имеющий лучшие эксплуатационные характеристики, чем режим DEC, был предложен режим работы алгоритмов блочного шифрования XEH. В 2025 г. был предложен метод сведения режима полнодискового шифрования XEH к режиму простой замены используемого алгоритма блочного шифрования за время $\mathcal{O}((n+1)\cdot 2^l)$. В данной работе показана применимость и уточнены характеристики метода на практике.

Режим XEH [1, 2] является более стойким в модели доказуемой стойкости, чем XTS [3] и лишен недостатка DEC [4], требующего хранения значительных объемов вспомогательной информации, но для него был предложен метод сведения к режиму простой замены.

В [5] были предложены два алгоритма по восстановлению секретных параметров τ_3 и τ_1, τ_2 режима XEH. Алгоритмы выполняются последовательно и трудоемкость восстановления всех трех параметров оценена как $O\big((n+1)2^l\big)$ операций умножения в $\mathbb{F}$ ($l-$длина блока шифра, а $n-$ число блоков в секторе). Указанная трудоемкость получена, в том числе, исходя из оценки вероятности успеха алгоритмов. Оценка для первого алгоритма получена с помощью метода Чернова, а для второго теоретически показано, что вероятность его успеха близка к 1. Представляет интерес верифицировать оценки вероятностей успеха на практике.

Моделирование работы алгоритмов проведено с использованием реализации режима XEH от авторов [1, 2] и редуцированного алгоритма шифрования Speck 16/32. От оригинального Speck 32/64 [6] он отличается только длиной блока текста и ключа. Выбор алгоритма обусловлен наличием версии с длиной блока 32 бита и простотой в программной реализации.

Для 500 случайных (величина имеет равномерное распределение на множестве 32-разрядных целых чисел) значений секретных ключей и номеров секторов произведено восстановление секретных параметров режима XEH. В каждом из случаев были найдены истинные значения τ_1, τ_2, τ_3. В табл. 1 приведены данные о числе кандидатов для значений

параметров (оно определяет вероятность восстановления истинного значения параметра и влияет на трудоемкость атаки).

Таблица 1. Число кандидатов для истинных значений τ_1, τ_2, τ_3

Число кандидатов	Значения τ_3	Вероятность числа кандидатов	Значений τ_1, τ_2	Вероятность числа кандидатов
1	193	0,386	186	0,372
2	178	0,356	189	0,378
3	89	0,178	86	0,172
4	33	0,066	28	0,056
5	5	0,01	11	0,022
6	1	0,002	0	0
7	1	0,002	0	0

Заметим, что для значения τ_3 найденные вероятности на много порядков отличаются от оценок из работы [5] (вероятности для числа кандидатов 6 и 7 $\sim 10^{-13}$ и 10^{-20} соответственно). Предположение о равенстве вероятности неуспеха вероятности случайного совпадения для τ_1, τ_2 в 2^{-l} также не подтверждается на практике.

Список литературы

1. Фирсов Г.В., Коренева А.М. Об одном режиме работы блочных шифров, используемом для защиты информации на носителях с блочно-ориентированной структурой // Современные информационные технологии и ИТ-образование. – 2022. – Т. 18. – №. 3. – С. 691–701.

2. Firsov G. and Koreneva A. On improved security bounds of one block ciphers mode of operation for protection of block-oriented system storage devices // J. Comput. Virol. Hack. Tech. 2024. V. 20. No. 3. P. 513–23.

3. Рекомендации по стандартизации Р 1323565.1.042-2022 «Информационная технология. Криптографическая защита информации. Режим работы блочных шифров, предназначенный для защиты носителей информации с блочно-ориентированной структурой». М.:Стандартинформ, 2022.

4. M Dworkin M. J. Recommendation for Block Cipher Modes of Operation: the XTS-AES Mode for Confidentiality on Storage Devices. – National Institute of Standards and Technology, 2010. – №. NIST Special Publication (SP) 800-38E.

5. Захаров Д.А., Чухно А.Б. О возможности сведения режима дискового шифрования XEH к режиму простой замены с использованием атаки на основе подобранных открытых сообщений //Прикладная дискретная математика. Приложение. – 2025. – №. 18. – С. 129–133.

6. Beaulieu R. et al. The SIMON and SPECK lightweight block ciphers //Proceedings of the 52nd annual design automation conference. – 2015. – P. 1 – 6.

УДК 519.7

А.О. МАКАРОВ

Национальный исследовательский ядерный университет «МИФИ», Москва

СХЕМА ПОСЛЕДОВАТЕЛЬНОЙ АГРЕГИРОВАННОЙ ЭЛЕКТРОННОЙ ПОДПИСИ С ЛЕНИВОЙ ПРОВЕРКОЙ НА ОСНОВЕ ТЕОРИИ АЛГЕБРАИЧЕСКОГО КОДИРОВАНИЯ

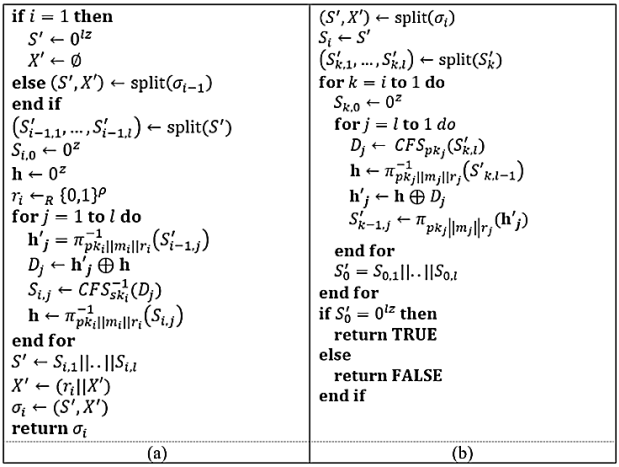
В работе представлена новая схема последовательной агрегированной электронной подписи с ленивой проверкой LARCFS: приводится её формальное описание, а также оценка теоретической стойкости в сведении к стойкости схемы электронной подписи CFS на основе кодов Гоппы.

Схемы последовательной агрегированной электронной подписи позволяют группе независимых подписантов сформировать единую подпись для множества сообщений, размеры которой меньше суммарного размера индивидуальных подписей. Свойство ленивой проверки схем последовательной агрегированной подписи позволяют не проверять текущую агрегированную подпись при формировании следующей, что увеличивает производительность процедуры формирования подписи.

Представим формальное описание схемы LARCFS. *Генерация ключей*. Параметры схемы – натуральные числа m, t, $n = 2^m$, δ, l, ρ, причем $\binom{n}{t+\delta} > 2^{mt}$, криптографические хэш-функции h_i, $i = 1, \dots, l$; двоичный код Гоппы $\Gamma(g, S)$, заданный многочленом $g \in \mathbb{F}_n$ степени t с определяющим множеством S. Пусть H систематическая $mt \times n$ матрица проверки кода $\Gamma(G, s)$. $pk = H$ является открытым ключом, (g, S, D_Γ) образует закрытый ключ, где D_Γ – алгоритм декодирования синдрома кода Γ. $\pi: K \times \{0,1\}^k \to \{0,1\}^k$ – идеальный шифр, где K – множество ключей идеального шифра.

Агрегированная подпись. Пусть m_i – сообщение, подписанное пользователем u_i. $pk = \{pk_1, \dots, pk_n\}$ – открытые ключи пользователей, σ_{i-1} — предыдущее значение агрегированной подписи. Для пользователя u_i процедура формирования подписи представлена на рис. 1 (a).

Агрегированная проверка. Пусть m_i – сообщение, подписанное пользователем $u_i \in U$. $pk = \{pk_1, \dots, pk_i\}$ – открытые ключи пользователей U, σ_i – агрегированная подпись, созданная пользователями для сообщений $\{m_j | \, 1 \le j \le i\}$. Подпись σ_i представляется в виде $\sigma = (S', X')$, где $X' = (r_i, || \dots || r_1)$, $|S'| = z$ бит, $|r_j| = \rho$ бит, $j \in \{1, \dots, i\}$. Дальнейший алгоритм вычисления представлен на рис. 1 (b).



if $i = 1$ **then**
  $S' \leftarrow 0^{lz}$
  $X' \leftarrow \emptyset$
else $(S', X') \leftarrow \text{split}(\sigma_{i-1})$
end if
$(S'_{i-1,1}, \dots, S'_{i-1,l}) \leftarrow \text{split}(S')$
$S_{i,0} \leftarrow 0^z$
$\mathbf{h} \leftarrow 0^z$
$r_i \leftarrow_R \{0,1\}^\rho$
for $j = 1$ **to** l **do**
  $\mathbf{h}'_j = \pi^{-1}_{pk_i||m_i||r_i}(S'_{i-1,j})$
  $D_j \leftarrow \mathbf{h}'_j \oplus \mathbf{h}$
  $S_{i,j} \leftarrow CFS^{-1}_{sk_i}(D_j)$
  $\mathbf{h} \leftarrow \pi^{-1}_{pk_i||m_i||r_i}(S_{i,j})$
end for
$S' \leftarrow S_{i,1}||\dots||S_{i,l}$
$X' \leftarrow (r_i||X')$
$\sigma_i \leftarrow (S', X')$
return σ_i

(a)

$(S', X') \leftarrow \text{split}(\sigma_i)$
$S_i \leftarrow S'$
$(S'_{k,1}, \dots, S'_{k,l}) \leftarrow \text{split}(S'_k)$
for $k = i$ **to** 1 **do**
  $S_{k,0} \leftarrow 0^z$
  for $j = l$ **to** 1 *do*
    $D_j \leftarrow CFS_{pk_j}(S'_{k,l})$
    $\mathbf{h} \leftarrow \pi^{-1}_{pk_j||m_j||r_j}(S'_{k,l-1})$
    $\mathbf{h}'_j \leftarrow \mathbf{h} \oplus D_j$
    $S'_{k-1,j} \leftarrow \pi_{pk_j||m_j||r_j}(\mathbf{h}'_j)$
  end for
  $S'_0 = S_{0,1}||\dots||S_{0,l}$
end for
if $S'_0 = 0^{lz}$ **then**
  return TRUE
else
  return FALSE
end if

(b)

Рис. 1. Алгоритм формирования (a) и проверки (b) агрегированной электронной подписи, где $CFS^{-1}_{sk_i}$ — вычисление подписи схемы CFS

Теоретическая стойкость схемы LARCFS может быть показана в игровой модели Белларе-Рогавея, аналогично доказанному для схемы LMQSAS [1]. Пусть функция проверки подписи схемы CFS [2] с использованием кодов Гоппы – (t', ϵ')-стойкая односторонняя функция с секретом. Тогда схема последовательной агрегированной электронной подписи LARCFS является $(t, q_H, q_\pi, z, \epsilon)$-стойкой для всех эффективных противников с временем работы не более t и преимуществом ϵ, делающих не более q_H запросов к случайному оракулу, не более q_π запросов к оракулу идеального шифра, для всех t', ϵ', z, где z – размер агрегируемой части агрегированной подписи, $m, t, l \in \mathbb{N}$ – параметры схемы:

$$\epsilon \leq \frac{q_H 2^{z+\rho}}{(2^z - q_\pi^2)(2^\rho - q_H^2)}\epsilon' + q_\pi^2/2^z,$$
$$t = t'/l.$$

Список литературы

1. Макаров А.О. Схема Постквантовой агрегированной подписи с ленивой проверкой на основе многомерных квадратичных многочленов//Безопасность Информационных Технологий, 2023, Т. 30, N 3, С. 30–50.

2. Courtois N.T., Finiasz M., Sendrier N. How to Achieve a McEliece-Based Digital Signature Scheme//Advances in Cryptology — ASIACRYPT 2001/ ed. C. Boyd. – Berlin, Heidelberg: Springer, 2001. – P. 157–174.

УДК 519.7

Д.А. КОЛЕСОВ

Национальный исследовательский ядерный университет «МИФИ», Москва

ОПТИМИЗАЦИЯ РЕАЛИЗАЦИИ БЛОЧНОЙ ШИФРСИСТЕМЫ SPARX НА ПРОЦЕССОРАХ РАЗЛИЧНЫХ АРХИТЕКТУР

Целью работы является разработка высокоэффективных реализаций блочных шифров SPARX-64/128, SPARX-128/128 и SPARX-128/256 для процессорных архитектур x86-64, ARM и RISC-V. Проведено исследование структуры алгоритма и существующих оптимизированных реализаций, реализованы оригинальные подходы к параллельной обработке и построено алгебраическое описание алгоритма развертывания ключа. Особое внимание было уделено низкоуровневой оптимизации – как на языке C, так и на ассемблере NASM, что позволило достичь максимальной производительности в реальных условиях исполнения. В результате получены реализации, превосходящие по скорости зашифрования, расшифрования и генерации ключей известные аналоги на всех тестируемых платформах, что подтверждается сравнительным анализом производительности.

Эффективность современных криптографических систем в значительной степени определяется качеством программной реализации алгоритмов, особенно в условиях ограниченных вычислительных ресурсов. ARX-шифры, такие как SPARX, обладают значительным потенциалом для оптимизации благодаря использованию простых арифметико-логических операций. Однако существующие реализации [1–4] не в полной мере используют возможности современных процессорных архитектур, что актуализирует задачу разработки оптимизированных версий с учетом специфики x86-64, ARM и RISC-V.

Задача состояла в создании оптимизированных реализаций алгоритмов SPARX-64/128, SPARX-128/128 и SPARX-128/256, обеспечивающих максимальную производительность на процессорах архитектур x86-64, ARM и RISC-V. В качестве основы использовалась эталонная реализация [1] и работа [2], в которой предложен метод двусторонней обработки ("2-way") для 32-битных архитектур. Разработаны модифицированные ARX-блоки, позволяющие обрабатывать два 16-битных операнда параллельно в одном 32-битном регистре, что эквивалентно программной SIMD-реализации без использования специализированных инструкций. Для SPARX-128/128 и SPARX-128/256 парадигма расширена для одновременной обработки четырех ветвей состояния. Построены

алгебраические модели для модифицированных алгоритмов генерации раундовых ключей $K_4^{64}, K_4^{128}, K_8^{256}$, что позволило создать корректные и эффективные реализации.

Для SPARX-64/128 разработана ассемблерная реализация, использующая динамическую генерацию раундовых ключей в регистрах, развертку циклов, минимизацию обращений к памяти и перестановку инструкций для повышения загрузки конвейера процессора.

Сравнительный анализ производительности с существующими реализациями [1–4] показал преимущество разработанных реализаций по сравнению с существующими аналогами. На архитектуре x86-64 собственная реализация SPARX-64/128 демонстрирует прирост скорости зашифрования и расшифрования на 10% относительно ближайшего аналога. Ключевой особенностью реализации на NASM является интеграция алгоритма развертывания ключа непосредственно в алгоритм шифрования, что исключает необходимость предварительных вычислений и снижает нагрузку на подсистему памяти.

Для процессора ARM Cortex-M33 зафиксированы следующие показатели прироста производительности:

- SPARX-64/128: зашифрование – 19,5%, расшифрование – 63%, генерация ключей – 18%.
- SPARX-128/128: зашифрование – 61,7%, расшифрование – 79,5%, генерация ключей – 20,8%.
- SPARX-128/256: зашифрование – 70%, расшифрование – 70%, генерация ключей м 147%.

Для объективной оценки эффективности проведен анализ количества машинных тактов, необходимых для выполнения операций шифрования. Результаты подтвердили преимущество разработанных реализаций.

Список литературы

1. SPARX – Reference implementation [Электронный ресурс] // GitHub. 2016. URL: https://github.com/cryptolu/SPARX (дата обращения: 14.06.2025).

2. Two-way SPARX/CHAM Implementation [Электронный ресурс] / ByoungJin Seok // GitHub. URL: https://github.com/ByoungJinSeok/Two-way (дата обращения: 10.04.2025).

3. Rust implementation of SPARX [Электронный ресурс] // GitHub. URL: https://github.com/jedisct1/rust-sparx (дата обращения: 10.04.2025).

4. SPARX Cipher in Rust [Электронный ресурс] / User: quininer // GitHub. 2017. URL: https://github.com/quininer/sparx-cipher (дата обращения: 10.04.2025).

УДК 519.7

Ю.С. КАЛИНИН

ООО «Центр сертификационных исследований», Москва

ОБ ОЦЕНКАХ ИЗМЕНЕНИЯ ПОРЯДКА БУМЕРАНГ-РАВНОМЕРНОСТИ ПОДСТАНОВКИ УМНОЖЕНИЕМ ЕЕ НА ТРАНСПОЗИЦИЮ

Рассматриваются бумеранг-матрица и порядок бумеранг-равномерности произвольной подстановки относительно метрического подхода. Получены оценки порядка бумеранг-равномерности произвольной подстановки, умноженной на транспозицию. В качестве следствия найдены порядки для APN-подстановок.

В 1999 г. Вагнер Д. [1] предложил модификацию разностного метода анализа, названную «метод бумеранга». Его преимущество над стандартным разностным методом заключаются в том, что даже при наличии невысокого значения порядка разностной равномерности, шифр всё равно может быть уязвим. Метод бумеранга уже применялся ко многим блочным шифрам. Кроме того, с использованием этого метода проведён анализ отечественных стандартов «ГОСТ Р 34.12-2015» и «ГОСТ 28147-89». Параметр S-блока, который влияет на стойкость к методам типа бумеранга, получил название «бумеранг-равномерность».

Пусть $n \in \mathbb{N}$, $S(\mathbb{F}_{2^n})$ – симметрическая группа на поле $\mathbb{F}_{2^n}$. В [2] введена бумеранг-матрица $\boldsymbol{\beta}(\mathrm{s}) = [\![\beta_s(\varepsilon,\delta)]\!]$ (BCT – Boomerang connectivity table), элементы которой для подставновки $s \in S(\mathbb{F}_{2^n})$ над полем $\mathbb{F}_{2^n}$ задаются условием

$$\beta_s(\varepsilon,\delta) = |\{x \in \mathbb{F}_{2^n} : s^{-1}(s(x)+\delta)+s^{-1}(s(x+\varepsilon)+\delta) = \varepsilon\}|$$

для всех $\varepsilon,\delta \in \mathbb{F}_{2^n}\backslash\{0\}$. Порядком бумеранг-равномерности $\beta(\mathrm{s})$ подстановки называется наибольший элемент бумеранг-матрицы $\beta(\mathrm{s})$, т.е.

$$\beta(\mathrm{s}) = \max\{\beta_s(\varepsilon,\delta)|\varepsilon,\delta \in \mathbb{F}_{2^n}\backslash\{0\}\}.$$

Основные свойства порядка бумеранг-равномерности и бумеранг-матрицы описаны в [2, 3].

Бумеранг-спектром назовем множество

$$B(s) = \{\beta_s(\varepsilon,\delta)|\varepsilon,\delta \in \mathbb{F}_{2^n}\backslash\{0\}\}.$$

Одним из подходов к исследованию функций является метрический. Он направлен на решение важных криптографических проблем, например,

описание всех конструкций бент-функций, построение подстановок с хорошими криптографическими свойствами и других.

Зафиксируем произвольную подстановку $s \in S(\mathbb{F}_{2^n})$ и транспозицию $\tau \in S(\mathbb{F}_{2^n})$. Подстановке s и транспозиции τ поставим в соответствие подстановку $g_s^{(\tau)} \in S(\mathbb{F}_{2^n})$, заданную условием

$$g_s^{(\tau)}: x \mapsto s\big(\tau(x)\big) \text{ для каждого } x \in \mathbb{F}_{2^n}. \quad (1)$$

Получим оценки бумеранг-равномерности подстановки $g_s^{(\tau)}$.

Теорема. *Для любых транспозиции* $\tau \in S(\mathbb{F}_{2^n})$ *и подстановки* $s \in S(\mathbb{F}_{2^n})$ *порядок бумеранг-равномерности подстановки* $g_s^{(\tau)}$*, заданной условием* (1)*, удовлетворяет неравенстве*

$$\left|\beta(\mathrm{s}) - \beta\left(g_s^{(\tau)}\right)\right| \leq 8.$$

Из теоремы следует, что максимальное изменение порядка бумеранг-равномерности, которое можно получить при действии одной транспозицией по модулю не превосходит 8.

Следствие. *Пусть* s – APN-*подстановка на* $\mathbb{F}_{2^n}$ *и* $g_s^{(\tau)}$ *задана условием* (1). *Тогда* $\beta(g_s^{(\tau)}) \leq 10$.

Отметим, что случай APN-подстановок подробнее рассматривался в [4].

Список литературы

1. Wagner D. The boomerang attack, LNCS, 1999, т. 1636, с. 156–170.
2. Cid C., Huang T., Peyrin T., Sasaki Y., Song L. Boomerang connectivity table: a new cryptanalysis tool, Eurocrypt 2018, LNCS, т. 10821, с. 683–714.
3. Boura C., Canteaut A. On the boomerang uniformity of cryptographic S-boxes IACR Transitions on Symmetric Cryptology, 2018, т. 3, с. 290–310.
4. Калинин Ю.С. О бумеранговом спектре функций, находящихся на расстоянии не более два от класса APN-функций. Прикладная дискретная математика. Приложение, 2025, №18, с. 49–56.

УДК 519.7

А.В. КОНОВАЛОВ

Национальный исследовательский ядерный университет «МИФИ», Москва

АНАЛИЗ КОРРЕКТНОСТИ И СТОЙКОСТИ ШИФРСИСТЕМЫ UFHE-ILC

Целью работы является анализ семейства, основанного на круговом поле, неограниченной полностью гомоморфной шифрсистемы UFHE-ILC, предложенной [1]. В ходе исследования выявлена неточность в процедуре генерации ключей, связанная с проверкой взаимной простоты идеалов, и предложен корректный критерий. Основным результатом является разработка и реализация полиномиального алгоритма восстановления секретного ключа, основанного на поиске целочисленного корня специально построенного многочлена.

В [1] была предложена неограниченная полностью гомоморфная шифрсистема (UFHE-ILC), основанная на идеальных решётках в кольце многочленов $\mathbb{Z}[x]/g(x)$ и китайской теореме об остатках. Для практического применения авторы представили семейство данной системы, где в качестве $g(x)$ выбирается круговой многочлен $g(x) = x^{p-1} + \cdots + x + 1$ для простого p, а закрытый ключ строится на основе главных идеалов вида $\Lambda_{q_i} = < x^{p-2} + q_i >$. Безопасность системы, согласно авторам, основывается на сложности задачи нахождения корня многочлена высокой степени.

Во-первых, был проанализирован алгоритм генерации ключей. В [1] утверждается, что для взаимной простоты идеалов Λ_{q_1} и Λ_{q_2} достаточно взаимной простоты чисел q_1 и q_2. Было показано, что это утверждение неверно. На основании работ [2, 3] сформулирован и доказан точный критерий:

Теорема 1. *Идеалы Λ_{q_1} и Λ_{q_2} взаимно просты тогда и только тогда, когда взаимно просты их одномерные модули $t(\Lambda_{q_1})$ и $t(\Lambda_{q_2})$, где $t(\Lambda_q) = g(-q)$.*

Таким образом, для корректной генерации ключей необходимо выполнять проверку $\text{НОД}\big(g(-q_1),\ g(-q_2)\big) = 1$.

Во-вторых, была продемонстрирована уязвимость системы. Открытый ключ содержит значение одномерного модуля $t = t(\Lambda_q) = g(-q)$. Задача восстановления секрета q сводится к нахождению целочисленного корня многочлена $h(x) = g(-x) - t$.

Теорема 2. *Пусть задано значение одномерного модуля* $t = g(-q)$ *и параметр* $r = O(1)$. *Тогда секретный параметр* q *может быть восстановлен за полиномиальное время от* $\deg g$ *и* $\log q$.

Шаги алгоритма:

1. Выбрать набор простых чисел $p_1, \dots, p_r$.
2. Для каждого p_i находятся корни многочлена $h(x)$ $(mod\ p_i)$. Шаг основан на вероятностных методах факторизации над конечными полями, в частности на алгоритме Кантора-Зассенхауса [4].
3. С помощью китайской теоремы об остатках из наборов корней по разным модулям восстанавливаются кандидаты на целочисленный корень q'.
4. Выполняется проверка $h(q') = 0$.

Сложность алгоритма оценивается как $O(\log^2 q \cdot \deg^{O(1)} g)$.

Эффективность шага 2, ключевого для практической реализации атаки, была подтверждена моделированием. Эксперименты по факторизации многочленов степени n показали, что среднее число итераций алгоритма Кантора-Зассенхауса демонстрирует логарифмический рост, при этом распределение числа итераций сконцентрировано вокруг среднего значения, что иллюстрируется табл. 1.

Таблица 1. Результаты моделирования алгоритма Кантора-Зассенхауса.

n	Среднее число итераций	Медиана	Стандартное отклонение
5	4.85	4	1.71
10	6.86	7	1.78
20	8.89	9	1.77
30	10.07	10	1.80
40	10.93	11	1.86
50	11.54	11	1.80

Список литературы

1. Zheng Zhiyong, Liu Fengxia, Tian Kun. An Unbounded Fully Homomorphic Encryption Scheme Based on Ideal Lattices and Chinese Remainder. 2023, arXiv:2301.12060.

2. Marcus Daniel A. Number Fields. Universitext. 2 ed, Springer, 2018, ISBN: 978-3-319-90232-6.

3. Buhler Jonathan. Resultants, Discriminants, Bezout, Nullstellensatz, etc. Algebraic Number Theory Class Notes, Reed College, https://people.reed.edu/~jpb/alg/notes/101.pdf.

4. Joachim von zur Gathen, Panario Daniel. Factoring Polynomials Over Finite Fields: A Survey // Journal of Symbolic Computation, 2001, Vol. 31, no. 1–2, p. 3–17.

УДК 519.7

Е.Д. ШАЛЮТИНА

Национальный исследовательский ядерный университет «МИФИ», Москва

О КРИПТОГРАФИЧЕСКИХ СВОЙСТВАХ СЕМЕЙСТВА S-БОКСОВ

В работе исследуются криптографические свойства параметрического семейства S-боксов на аддитивной группе n-мерном векторном пространстве над полем $\mathbb{F}_{2^d}$ и аддитивной группе кольца вычетов $\mathbb{Z}_{2^n}$. Получен критерий его биективности, а также условия инволютивности.

В современных алгоритмах блочного шифрования с помощью S-боксов оценивается стойкость к разностному и линейному криптоанализу. Значительный интерес представляет анализ S-боксов, используемых в российских стандартах шифрования «Стрибог» и «Кузнечик» [1].

В современной криптографии широко используются такие алгебраические структуры как аддитивная группа кольца вычетов $\mathbb{Z}_{2^n}$ и аддитивная группа над полем векторов $V_n(2^d)$. В данной работе вводится и исследуется криптографические свойства обобщенного параметрического семейства S-боксов, построенного по аналогичной схеме [2] в этих алгебраических структурах.

Пусть $n \geq 1$, $d \geq 2$; $V_n(2^d) -$, $(X,*)$ – абелева группа с бинарной операцией *, $X \in \{V_n(2^d), \mathbb{Z}_{2^n}\}$, $P(X)$ – полугруппа всех преобразований на X; $S(X) -$ симметрическая группа на X; $\mathcal{A}_{2^n}-$ знакопеременная группа степени 2^n.

Четверке преобразований $(b_1, b_2, b_3, b_4) \in P(X)^4$ поставим в соответствие параметрическое семейство S-боксов, заданное преобразованием $g_{b_1,b_2,b_3,b_4}: X^2 \to X^2$, его схема представлена на рис. 1.

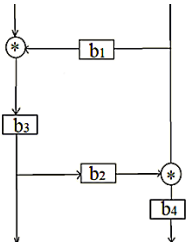


Рис. 1. Схема параметрического семейства S-боксов.

Пусть $X \in \{V_n(2^d), \mathbb{Z}_{2^n}\}$. Заметим, что преобразование параметрического семейства S-боксов g_{b_1,b_2,b_3,b_4} является композицией 2-раундового преобразования Фейстеля с функциями усложнения b_1 и $b_2 b_3$.

Теорема 1. *Пусть* $X \in \{V_n(2^d), \mathbb{Z}_{2^n}\},\ n \geq 1,\ d \geq 2,\ g_{b_1,b_2,b_3,b_4}: X^2 \to X^2$ *– отображение параметрического семейства S-боксов (рис. 1),* $b_i \in P(X)$, $i = 1,2,3,4$. *Тогда и только тогда отображение* g_{b_1,b_2,b_3,b_4} *является биективным, когда биективны преобразования* b_3, b_4.

Следствие 1. *Пусть* $X \in \{V_n(2^d), \mathbb{Z}_{2^n}\}$, $g_{b_1,b_2,b_3,b_4}: X^2 \to X^2$ *– отображение параметрического семейства S-боксов (рисунок 1),* $b_i \in P(X),\ i = 1,2,3,4$. *Тогда и только тогда* g_{b_1,b_2,b_3,b_4} *– аффинное биективное преобразование, когда:*

1) *если* $X = V_n(2^d),\ \ mo\ b_1, b_2, b_3, b_4 \in B\big(V_n(2^d)\big)$,

где $B\big(V_n(2^d)\big) =$

$$= \left\{b: V_n(2^d) \to V_n(2^d) \middle| b(x) = x^{2^k} + c\ \ \forall (k,c) \in \{1, \dots, d-1\} \times V_n(2^d)\right\};$$

2) *если* $X = \mathbb{Z}_{2^n},\ \ mo\ b_1, b_2, b_3, b_4 \in B(\mathbb{Z}_{2^n})$,

где $B(\mathbb{Z}_{2^n}) = \{b: \mathbb{Z}_{2^n} \to \mathbb{Z}_{2^n} | b(x) = x + c\ \ \forall c \in \mathbb{Z}_{2^n}\}$.

Несложно показать, что если $X \in \{V_n(2), \mathbb{Z}_{2^n}\}$ и b_i – аффинное биективное преобразование, то $b_i \in \mathcal{A}_{2^n}$ для $i = 1,2,3,4$.

Также получен общий вид разностной матрицы S-бокса как композиции разностных матриц компонентных преобразований $b_i \in P(X)$, $i = 1,2,3,4$, а также проведена оценка порядка разностной равномерности над $V_8(2)$ и аддитивной группы кольца вычетов $\mathbb{Z}_{2^8}$ в зависимости от структуры преобразований b_1, b_2, b_3, b_4. На основании полученных результатов были выделены классы преобразований $b_i,\ i = 1,2,3,4$. Кроме того, найдены условия инволютивности преобразования g_{b_1,b_2,b_3,b_4} над аддитивной группой кольца вычетов $\mathbb{Z}_{2^n}$ и аддитивной группой над полем векторов $V_n(2)$.

Список литературы

1. ГОСТ 34.12-2018. Информационная технология. Криптографическая защита информации. Блочные шифры. – Введ. 2019-06-01. – М.: Стандартинформ.

2. Reverse-Engineering the S-Box of Streebog, Kuznyechik and STRIBOBr1 (Full Version) / A. Biryukov, L. Perrin, A. Udovenko.

УДК 519.7

А.А. ВАРФОЛОМЕЕВ

Московский государственный университет им. Н.Э. Баумана,
Национальный исследовательский ядерный университет «МИФИ», Москва

МОДЕРНИЗАЦИЯ МЕХАНИЗМА АУТЕНТИФИКАЦИИ ОДНОЙ МАТРИЧНОЙ РЕАЛИЗАЦИИ ПРОТОКОЛА

В работе продолжено рассмотрение матричной реализация классического трехэтапного протокола Шамира, предложенной Дюпоном в [1] и предназначенной для низкоресурсных устройств [2]. Предлагается другой способ обеспечения аутентификации участников на основе предварительного распределения ключей, учитывающего коммутируемость ключевых матриц специального вида.

Протокол Шамира [3−5] является классическим протоколом, поэтому представляет интерес еще одна новая его реализация [1] на основе случайных секретных квадратных матриц над конечным полем.

В реализации Дюпона для протокола Шамира, открытый текст представляется квадратной матрицей M размера 24×24 над целыми числами в интервале $[-20, \dots, 0, \dots, 20]$. Подлинность участников предлагается обеспечить с помощью перестановочных матриц UI (“unequivocal identifier”), которые должны быть известны всем участникам связи (Разделы 3.2, 4.2, 5.3.3, 7.1.4 из [1]).

Матрицы $\mathrm{UI}^{(\mathrm{P},l)}, \mathrm{UI}^{(\mathrm{P},r)}$ – идентификационные матрицы участника P, $\mathrm{P}^{(l)}, \mathrm{P}^{(r)}$ – ключевые матрицы пользователя P, соответственно умножаемые слева и справа; $\mathrm{F}^{(\mathrm{P},l)}, \mathrm{F}^{(\mathrm{P},r)}$ – матрицы вырабатываются участником для каждого сеанса связи и имеют блочно-диагональный вид с восемью циркулянтными 3×3 матрицами на диагонали, $\mathrm{P} \in \{\mathrm{A}, \mathrm{B}\}$.

С использованием указанных перестановочных матриц и ключевых матриц протокол имеет следующий вид:

1 раунд. Участник A отправляет B:

$$C_1 = \mathrm{UI}^{(\mathrm{B},l)} * \mathrm{A}^{(l)} * \mathrm{M} * \mathrm{A}^{(r)} * \mathrm{UI}^{(\mathrm{B},r)};$$

2 раунд. Шаг 1. Участник B восстанавливает $\mathrm{A}^{(l)} * \mathrm{M} * \mathrm{A}^{(r)}$ из C_1;

Шаг 2. Вычисляет и отправляет

$$C_2 = \mathrm{UI}^{(\mathrm{A},l)} * \mathrm{B}^{(l)} * \mathrm{A}^{(l)} * \mathrm{M} * \mathrm{A}^{(r)} * \mathrm{B}^{(r)} * \mathrm{UI}^{(\mathrm{A},r)};$$

3 раунд. Шаг 1. Участник A восстанавливает $\mathrm{B}^{(l)} * \mathrm{A}^{(l)} * \mathrm{M} * \mathrm{A}^{(r)} * \mathrm{B}^{(r)}$;

Шаг 2. Вычисляет и отправляет

$$C_3 = \left(\mathrm{A}^{(l)}\right)^{-1} * \mathrm{B}^{(l)} * \mathrm{A}^{(l)} * \mathrm{M} * \mathrm{A}^{(r)} * \mathrm{B}^{(r)} * \left(\mathrm{A}^{(r)}\right)^{-1} =$$

$$= \mathrm{B}^{(l)} * \mathrm{M} * \mathrm{B}^{(r)}.$$

В качестве ключевых матриц генерировались матрицы вида:

$$\mathrm{P}^{(l)} = S^{(l)} * \mathrm{F}^{(\mathrm{P},l)} * \left(S^{(l)}\right)^{-1},$$
$$\mathrm{P}^{(r)} = S^{(r)} * \mathrm{F}^{(\mathrm{P},r)} * \left(S^{(r)}\right)^{-1}$$

для всех $\mathrm{P} \in \{\mathrm{A}, \mathrm{B}\}$, где обратимые матрицы $S^{(l)}, S^{(r)}$ являются общими структурными элементами для всех участников сети.

Для работы протокола необходимо, чтобы ключевые матрицы двух конкретных участников связи для левого и правого умножения на матрицу открытого текста были коммутирующими. Предлагается отказаться от использования матриц UI и заменить способ аутентификации на знание участниками набора чисел, определяющих способ независимого построения участниками коммутирующих матриц. Например, для коммутации матриц

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \qquad \begin{pmatrix} w & x \\ y & z \end{pmatrix}$$

достаточно, чтобы участники A и B выбирали независимо соответственно элементы a, b, c, d и w, x, y, z из конечного поля $\mathrm{GF}(q)$ с условием, что

$$(a-d)/b = (w-z)/x = k \text{ и } (a-d)/c = (w-z)/y = m.$$

Числа k и m могут быть предварительно распределены одним из известных методов, а их число определяется выбором большого параметра q. В отличии от перестановочных матриц UI набор чисел k и m проще распределить и хранить. Может быть и другая информация от A к B для вычисления им своей секретной коммутирующей ключевой матрицы. Ключевые матрицы большего размера могут получаться из подобных матриц блочно диагональным способом.

Предложенный в работе метод аутентификации отправителей и получателей сообщений может упростить матричную реализацию протокола Шамира для низкоресурсных систем.

Список литературы

1. Dupont F. A new Shamir's three pass random matrix ciphering mechanism, Journal of Computer Virology and Hacking Techniques, Springer-Verlag France SAS, part of Springer Nature 2023, https://doi.org/10.1007/s11416-023-00467-0.

2. Варфоломеев А.А. Некоторые замечания к новой матричной реализации трехэтапного протокола Шамира. КИБ 2023, – М.: НИЯУ МИФИ, 2023.

3. Konheim A. Cryptography. A Primer. John Willey&Sons, Inc., 1981. – 432 с.

4. Шнайер Б. прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – М.: Издательство ТРИУМФ, 2002 – 816 с.

5. Рубин Ф. Криптография с секретным ключом. – М.: ДМК Пресс, 2022. – 386 с. (16 глава. Трехпроходный протокол).

УДК 519.7

А.С. ИСМАГИЛОВА

Уфимский университет науки и технологий

АЛГЕБРАИЧЕСКИЕ ИНСТРУМЕНТЫ ДЛЯ ПОСТРОЕНИЯ КРИПТОГРАФИЧЕСКИХ СИСТЕМ

Целью настоящего исследования является анализ криптографической модели, основанной на изоморфизме групп обратимых элементов над ассоциативными кольцами, с ортогональными идемпотентами и кольцевым гомоморфизмом, для реализации шифрующих преобразований. Полученные результаты могут применяться при построении криптосистем, обладающих гомоморфными свойствами. Предложенная конструкция применима в постквантовой криптографии, обфускации программ и протоколах обмена ключами.

Рассмотрим коммутативные кольца с единицей R, S. Коммутативность по понятным причинам упрощает вычисления и подходит для построения систем, где требуется детерминированная обработка данных. Наложим условия $1/2 \in R$, $1/2 \in S$, $1/3 \in R$, которое может быть эффективно при построении обратных преобразований или обфускации функций. Рассмотрим $GL_2(R)$ группу обратимых матриц второго порядка над кольцом R − алгебраическую структуру, в которой выполняются операции над данными или ключами. Подгруппа $E_2(R) \subset GL_2(R)$, порожденная матрицами $I + rE_{ij}$, где E_{ij} − матричные единицы, моделирующая базовые операции над данными, I − единичная матрица второго порядка. Функция $\varphi: GL_2(R) \to GL_2(S)$, отображающая одну группу обратимых матриц в другую, может моделировать процесс шифрования. Здесь R − множество открытых данных, а S − множество зашифрованных данных. Тогда существуют ортогональный идемпотент $e \in S$, выделяющий часть зашифрованного множества данных, зависящих от исходного текста, и гомоморфизм $\theta: R \to eS$, переводящий элементы кольца R в соответствующие им зашифрованные образы. Справедливо следующее предложение.

Предложение. Процесс шифрования представляет собой отображение $\varphi(A) = \theta(A)e + (1 - e)$, состоящее из зашифрованной части $\theta(A)e$, зависящей от $A \in E_2(R)$, и $(1 - e)$ − обфускации, фиктивной компоненты.

Подробное математическое исследование данного результата, включая доказательства и структурные свойства, приведено в более ранних работах

автора [1]. Эти результаты дают основу для построения новых криптографических примитивов.

Приведем пример реализации описанного преобразования.

Пусть R − кольцо матриц второго порядка над конечным полем вычетов $Z/79Z$; $S = R \times R$; I − единичная матрица в R; R содержит обратимые элементы, образующие группу $GL_2(Z/79Z)$; $1/2 \in R$, $1/3 \in R$, $1/2 \in S$; $e \in S$, $e = (I, 0)$.

Очевидно, что e − ортогональный идемпотент:

$$e^2 = (I,0)(I,0) = (I^2,0) = (I,0) = e, \quad e(1-e) = (I,0)(0,I) = (0,0).$$

Определим отображение $\theta: R \to eS$ следующим образом:

$$\theta(A) = (A,A)e = (A,0), \quad \forall A \in R.$$

Ясно, что θ − кольцевой гомоморфизм:

$$\theta(A+B) = (A+B,0) = (A,0) + (B,0) = \theta(A) + \theta(B),$$
$$\theta(AB) = (AB,0) = (A,0)(B,0) = \theta(A)\theta(B).$$

Выберем открытый текст в виде обратимой матрицы $A \in GL_2(Z/79Z)$:

$$A = \begin{pmatrix} 2 & 3 \\ 5 & 7 \end{pmatrix}, \quad \det A = -1, \quad -1 \equiv 78 \bmod 79.$$

Применим шифрующее отображение

$$\varphi(A) = \theta(A)e + (1-e) = (A,0) + (0,I) = (A,I),$$

т.е. шифрующее отображение есть пара матриц $(A, I) \in S$.

Для расшифрования достаточно извлечь первую компоненту шифротекста $\varphi(A) = (A, I)$, т.е. не зная e и φ восстановить A невозможно.

Таким образом, безопасность системы основана на сложности восстановления исходной матрицы A из шифротекста (A, I) без знания структуры кольца S, идемпотента e и гомоморфизма θ.

Усложнить систему можно также применив случайное сопряжение, например, такую матрицу $M \in GL_2(S)$, что $\varphi'(A) = M\varphi(A)M$.

Таким образом, любое преобразование, сохраняющее групповую структуру, может быть представлено как комбинация зашифрованного отображения и фиктивного слагаемого. Дальнейшие исследования могут быть масштабированы, например, на некоммутативные структуры.

Список литературы

1. Ismagilova, A.S. A homomorphism of the group GL2(R) / A.S.Ismagilova // Journal of Mathematical Sciences. – 2007. – Vol. 144, No. 2. – P. 3938–3948. – DOI 10.1007/s10958-007-0246-7.

УДК 004.056

К.Г. КОГОС

Национальный исследовательский ядерный университет «МИФИ», Москва

О НОРМАЛИЗАЦИИ ТРАФИКА ПО ВРЕМЕНИ ПРИ ПРОТИВОДЕЙСТВИИ УТЕЧКЕ ИНФОРМАЦИИ ПО СКРЫТЫМ КАНАЛАМ

Скрытые каналы могут быть построены «невидимым» для традиционных средств защиты информации способом [1], следовательно, предотвращение утечки информации с их использованием не перестает быть актуальным. Известно, что большую угрозу для утечки информации представляют скрытые каналы по памяти [2, 3]. Однако если после применения методов нормализации трафика по памяти угроза утечки информации все еще актуальна, следует вводить механизм ограничения скрытого канала по времени. К таким способам относят полную и частичную нормализацию длин межпакетных интервалов, исследованных в настоящей работе.

Нормализация по времени осуществляется за счет введения дополнительных задержек пакетов и генерации фиктивного трафика таким образом, чтобы в момент отправки между всеми пакетами были равные межпакетные интервалы $t_{вып}$. Если следующий после только что отправленного пакета получен через время $t(i) \le t_{вып}$, то этот пакет задерживается на время $t_{вып}-t(i)$, и только потом отправляется. Если же пакет получен через $t(i) > t_{вып}$, то генерируется и последовательно отправляется $\lceil t(i)-t_{вып} \rceil$-1 пакетов, после чего отправляется содержащий полезную нагрузку пакет, с необходимой задержкой. Схема приведена на рис. 1.

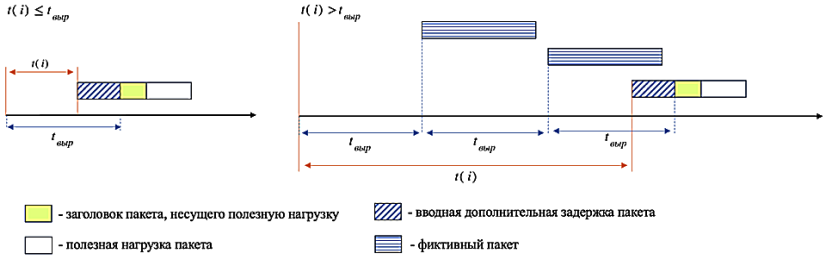


Рис. 11. Схема полной нормализации трафика по времени

Поскольку при полной нормализации трафика по времени эффективная пропускная способность канала связи значительно снижается, проанализируем реализацию подхода, заключающегося в частичной нормализации трафика. В этом случае в трафике возможно

применение двух длин межпакетных интервалов: $t_{выр1}$ и $t_{выр2}$, $t_{выр1}<t_{выр2}$. Для минимизации длин фиктивных пакетов в случае отсутствия пакетов, содержащих полезную нагрузку, отправляются фиктивные пакеты с межпакетными интервалами $t_{выр2}$.

Пусть получен пакет с межпакетным интервалом длиной $t(i)$. Тогда:

– если $t(i)\le t_{выр1}$, то пакет задерживается на $t_{выр1}-t(i)$;

– если $t_{выр1}<t(i)\le t_{выр2}$, то пакет задерживается на $t_{выр2}-t(i)$;

– если $t(i)>t_{выр2}$, то отправляется $\lceil t(i)-t_{выр2}\rceil$-1 фиктивный пакет с межпакетными интервалами $t_{выр2}$, а межпакетный интервал для отправки пакета с полезной нагрузкой определяется согласно первым двум пунктам схемы, представленной на рис. 2.

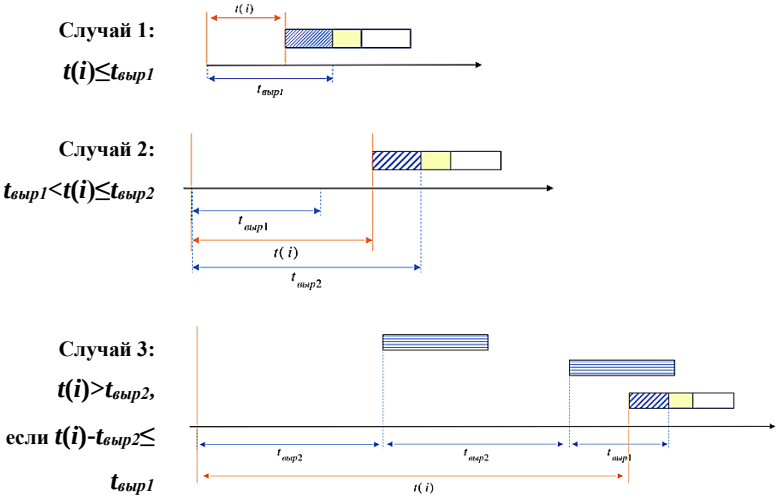


Рис. 2. Схема частичной нормализации трафика по времени

Выбор параметров метода противодействия $t_{выр1}$ и $t_{выр2}$ должен определяться минимизацией доли фиктивных пакетов в трафике и ограничением на допустимую среднюю задержку пакетов.

Список литературы

1. Грушо А.А. Скрытые каналы и безопасность информации в компьютерных системах // Дискретная математика. – 1998. – Т. 10, № 1.

2. Dua A., Jindal V., Bedi P. Detecting and Locating Storage-Based Covert Channels in Internet Protocol Version 6 // IEEE Access. – 2022. – Vol. 10. – P. 110661–110675.

3. Когос К.Г., Финошин М.А., Айрапетян С.В. Метод идентификации скрытых каналов по памяти в сетях пакетной передачи данных // Безопасность информационных технологий. – 2021. –Т. 28. № 3. – С. 56-64.

УДК 519.719.2

Д.М. КРАПИВЕНЦЕВ

Национальный исследовательский ядерный университет «МИФИ», Москва

ЗАЩИТА ОТ КОЛЛИЗИЙ СЕРИЙНЫХ НОМЕРОВ В ИНФРАСТРУКТУРЕ ОТКРЫТЫХ КЛЮЧЕЙ

Управление жизненным циклом ключей асимметричных криптосистем обычно обеспечивается системой удостоверяющих центров, выпускающих сертификаты по стандарту X.509. Предлагается алгоритмический способ решения проблемы защиты уникальных данных в сертификатах открытых ключей для обеспечения корректного и устойчивого функционирования архитектуры открытых ключей с использованием избыточного кодирования.

Серийные номера сертификатов являются уникальными для фиксированного удостоверяющего центра, благодаря чему осуществляется связка элементов открытого ключа, серийного номера сертификата и владельца закрытого ключа. Серийные номера являются обязательным атрибутом сертификатов открытых ключей, атрибутных сертификатов согласно международному стандарту X.509 [1, 2].

Вопросы надежности при формировании сертификата и возможности их фальсификации с точки зрения анализа полей сертификатов и их возможных значений исследовались в небольшом количестве исследований, например, в [3, 3]. Вопросы практической защиты дополнительными механизмами, которые предлагаются в данной работе, обычно не рассматриваются.

В процессе жизнедеятельности информационных систем некоторые сертификаты должны прекратить свое действие, например, вследствие компрометации ключевой пары, либо при увольнении сотрудника. Стандарты определяют механизм прекращения действия с помощью списков досрочно прекративших действие сертификатов (certificate revocation list, CRL) [[1, 2, 5].и с помощью запросов о статусе сертификата на текущий момент времени (через online certificate status protocol, OCSP) [6, 6].В силу того, что сертификаты являются достаточно объемным объектом с точки зрения используемой для его хранения памяти, с учетом потенциально больших размеров открытых ключей в постквантовых криптосистемах, а также с учетом того, что владелец сертификата не всегда хочет раскрывать сведения сертификата неопределенному кругу лиц, в CRL, выпускаемых удостоверяющими центрами, и в ответах протокола OCSP указываются только серийные номера сертификатов.

Таким образом, статус сертификата проверяющая сторона определяет только по серийному номеру.

Как CRL, так и OCSP являются защищенными объектами, целостность которых обеспечивается цифровой подписью (которую можно также трактовать как электронную), поэтому единственным требованием к безопасности, помимо стойких криптографических функций, является уникальность серийных номеров.

В реальном мире, а не в идеализированной модели, корректное функционирование средств удостоверяющих центров и средств электронной подписи полагается на правильную работу технических средств. Как мы знаем, при работе технических средств могут наблюдаться определенные искажения [8]. Внутренние алгоритмы корректировки ошибок существуют, но из-за отсутствия их полноценного описания и точных оценок полагаться только на них не представляется возможным.

Для защиты от искажения предлагается использовать алгоритмическое решение через избыточное кодирование серийных номеров, чтобы сократить множество допустимых серийных номеров. Такие алгоритмы распространены, например, для защиты номеров банковских карт и денежных купюр. Использование избыточности позволит сократить вероятность ложного определения серийных номеров при проверке.

Список литературы

1. ITU-T Recommendation X.509. Information technology - Open systems interconnection - The Directory: Public-key and attribute certificate frameworks. 2008.
2. RFC 5280. Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.
3. Zulfiqar, M., Janjua, M.U., Hassan, M. Tracking adoption of revocation and cryptographic features in X.509 certificates. Int. J. Inf. Secur. 2022, №21, pp. 653–668. DOI: https://doi.org/10.1007/s10207-021-00572-5.
4. Wang, J. The Prediction of Serial Number in OpenSSL's X.509 Certificate: Research Article. 2019. HindawiSecurity and Communication NetworksVolume 2019, Article ID 6013846, 11 pageshttps://doi.org/10.1155/2019/6013846.
5. Р 1323565.1.023–2022 «Использование алгоритмов ГОСТ Р 34.10–2012, ГОСТ Р 34.11–2012 в сертификате, списке аннулированных сертификатов (CRL) и запросе на сертификат PKCS #10 инфраструктуры открытых ключей X.509».
6. RFC 6960. X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP.
7. Р 1323565.1.059–2024 «Информационная технология. Криптографическая защита информации. Использование российских криптографических алгоритмов в протоколе получения актуальных статусов сертификатов (OCSP)».
8. Надёжность электрорадиоизделий, 2006: справочник / М.: ФГУП «22 ЦНИИИ МО РФ», 2008. – 641 с.

УДК 004.056

В.А. ШЕВЧЕНКО, С.В. ЗАПЕЧНИКОВ

Национальный исследовательский ядерный университет «МИФИ», Москва

ПОДХОДЫ К РЕАЛИЗАЦИИ ПРОТОКОЛОВ КОНФИДЕНЦИАЛЬНОГО ПРИМЕНЕНИЯ МОДЕЛЕЙ МАШИННОГО ОБУЧЕНИЯ НА ОСНОВЕ ГРАФОВ С ПРИМЕНЕНИЕМ ПЛАТФОРМЫ «КОНФГРАФ»

В работе рассмотрены основные риски применения моделей машинного обучения, а также основные идеи конфиденциального машинного обучения. Представлены подходы к реализации конфиденциального применения моделей машинного обучения на основе графов с применением платформы «КонфГраф» на примере протокола конфиденциального поиска максимального значения в массиве.

Технологии искусственного интеллекта (ИИ) прочно вошли в нашу жизнь. Общеизвестно, что модели машинного обучения (МО) служат ядром технологий ИИ, однако технологии обеспечения информационной безопасности ИИ отстают от высоких темпов его развития. Актуальными являются такие риски применения моделей МО, как:

- хранение и применение предварительно обученных моделей МО в недоверенных вычислительных средах (например, в облаке);
- обработка запросов к модели МО в открытом виде.

Конфиденциальное машинное обучение (КМО) – область знаний на стыке МО и криптографии. В системах КМО данные риски устраняются путем применения криптографических протоколов. Инструментальным базисом КМО служат безопасные многосторонние вычисления (БМВ). Основная задача БМВ – определение способов построения функции $y = F(x_0, \dots, x_{n-1})$, где x_i – конфиденциальные данные i -го участника протокола БМВ, для которой гарантируется, что x_i не станет известно никому, кроме i-го участника протокола БМВ и значение функции $F(x_0, \dots, x_{n-1})$ одинаково для всех участников протокола и известно им [1].

Схемы разделения секрета (СРС) – один из криптографических примитивов, лежащих в основе большого числа протоколов БМВ. Основная их идея заключается в разделении секрета X на n долей $x_0, \dots, x_{n-1}$ в соответствии с алгоритмом $Shr: X \to X_1^n$ и отправке соответствующей доли секрета x_i i-му участнику протокола таким образом, что в дальнейшем секрет X может быть восстановлен с помощью алгоритма $Rec: X_1^n \to X$.

Анализ существующих систем КМО показал наличие очень небольшого количества решений для моделей МО на основе графов [2]. В связи с этим авторами доклада была разработана платформа конфиденциального применения предварительно обученных графовых нейронных сетей «КонфГраф».

Рассмотрим протокол поиска максимального значения в массиве, являющийся основой graphSAGE с агрегированием сообщений поиском максимального значения и реализованный в «КонфГраф».

Поиск максимального значения в массиве, элементы которого разделены на доли между двумя участниками с помощью СРС, требует разработки отдельного протокола БМВ. Предлагаемая его реализация основана на конфиденциальной проверке числа на положительное значение.

Пусть $a_0, \dots, a_{n-1}$ – массив из n элементов. Общая идея итеративного поиска максимального значения в массиве состоит в вычислении $m = m \cdot \big((m - a_{i+1}) > 0\big) + a_{i+1} \cdot \Big(1 - \big((m - a_{i+1}) > 0\big)\Big),\ \ i \in \{0, n-2\},\ \ m = a_0$ при $i = 0$. Значение m возвращается в качестве результата.

Указанное выражение состоит из умножения, сложения и сравнения с нулем, что говорит о возможности реализации конфиденциального протокола поиска максимального значения в массиве путем их замены на соответствующие протоколы БМВ на основе СРС. Протокол будет иметь вид:

Для всех $j \epsilon \{0, n-2\}$:

$$\langle g \rangle_i^A = \mathrm{GTZ}\big(\langle m \rangle_i^A - (\langle a \rangle_i^A)_{j+1}\big),$$
$$\langle l \rangle_i^A = (q \cdot 2^{-1} \bmod q - \langle g \rangle_i^A + i) \bmod q,$$
$$\langle x \rangle_i^A = \langle m \rangle_i^A \cdot \langle g \rangle_i^A, \langle y \rangle_i^A = (\langle a \rangle_i^A)_{j+1} \cdot \langle l \rangle_i^A,$$
$$\langle m \rangle_i^A = \langle x \rangle_i^A + \langle y \rangle_i^A \bmod q,$$

где $\mathrm{GTZ}(\langle x \rangle_i^A)$ – протокол конфиденциального сравнения с нулем [3], q – большое простое число.

Можно убедиться, что подход к реализации отдельных операций при помощи протоколов БМВ из состава «КонфГраф» позволяет создать протокол конфиденциального применения моделей МО на основе графов. Таким образом, можно устранить указанные риски применения данных моделей МО.

Список литературы

1. Evans D., Kolesnikov V., Rosulek M. A pragmatic introduction to secure multi-party computation. NOW Publishers, 2018.

2. 31. Encudero D. An Introduction to Secret-Sharing-Based SMPC, Cryptology ePrint Archive, 2022. – 102 p. URL: https://eprint.iacr.org/2022/062 (дата обращения: 10.10.2025).

3. Catrina O., de Hoogh S. Improved Primitives for Secure Multiparty Integer Computation. Security and Cryptography for Networks. Lecture Notes in Computer Science, vol 6280, Springer, 2010, pp 182–199. DOI: https://doi.org/10.1007/978-3-642-15317-4_13).

УДК 519.719.2

М.А. ГРИШИН

Национальный исследовательский ядерный университет «МИФИ», Москва

ОБЗОР МЕТОДОВ И ИНСТРУМЕНТАЛЬНЫХ СРЕДСТВ ФАЗЗИНГ-ТЕСТИРОВАНИЯ РЕАЛИЗАЦИЙ КРИПТОГРАФИЧЕСКИХ БИБЛИОТЕК

Работа посвящена исследованию подходов инструментальной и технологической поддержки автоматизированного выявления ошибок и уязвимостей в реализациях криптографических библиотек с применением техники фаззинга. Проведена классификация существующих фаззеров, реализуемых ими схем тестирования применительно к криптографическим функциям и протоколам, а также их сравнительный анализ. В результате проведенного анализа выявлен ряд недостатков в существующих релевантных фаззинг-системах и предложены перспективные направления их развития.

Криптографические алгоритмы играют ключевую роль в обеспечении информационной безопасности современных компьютерных систем. Дефекты в их реализациях способны привести к возникновению уязвимостей, снижающих устойчивость системы к угрозам, поэтому своевременное обнаружение и ликвидация ошибок становится приоритетной задачей. Фаззинг - техника автоматизированного выявления уязвимостей посредством подачи некорректных либо частично корректных данных на вход тестируемого ПО [1]. В то же время сложность архитектуры криптографических алгоритмов и специфика требований к обработке входных данных обуславливают потребность в разработке специализированных инструментальных средств, направленных на повышение эффективности и точности фаззинг-тестирования.

В табл. 1 представлен обзор распространенных инструментальных средств (ИС) и применяемых ими методов обнаружения ошибок, среди которых отдельно можно выделить:

1) *метод дифференциального тестирования* – в общем случае заключается в проверке принадлежности значения некоторой функции $\boldsymbol{f}(\boldsymbol{p_1}(\boldsymbol{x}), \dots, \boldsymbol{p_n}(\boldsymbol{x}))$ критической области, где $\boldsymbol{p_1}, \dots, \boldsymbol{p_n}$ – разные реализации одного алгоритма. В базовом случае проверяется $\boldsymbol{p_1}(\boldsymbol{x}) = \boldsymbol{p_2}(\boldsymbol{x})$;

2) *метод кросс-проверок* – выявление логической неконсистентности в результатах применения композиции функций одной реализации $\boldsymbol{p}$ $\boldsymbol{Verify}\left(\boldsymbol{f_p^1}\circ \ldots \circ \boldsymbol{f_p^n}(\boldsymbol{x})\right) \in \{\mathbf{0},\mathbf{1}\}$;

3) *семантический метод* – генерация семантически корректных тестовых наборов с целью обхода множества проверок в реализациях.

Таблица 1. Распространенные методы фаззинга криптографических библиотек

ИС	Классификация	Цель	Типы ошибок	Методы
CDF	Генерационный, черный ящик	Реализации базовых примитивов (функции в OpenSSL, SymCrypt, wolfCrypt и т.д.)	ошибки логики реализации; утечки времени	дифференциальное тестирование; кросс-проверки
Cryptofuzz	Комбинированный, серый ящик		ошибки работы с памятью; ошибки логики реализации	дифференциальное тестирование; кросс-проверки;
CLFuzz	Мутационный, серый ящик		ошибки логики реализации; ошибки работы с памятью; архитектурные ошибки	семантический метод; дифференциальное тестирование; кросс-проверки;
Tls-fuzzer dtls-fuzzer	Генерационный, черный ящик	TLS/DTLS/SSL реализации (клиент / сервер)	отклонения от спецификаций; ошибки памяти в парсерах сообщений; нарушение последовательности сообщений в handshake	стресс-метод; сценарный метод

На основе проведенного анализа можно предложить следующие возможные направления модификации фаззинг-схем тестирования криптографических библиотек:

1) расширение множества проверяемых фаззером криптографических свойств, в частности, с помощью интеграции с релевантными сканнерами, переход к отслеживанию многофакторных состояний;

2) построение распределенной системы тестирования с выделенными фаззинг-кластерами, отвечающими за поиск отдельных классов ошибок, для повышения отказоустойчивости и ускорения анализа;

3) разработка и применение адаптивных биомимикрических алгоритмов в семантико-ориентированном фаззинге как альтернативы случайному выбору операторов мутации.

Список литературы

1. ГОСТ Р 56939-2024 Защита информации. Разработка безопасного программного обеспечения. Общие требования. М.: Стандартинформ, 2024. – 120 с. – Утверждён приказом Росстандарта от 24.10.2024 № 1504-ст.

УДК 004.056

А.А. КОЗЛОВ

Национальный исследовательский ядерный университет «МИФИ», Москва

АНАЛИЗ ПОВЕРХНОСТИ АТАКИ НА СОВРЕМЕННЫЕ АВТОМОБИЛИ

Современные автомобили уже давно не просто средство для передвижения. Встроенные в них сервисы предоставляют пользователям широкие возможности: от подогрева сидений до заказа билетов в театр. Вместе с развитием потребительских сервисов развивались также системы и сервисы, обеспечивающие безопасность водителя [1]. Однако, подобные решения, призванные повысить удобство вождения и сделать его более безопасным, архитектурно основаны на технологиях и алгоритмах, которые сами по себе несут угрозы информационной безопасности [2]. Внедрение новых технологий в автомобилестроение, порой без должного внимания к информационной безопасности, влечет за собой рост способов реализации угроз безопасности [3]. В докладе для каждого из доменов ИБ: физического, локального и удаленного, обсуждаются поверхность атаки и возможности потенциальных злоумышленников. В заключении рассматриваются способы обеспечения безопасности современных автомобилей, а также обозначаются открытые вопросы.

Основываясь на внутренней технической оснащенности и функциональных возможностях, без ограничения общности разделить все автомобили на три категории:

- Устаревший автомобиль
- Классический автомобиль
- Современный автомобиль

В контексте анализа безопасности автомобилей следует разделять всех злоумышленников по двум атрибутам:

- наличие ресурсов (деньги, время)
- наличие профильных технических знаний.

Из такой аналитической позиции видна тенденция снижения порога вхождения в область информационной безопасности автомобилей. В основном - за счет удешевления аппаратных инструментов воздействия и архитектурной схожести автомобиля с уже хорошо изученными объектами ЛВС. Кроме того, сами автомобили стали более доступными для исследования. Если раньше автомобиль был предметом роскоши, то сейчас он есть почти в каждой семье.

Тренд снижения порога вхождения неразрывно связан с еще одним трендом – изменения объектов воздействия внутри автомобиля. В соответствии с картой потоков данных автомобиля, всего можно выделить три типа информационных доменов:

- физический (требуется физический контакт с объектом, например, шина CAN)
- локальный (adjacent) (взаимодействие возможно в пределах до 100 м, например, WiFi)
- удаленный (взаимодействие возможно на расстоянии много большим 100 м от объекта, например, GSM).

В настоящее время вопросом обеспечения безопасности действительно озаботились государственные регуляторы, автомобильные вендоры и компании в области информационной безопасности Каждый из них в рамках своих полномочий вносит свой вклад в обеспечение безопасности автомобильной индустрии. Их скоординированные усилия в области информационной безопасности обеспечивают снижение вероятности реализации угроз безопасности, достигаемое различными методами, направленными на:

- уменьшение поверхности атаки
- повышение сложности реализации компьютерной атаки
- повышение скорости реагирования на инциденты ИБ

Открытые вопросы включают в себя:

- разработку новой архитектуры ЛВС и ЭБУ автомобиля, ориентированной на безопасность (Security by Design)
- разработку новых моделей событий безопасности на основе доступных данных через TCU автомобиля

Список литературы

1. Мардоян Гурген Робертович, Симонян Рубен Игоревич, Карпов Никита Андреевич, Пронин Николай Александрович, Метелев Сергей Юрьевич Современные подходы к испытанию систем ADAS на всех этапах разработки // Труды НГТУ им. Р.Е. Алексеева. 2018. №4 (123).

2. Клиновенко В.В., Колистратов М.В. Автомобильная электроника и угроза ее информационной безопасности // E-Scio. 2021. №9 (60).

3. Скатков Александр Владимирович, Брюховецкий Алексей Алексеевич, Моисеев Дмитрий Владимирович, Воронин Дмитрий Юрьевич. Обеспечение безопасности интеллектуальных транспортных средств в инфраструктуре умного города // International Journal of Open Information Technologies. 2020. №11.

УДК 004.056

Н.А. РАЗВАЛОВ

Ярославский государственный университет им. П.Г. Демидова

ПРИМЕНЕНИЕ ВОДЯНЫХ ЗНАКОВ ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ЦИФРОВЫХ КАРТ

Работа посвящена защите авторских прав на цифровые карты путем внедрения цифровых водяных знаков (ЦВЗ) в координаты картографических объектов. Предложен метод, устраняющий уязвимость существующего подхода к атаке вращением. Суть метода заключается в определении «начального положения» данных, встраивании ЦВЗ в этом положении и последующем восстановлении данных после атаки за счет восстановления ориентации. Экспериментальные результаты подтверждают устойчивость метода к геометрическим преобразованиям, включая вращение.

С ростом популярности пространственных данных возникает проблема защиты авторских прав. Поскольку данные могут быть легко скопированы и распространены без согласия правообладателя, существует риск потери контроля над информацией и нарушения авторских прав.

Для решения этой проблемы используются различные методы защиты, включая цифровые водяные знаки (ЦВЗ). ЦВЗ представляют собой скрытые метки, внедряемые в пространственные данные. Эти метки могут содержать информацию о правообладателе, дате создания, версии данных и других атрибутах.

Применение ЦВЗ позволяет идентифицировать источник данных, отслеживать их распространение и предотвращать несанкционированное копирование. Способ внедрения ЦВЗ должен обеспечить устойчивость водяных знаков к искажениям и атакам злоумышленников.

Рассмотрим один из методов встраивания ЦВЗ, являющийся модификацией метода LSB: каждый бит водяного знака многократно встраивается в младшие разряды координат точек цифровой карты [1]. Предлагается использовать для встраивания бита водяного знака 15-ый и 16-ый знаки после запятой, поскольку они имеют меньшее влияние на точность координат, чем другие позиции. Анализ метода на устойчивость к различным видам атак показал, что он чувствителен к атаке вращением.

В настоящем исследовании предлагается модификация метода [1], устойчивого в том числе и к атаке вращением.

Правильным положением назовем такое положение пространственных данных, которое можно идентифицировать. На первом шаге предлагаемого метода выделяются ключевые точки картографических объектов, то есть те, которые оказывают значительное влияние на форму и остаются неизменными при смене масштаба. Для этой цели используется один из алгоритмов геометрического упрощения, например, алгоритм Дугласа-Пейкера [2]. На втором шаге применяется алгоритм нахождения минимального ограничивающего прямоугольника (MBR). Результатом работы алгоритма является минимальный по площади прямоугольник, внутри которого содержатся все векторные данные. Для каждого набора точек существует только один минимальный ограничивающий прямоугольник. Правильным положением векторных данных будем считать положение, когда минимальный ограничивающий прямоугольник находится параллельно осям координат. Производится поворот пространственных данных в правильное положение, затем встраивание ЦВЗ согласно исходному методу и обратный поворот к начальному положению.

Перед извлечением ЦВЗ также строится минимальный ограничивающий прямоугольник. Для разворота данных в правильное положение будет существовать четыре варианта, когда стороны ограничивающего прямоугольника будут параллельны осям координат. Один из них будет являться правильным положением, в которое производилось встраивание. Одна из четырех попыток извлечения ЦВЗ будет успешной.

Тестирование показало, что улучшенный вариант метода позволил устранить уязвимость к атаке вращением. Улучшенный метод продемонстрировал стабильность и высокую устойчивость ко всем видам атак, включая сложные преобразования, такие как масштабирование, добавление и удаление объектов.

Список литературы

1. Haowen Yan A normalization-based watermarking scheme for 2D vector map data / Haowen Yan, Liming Zhang, Weifang Yang // Earth Sci Inform. – 2017. – № 10. – P. 471–481.

2. Douglas D. H., Peucker T. K. Algorithms for the reduction of the number of points required to represent a digitized line or its caricature // Canadian Cartographer. – 1973. – 10(2) – p. 112–122.

УДК 004.056

А.И. БЕЛОЗУБОВА

Национальный исследовательский ядерный университет «МИФИ», Москва

ОГРАНИЧЕНИЕ ПРОПУСКНОЙ СПОСОБНОСТИ СКРЫТЫХ КАНАЛОВ ПО ВРЕМЕНИ: ВВЕДЕНИЕ ЗАДЕРЖЕК

Скрытым каналом называется изначально непредназначенный для коммуникации канал, который может быть использован для нарушения политики безопасности. Актуальность проблеме утечке информации по таким каналам придает возможность построения необнаруживаемых скрытых каналов [1]. Один из методов борьбы со скрытыми каналами заключается в ограничении их пропускной способности до допустимого значения $C_{доп}$, которое считается безопасным. В качестве способа ограничения пропускной способности сетевых скрытых каналов по времени (ССКВ) выбрано добавление задержек перед отправкой IP-пакетов [2, 3]. Актуальной остается задача выбора параметра метода противодействия. В статье кратко описана разработанная прикладная методика выбора значения параметра исследуемого метода противодействия и приведены результаты её апробации.

Для борьбы с утечкой информации по скрытым каналам путем введения шума в ССКВ для ограничения их пропускной способности, была разработана прикладная методика противодействия. Для использования методики необходимо установить допустимое значение $C_{доп}$. Методика противодействия рассматривает ССКВ, основанные на изменении длин межпакетных интервалов ($СК_{ми}$) [4].

Пусть значения вводимых задержек перед отправкой IP-пакетов распределены по некоторому закону на интервале (0; d). Методика противодействия позволяет выбрать значение параметра d, которое обеспечит снижение пропускной способности ССКВ до значения $C \leq C_{доп}$, а также минимизирует нагрузку на коммуникационный канал. Блок-схема методики представлена на рис.1.

Для апробации методики было установление значение $C_{доп}$=100 б/с согласно рекомендациям TCSEC и IBM Knowledge Center. В результате применения методики для $СК_{ми}$ определено:

1. без противодействия пропускная способность $СК_{ми}$ достигает 404 бит/с, что требует введения контрмер,
2. пропускная способность $СК_{ми}$ снижается до 99 бит/с при d=43 мс,
3. невозрастающая плотность распределения задержек снижает нагрузку на канал связи на 3% по сравнению с задержками, значения которых распределены равномерно.

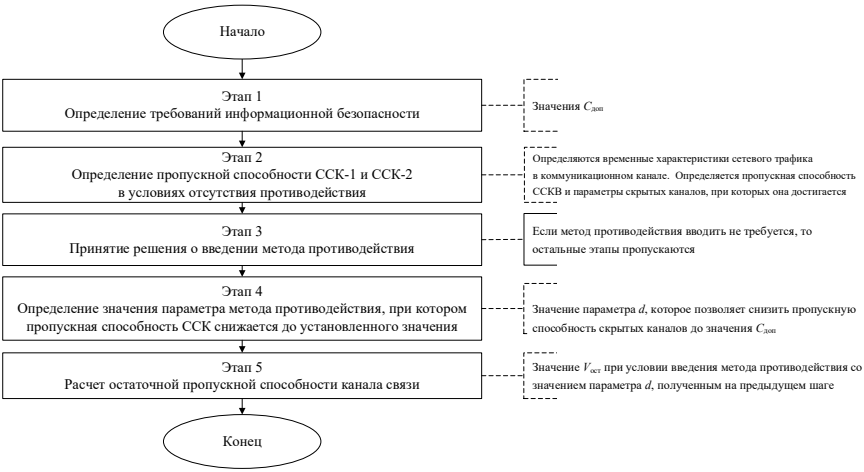


Рисунок 21 — Блок-схема методики противодействия утечке информации по ССКВ

Таким образом, автором предложена методика противодействия утечке информации по ССКВ путем ограничения их пропускной способности за счет введения шума в скрытый канал. Новизна методики заключается в наличии алгоритма определения параметра противодействия, который позволяет снизить пропускную способность ССКВ до заданного значения и рассматривает способы снижения нагрузки на коммуникационный канал. Методика применима в случае, когда политикой безопасности допускается функционирование ССКВ с пропускной способностью не выше установленного уровня.

Список литературы

1. Грушо А.А. Скрытые каналы и безопасность информации в компьютерных системах // Дискретная математика. – 1998. – Т. 10, № 1.

2. Белозубова А.И., Епишкина А.В., Когос К.Г. Ограничение пропускной способности сетевых скрытых каналов по времени путём введения дополнительных случайных задержек перед отправкой пакета // Безопасность информационных технологий. – 2021. – Т. 28, № 4. – С. 74–89.

3. Belozubova A., Epishkina A., Kogos K. How to Limit Capacity of Timing Covert Channel by Adding Extra Delays // Procedia Computer Science. – 2021.

4. Sellke S.H., Wang C.-C., Bagchi S., Shroff N.B. Covert TCP/IP Timing Channels: Theory to Implementation // Proceedings of the 28th IEEE Conference on Computer Communications (INFOCOM). – 2009.

УДК 004.056

Е.А. БАСЫНЯ, В.Ю. САПЕГИН

Национальный исследовательский ядерный университет «МИФИ», Москва

ВИРТУАЛЬНАЯ СЕТЕВАЯ ЛАБОРАТОРИЯ МОДЕЛИРОВАНИЯ, МОНИТОРИНГА И АНАЛИЗА СКРЫТЫХ КАНАЛОВ СВЯЗИ

В работе представлена разработка виртуальной сетевой лаборатории, предназначенной для моделирования, мониторинга и анализа скрытых каналов связи с применением децентрализованной системы обработки и хранения сетевых данных. Целью исследования являлось создание воспроизводимой, доверенной и масштабируемой среды, обеспечивающей проведение экспериментов в области построения и исследования виртуальных защищенных каналов связи, функционирующих на базе стека протоколов TCP/IP версии 4 и 6.

Обеспечение достоверности и воспроизводимости результатов научно-исследовательской деятельности является приоритетной задачей. Для ее достижения в прикладных научных изысканиях и программной инженерии следует разрабатывать и внедрять виртуальные сетевые лаборатории, которые смогут обеспечить автоматизацию процесса развертывания и управления всеми инфраструктурными объектами.

В данной работе разработана архитектура виртуальной сетевой лаборатории с применением открытых средств виртуализации и управления инфраструктурой, что обеспечило ее гибкость, переносимость и возможность горизонтального и вертикального масштабирования.

Основной платформой виртуализации было выбрано решение Proxmox Virtual Environment. Использование Proxmox VE позволяет развертывать виртуальные машины с различными конфигурациями сетевых интерфейсов, моделировать сложные топологии VPN-соединений и управлять ресурсами вычислительного кластера через API.

Автоматизация инфраструктурного уровня реализована с помощью Terraform, который обеспечивает декларативное описание конфигурации вычислительных узлов, сетевых параметров и виртуальных сред. Ansible-применяется для автоматической установки и настройки компонентов VPN-инфраструктуры (например, WireGuard, OpenVPN, StrongSwan, Trojan, Xray), а также сервисов сбора и обработки телеметрических данных.

Особенностью разработанной виртуальной лаборатории является возможность эмуляции сетевых состояний, характерных для реальных распределенных систем. На уровне сетевых модулей виртуальных машин

моделируются параметры деградации каналов связи – задержки, джиттер, потери пакетов и ограничение пропускной способности. Для этого используются встроенные механизмы tc (Traffic Control) и netem, позволяющие вносить управляемые и воспроизводимые искажения в трафик между узлами.

Ключевой особенностью предлагаемого решения является применение децентрализованной системы обработки и хранения сетевых событий, реализованной на основе принципов, изложенных в [1]. Каждое сетевое событие, зафиксированное в процессе эксперимента, проходит процедуру хеширования и записи метаданных в децентрализованный реестр, что обеспечивает неизменность данных, прозрачность аудита и возможность независимой верификации результатов. Такая архитектура позволяет достичь доверенной фиксации результатов мониторинга VPN-трафика и повысить достоверность научно-практических исследований.

Для моделирования VPN-коммуникаций использовался метод построения самоорганизующихся защищенных каналов связи, основанный на стохастическом многоуровневом шифровании и оверлейных технологиях, описанных в [2]. Виртуальная сетевая лаборатория обеспечивает возможность воссоздания различных топологий взаимодействия узлов, что делает данный стенд эффективным инструментом для проверки эффективности методов защиты информации. Кроме того, в рамках данной лаборатории проводится исследование и апробация современных методов детекции VPN-трафика на основе машинного обучения (ML), реализуемых в режиме реального времени, включая алгоритмы анализа сетевых потоков и классификации зашифрованных соединений, основанные на принципах, представленных в [3].

Результаты разработки могут быть использованы для проведения научно-практических экспериментов, направленных на повышение доверенности и устойчивости VPN-инфраструктур, а также для тестирования новых методов защиты информации и протоколов безопасной передачи данных.

Список литературы

1. Басыня Е.А., Сафронов А.В. Метод формирования децентрализованного реестра событий информационной инфраструктуры предприятия //Вестник УрФО. Безопасность в информационной сфере. – 2019. – № 4 (34). – С. 35–44.

2. Basinya E.A. et al. System of a self-organizing virtual secure communication channel based on stochastic multi-layer encryption and overlay technologies. – 2022.

3. Wu H. et al. Real-time identification of VPN traffic based on counting Bloom filter and chained hash table from sampled data in high-speed networks // ICC 2022-IEEE International Conference on Communications. – IEEE, 2022. – P. 5070–5075.

УДК 004.056.55:519.24

А.В. КУЛИКОВА

АНО ВО «Университет Иннополис», Иннополис

АНАЛИЗ МЕТОДОВ ОБНАРУЖЕНИЯ ТОЧЕК ИЗМЕНЕНИЯ В ПОВЕДЕНЧЕСКИХ СИГНАЛАХ НА ОСНОВЕ БАЙЕСОВСКИХ МОДЕЛЕЙ ДЛЯ ИДЕНТИФИКАЦИИ СМЕНЫ СОСТОЯНИЙ ПОЛЬЗОВАТЕЛЯ В КРИПТОГРАФИИ

Работа посвящена математическому анализу байесовских методов обнаружения точек изменения в поведенческих временных рядах для непрерывной аутентификации. Формализована модель кусочно-стационарного процесса, введено апостериорное распределение над моментами изменения и доказаны условия его сходимости. Показана совместимость метода с криптографией: при принадлежности распределения экспоненциальному семейству обновления реализуемы через частично гомоморфное шифрование, а добавление шума по схеме дифференциальной приватности.

Поведенческие сигналы, такие как динамика набора текста, траектории мыши, сенсорные паттерны и др., отражают когнитивные и физиологические особенности пользователя. Их анализ позволяет реализовать непрерывную аутентификацию, выявляя моменты смены состояния, например, компрометацию сессии. Задача сводится к обнаружению точек изменения в кусочно-стационарном процессе (1).

$$\boldsymbol{x_t} \sim \boldsymbol{p}\big(\, \boldsymbol{x} \mid \boldsymbol{\theta}^{(k)} \,\big), \boldsymbol{t} \in (\boldsymbol{\tau_{k-1}}, \boldsymbol{\tau_k}], \tag{1}$$

где $\boldsymbol{\tau_k}$ −неизвестные моменты изменения, а $\boldsymbol{\theta(k)}$ – параметры поведенческого режима.

Для решения задачи используется рекуррентный байесовский подход Bayesian Online Change Point Detection (сокр. BOCPD), основанный на скрытой переменной $\boldsymbol{r_t = t - \tau}$ – длительности текущего сегмента. Апостериорное распределение обновляется по следующей формуле (2):

$$\boldsymbol{P(r_t \mid x_{1:t}) \propto P(x_t \mid x_{t-r_t:t-1}) \cdot P(r_t \mid r_{t-1}) \cdot P(r_{t-1} \mid x_{1:t-1})}, \tag{2}$$

где априори $P(\boldsymbol{r_t = 0 \mid r_{t-1}) = \lambda}$ задаёт геометрическое распределение моментов изменения. При условии, что $\boldsymbol{P(x_t \mid \theta)}$ принадлежит экспоненциальному семейству, обновление сводится к рекуррентному изменению достаточной статистики $\boldsymbol{s_t}$, что обеспечивает линейную вычислительную сложность $\boldsymbol{O(T)}$.

Также для решения поставленной задачи установлены условия корректности модели: Разделимость состояний: $\boldsymbol{KL}(\boldsymbol{p}(\cdot|\,\boldsymbol{\theta}^{(k)}) \parallel \boldsymbol{p}(\cdot|\,\boldsymbol{\theta}^{(k+1)})) \geq \boldsymbol{\delta} > 0$; Регулярность априора, где $\boldsymbol{\lambda}$ не слишком мало; Независимость внутри сегментов. При выполнении поставленных условий апостериорное распределение сходится к истинной точке изменения.

Поведенческие данные являются чувствительными, поэтому их обработка должна соответствовать GDPR [3] и ISO/IEC 24745 [4] в которых рассмотрены основные подходы, такие как гомоморфное шифрование [1] (если признаки $\boldsymbol{T}(\boldsymbol{x_t})$ линейны, обновление статистик $\boldsymbol{s_t}$ возможно в зашифрованном виде с использованием схем типа Пэйе) и дифференциальная приватность [2] (к статистикам добавляется шум $\boldsymbol{\eta_t} \sim \boldsymbol{Lap}(\boldsymbol{1}/\boldsymbol{\varepsilon})$. Метрика Вассерштейна между истинным и зашумлённым апостериорами ограничена (3)).

$$\boldsymbol{W_1}(\boldsymbol{P}, \boldsymbol{P}\sim) \leq \boldsymbol{C} \cdot \frac{\boldsymbol{\Delta s}}{\boldsymbol{\varepsilon}}. \quad (3)$$

Один из факторов, которые также стоит отметить - предлагается клиент-серверная архитектура, в которой клиент извлекает поведенческие признаки и шифрует достаточные статистики, сервер выполняет байесовское обнаружение точек изменения в зашифрованном виде, а результат возвращается клиенту для принятия решения. Такой подход полностью исключает доступ сервера к открытым биометрическим данным, что важно для соответствия требованиям конфиденциальности, включая стандарты GDPR и ISO/IEC 24745. Данный подход создаёт теоретический «мост» между байесовским машинным обучением и криптографией. Предложенный подход обеспечивает математически обоснованную, онлайн-совместимую и криптографически защищённую систему поведенческой аутентификации с формальными гарантиями точности и приватности.

Список литературы

1. Бабенко Л.К. и др. Защищенные вычисления и гомоморфное шифрование //Программные системы: теория и приложения. – 2014. – 25 с. – 2014.

2. Архипова А Б., Исаков И.В., Ершов Р.В. Методы обеспечения приватности в больших данных: аспекты информационной безопасности //Современное образование: интеграция образования, науки, бизнеса и власти. – 2022. – С. 52–56.

3. Денисов И.С., Ахматова Д.Р., Кабакова В.М. Сравнительная характеристика GDPR и российского законодательства о персональных данных //Экономика. Право. Общество. – 2020. – №. 1. – С. 21–27.

4. Bassit A. et al. Bloom Filter vs Homomorphic Encryption: Which approach protects the biometric data and satisfies ISO/IEC 24745? //2021 international conference of the biometrics special interest group (BIOSIG). – IEEE, 2021. – С. 1–6.

КИБ-2025

КИБЕРНЕТИКА
И ИНФОРМАЦИОННАЯ
БЕЗОПАСНОСТЬ

Направление

Информационно-аналитические системы безопасности

Руководитель секции – НОРКИНА А.Н., к.э.н., доцент,

директор ИФТЭБ НИЯУ МИФИ

УДК 004.51:004.8

В.А. УГЛЕВ

Московский университет МВД России имени В.Я. Кикотя

МЕТОДЫ ПИКТОГРАФИКИ ДЛЯ КОНЦЕНТРАЦИИ ДАННЫХ В АНАЛИТИЧЕСКИХ СИСТЕМАХ

В статье рассматриваются методы концентрации данных с помощью различных графических нотаций пиктографирования. Обсуждаются вопросы их применения в информационно-аналитических системах безопасности.

Результативность процедур интеллектуального анализа данных (ИАД) в информационных системах зависит не только от достоверности исходного массива и сложности проверяемых гипотез, но и от возможностей инструментальных средств концентрации данных. Чем сложнее объект, требующий свёртки данных, тем большей способностью к концентрации должны обладать возможности системы ИАД [1]. Особенно это важно, когда сам объект имеет множество количественных и качественных параметров. В информационно-аналитических системах безопасности это профили пользователей, модели их поведения, данные об объектах наблюдения (мониторинга) и пр. Рассмотрим такие средства когнитивной визуализации, как пиктографика, которые могут быть полезны при свёртке данных в аналитических системах безопасности.

Методы ИАД, ориентированные на визуализацию, включают в себя не только средства кластеризации и нейросетевой визуализации (например, метод эластичных карт [2]), но и различные графические нотации из раздела Data Visualization (часть Data Mining). Если упомянутые подходы (нейросети и кластеризация) не позволяют разворачивать исходные данные для ответа на вопрос «почему?» (происходит свёртка данных об объекте в гиперпространстве признаков в точку), то методы пиктографики из Data Visualization ориентированы на комплексную визуализацию данных с учётом деталей и неоднородного характера признаков [1].

Самыми простыми из них являются дашборды: они позволяют акцентировать внимание лица, принимающего решение, на проблемных моментах, но не позволяют осуществлять мониторинг сразу группы объектов. Другой подход: выражение комплексной оценки состояния объекта через близкое человеческому восприятию эмоции (метод фейкодера Джоунса) или лица, кодирующего в своих элементах разные параметры объекта анализа (метод лиц Чернова). Такой подход интересен

тем, что позволяет быстро сравнивать множество объектов, но он очень чувствителен к искажениям и диспропорциям, а также имеет сложности с выводом данных о динамике параметров [3]. Примером использования данного метода можно найти как для отражения уровня преступности в США [4], так и при мониторинге состояния объектов атомной промышленности [5].

Альтернативной группой методов для графической свёртки данных при пиктографировании является кодирование объектов в виде человеческих фигур. Начиная от модулора Ле Корбюзье и Тризкина [3], и оканчивая методом унифицированного графического воплощения активности (UGVA [3]). Последний метод интересен тем, что позволяет свёртывать данные как для статичных, так и для динамичных объектов, представляя их в виде групповой карты. В [6] приведен пример использования этой графической нотации для мониторинга работы сотрудников одного из подразделений корпорации «Росатом». Аналогичные образы можно получить при рассмотрении различных объектов, требующих обеспечения безопасности, мониторинга профилей активности пользователей по цифровому следу и пр.

Разработчики информационно-аналитических систем безопасности не просто нуждаются в эффективных модулях концентрации и визуализации состояния сложных объектов и их групп, но и в возможности свободно интегрировать такие модули в проекты. Для этого необходимо такие методы уметь использовать, а также иметь доступ к свободно-распространяемым версиям или реализовать их своими силами.

Список литературы

1. Han J., Kamber M., Pei J. Data mining concepts and techniques. The Morgan Kaufmann Series in Data Management Systems. 2011.

2. Gorban A., Zinovyev A. Fast and user-friendly non-linear principal manifold learning by method of elastic maps. Proceedings of the IEEE International Conference on Data Science and Advanced Analytics (DSAA), 2015, pp. 1–9. https://doi.org/10.1109/DSAA.2015.7344818.

3. Углев В.А. Поддержка процесса принятие решений с использованием нотации унифицированного графического воплощения активности (UGVA) // Вестник МГТУ им. Н.Э. Баумана. Сер. Приборостроение. – 2023. – № 3(144) – С. 125–140. https://doi.org/10.18698/0236-3933-2023-3-125-140.

4. Лица Чернова. [электронный ресурс]: режим доступа – https://ru.wikipedia.org/wiki/Лица_Чернова (дата обращения 24.10.2025).

5. Rosenfeld H., Moore S., Nost E., Roth R., Vincent K. Chernoff zombies. North America Cartographic Information Society, 2017(12).

6. Uglev V., Meshkov S., Kuznetsov M. Methodology of Complex Visual Representation of Human Activity Using Cognitive Visualization // Journal of Integrated Design and Process Science, 2024. vol. 27(3–4). pp. 184–199. https://doi.org/10.1177/10920617241289768.

УДК 343.98

Е.А. РАБЧЕВСКИЙ

IT компания ООО «СЕУСЛАБ», Пермь

МЕТОДИЧЕСКИЕ ОСНОВЫ ПРИМЕНЕНИЯ ТЕХНОЛОГИЙ OSINT В ПРАВООХРАНИТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ

В материале представлена комплексная методология применения OSINT технологий в правоохранительной деятельности. Проведение исследования обусловлено отсутствием в российской печати устоявшейся классификации служебных задач, при решении которых используются технологии OSINT. Предложенные различными авторами классификации, будучи ценными с точки зрения освещения отдельных аспектов применения OSINT в правоохранительной деятельности, пока не образуют единой системы [1–3]. Данное обстоятельство ведет к фрагментарному видению методов их решения, отсутствию комплексных методик, отсутствию обоснованных оценок сложности и стоимости технической реализации данных методик. На основе опыта создания и эксплуатации органами внутренних дел информационно-аналитической системы (Поисковая система «SEUS»), обобщен и классифицирован перечень задач, в решении которых эффективно применяются технологии OSINT, и соответствующих методов.

При попытке обобщения и классификации задач было предложено разделить их на три слоя.

Слой служебных задач, которые решаются различными аналитическими и техническими методами. Например, определение местонахождение разыскиваемых лиц, или выявление признаков противоправной деятельности, направленной на подрыв общественной безопасности, или установление личности объекта интереса и т.д. [4].

Слой подготовительных оперативно-аналитических задач. К таким можно отнести такие виды задач, как формирование поисковых признаков [5], погружение в информационную среду и т.д. Данные задачи зачастую игнорируются на практике, что приводит к низкой эффективности применения методов OSINT. А именно они определяют возможности качественной выборки оперативно-значимых материалов из первичных данных [6].

Отдельно выделен слой технических задач по сбору и первичной обработке исходных данных, решение которых осуществляется в автоматизированном режиме. На этом слое определяется номенклатура собираемой первичной информации, периодичность сбора этой информации, применяемые методы технической маскировки действий по

сбору данных, методы обработки первичной информации и хранения, и т.д. Практические сотрудники не задумываются о значимости данного этапа, вместе с тем подходы к реализации данного этапа значительно влияют на эффективность применения методов OSINT и стоимость соответствующих технических решений.

Разработанная методология обеспечивает систематизированный подход к внедрению OSINT в деятельность органов внутренних дел, включая и подготовку кадров и соответствующих методических материалов, технико-экономическое обоснование и создание и применение технических решений.

Список литературы

1. Фаниев П.А. Тихая разведка OSINT как способ получения криминалистически значимой информации //Научный портал МВД России. – 2023. – № 2 (62). – С. 82–87.
2. Иванов В.Ю. Использование OSINT в раскрытии и расследовании преступлений //Вестник Уральского юридического института МВД России. – 2023. – № 1 (37). – С. 62–66.
3. Батоев В.Б. О технологии поиска по открытым источникам «OSINT» в оперативно-розыскной деятельности //Вестник Уфимского юридического института МВД России. – 2023. – № 2 (100). – С. 66–71.
4. Минаев В.А. и др. Противодействие экстремистской идеологии в социальных медиа: математические модели и методы //Дальневост. юрид. ин-т МВД Россиии. – 2023. – С. 232.
5. Рабчевский Е.А., Анфалов А.В. Методические рекомендации по выявлению и оперативному анализу деструктивного контента в сети Интернет с помощью информационно-поисковых систем // Пермь, 2024. – 40 с.
6. Рабчевский Е.А., Анфалов А.В. Методические рекомендации по информационно-аналитической работе в мессенджере Telegram / Пермь, 2025 – 80 с.

УДК 004.9

К.А. МОЛОДЫКО, О.К. ГОЛОВНИН

Самарский национальный исследовательский университет им. академика С.П. Королева

АНАЛИЗ СОБЫТИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ С ИСПОЛЬЗОВАНИЕМ TREE-LSTM-ВЕКТОРОВ И LLM

В работе предложен гибридный подход для обнаружения аномальной активности в журналах событий информационной безопасности. Гибридный подход предполагает использование комбинации нейронных сетей и больших языковых моделей для обработки журналов событий, использующих стандартный формат Common Event Format. Проведены вычислительные эксперименты для проверки эффективности предложенного подхода, которые показали, что его использование позволяет реализовать более эффективное целевое решение. Результаты работы предназначены для использования в аналитических системах информационной безопасности.

Современные системы защиты информации генерируют огромное количество событий, которые являются основным источником информации для мониторинга рисков нарушения информационной безопасности, аудита и анализа инцидентов [1, 2]. Однако большой объём и разнообразие этих данных делают их аналитический анализ специалистом практически невозможным, а традиционные системы обнаружения и предотвращения вторжений, основанные на сигнатурах или статистических правилах, зачастую не способны выявить нетипичные угрозы [3]. В качестве альтернативы для работы с журналами событий выступают рекуррентные архитектуры нейросетей, предназначенные для построения векторных представлений с учётом их иерархической структуры [4].

В данной работе представлен гибридный подход к анализу журналов событий систем защиты информации, сочетающий векторизацию событий при помощи модели Tree-LSTM и классификацию их семантической значимости с использованием больших языковых моделей (LLM). В предложенном подходе извлеченные из журналов событий эмбеддинги формируются в компактные сводки, которые передаются в языковую модель для категоризации событий как нормальных или аномальных. В рамках проведенного исследования векторизация происходит без использования какой-либо специфической информации о семантике токенов, что снижает потенциальную точность модели. Все входные данные представлены в Common Event Format.

В ходе исследования проанализированы результаты, полученные традиционным подходом при отправке данных журналов событий в LLM, и результаты применения предложенного гибридного варианта. Получено распределение уверенности для верных (Correct) и ошибочных (Wrong) предсказаний. Гибридный подход продемонстрировал значительное улучшение в сравнении с традиционным, что подтверждается анализом ROC-кривой и AUC-метрикой, что позволяет сделать вывод о том, что предложенный подход обладает высокой обобщающей способностью и может быть адаптирован для различных сценариев использования.

Полученные результаты показали, что гибридный подход не только эффективнее в хранении и обработке данных, но и дает существенное увеличение показателей правильных классификаций. Поскольку предложенный подход оперирует информаций, представленной в стандартном формате Common Event Format, то он может быть масштабирован для применения в составе различных систем защиты информации.

Таким образом, предложенный подход не только обеспечивает высокую гибкость и обобщающую способность, но и позволяет реализовать более эффективное целевое решение, предназначенное для использования в аналитических системах информационной безопасности. Дальнейшие работы будут направлены на исследование влияния различных параметров модели на точность классификации и проведение экспериментов на более крупных наборах данных для подтверждения стабильности результатов.

Список литературы

1. Лубенцов, А.В. Синтез иерархической многоуровневой модели параметров для оценки эффективности системы защиты информации в условиях неопределенных данных / А.В. Лубенцов // Известия высших учебных заведений. Электроника. – 2024. – Т. 29; № 2. – С. 236–248.

2. Исхаков, А.Ю. Повышение эффективности систем защиты информации с помощью категоризации событий безопасности / А.Ю. Исхаков, С.Ю. Исхаков // Информационные и математические технологии в науке и управлении. – 2023. – № 2(30). – С. 152–164.

3. Котенко, И.В. Обнаружение атак и аномалий в контейнерных системах: подходы на основе сигнатур и правил / И.В. Котенко, М.В. Мельник // Искусственный интеллект и принятие решений. – 2025. – № 1. – С. 3–13.

4. Make it directly: Event extraction based on tree-LSTM and Bi-GRU / W. Yu [et al.] // IEEE Access. – 2020. – Vol. 8. – P. 14344–14354.

УДК 332(075.8)

А.И. ГУСЕВ

АО АКБ «Центрокредит», Москва
Национальный исследовательский ядерный университет «МИФИ», Москва

РОССИЙСКИЕ БАНКИ НАЧИНАЮТ ЭФФЕКТИВНО ПРОДВИГАТЬ ЗАЩИТУ ОТ ПРОДВИНУТОГО ФИШИНГА

Корпоративный и розничный блок российских банков начинает использовать особенности фишинговых атак на специфические социотехнические системы, представляющие их собственных целевых клиентов, как возможность эффективно продвигать не только услуги по их защите, но и более эффективно продавать и собственные банковские услуги. Для этого банк использует уже готовые наработки своего подразделения private banking в области вэйлинга по VIP-клиентам, причем не текущие, но и перспективные.

Заметное усиление и увеличение атак на VIP-клиентов российского private banking в последние годы напрямую связывается с активным использованием средств ИИ, позволяющим качественно модифицировать хорошо известный и неплохо изученный фишинг. Дело в том, что подобное усложнение снижает порог входа для реализации более обособленного и продвинутого вэйлинга (от whaling «охота на китов», нишевой фишинг нацеленный именно на VIP-клиентов). И не только для не слишком многочисленных и узкоспециализированных на этой нише хакеров-профи, сколько для неофитов, обычно выбирающих именно фишинг, из-за его простоты и изученности, как одно из перспективных начальных направлений обучения для своего последующего совершенствования.

На фоне непрерывного усиления атак на российский бизнес, соответствующий рост числа неофитов уже вполне закономерно приводит к тому, что и сам фишинг начинает усложняться, постепенно эволюционируя в сторону уже существующих методик более продвинутого вэйлинга. При этом последние можно адаптировать и для атак для менее состоятельных клиентов, уверенно расширяя целевую базу атак, отходом от узкой группы VIP-клиентов к менее состоятельным, как для профи, так и для набравшихся определенного опыта неофитов. Этому, еще больше способствует и тот факт, что целевой VIP-клиент-собственник российского бизнеса привык использовать механизм корпоративного дробления своей холдинговой структуры на группу связанных компаний МСБ, с уязвимостями, типичными для последних.

Ну а чем больше атак на российский бизнес в лице его типичного и массового представителя в виде МСБ, со стороны многочисленных неофитов, начинающих бить по уже заметным площадям, то тем выше вероятность (и это мы уже наблюдаем [1]) фишинговой атаки и на VIP-клиентов, причем уже близкой по сложности к вэйлингу, хотя и со стороны неофитов. Важно, что совершенствование средств ИИ, существенно облегчает им проведение таких непростых атак. На предварительном этапе OSINT благодаря ML превращается во вполне доступный «социальный инжиниринг-лайт».

Поэтому на фоне постоянных атак злоумышленников банк получил вполне убедительный аргумент, чтобы непрерывно и обоснованно, продвигать киберкультуру своим клиентам. Прямые угрозы, переход на более продвинутую систему управления рисками, обеспечения непрерывности бизнеса в условиях новых вызовов, все это не только сейчас, но в ближайшие годы тот самый комплекс услуг, эффективно продвигаемый и продаваемый банком через продуктовый ряд своих контрагентов в сфере ИБ. Но не только. Одновременно с этим, можно не менее эффективно, отходя от схем процентного распределения дохода, продвигать и непосредственные банковские услуги по оптимизации структуры бизнеса клиента. Причем уже готовыми наработками private banking, но не только прошлыми, но и текущими, а главное и перспективными. Что постепенно и начинает реализовываться в корпоративном и розничном блоке российских банков, которые начинают использовать особенности атак на специфические социотехнические системы, представляющие их собственных целевых клиентов, как возможность эффективно продвигать не только услуги по их защите, но и более эффективно продавать и собственные банковские услуги.

Список литературы

1. Gusev, A. New cyberattacks vectors of Russian critical infrastructure enterprises: Domestic private banking sector view within AI protection methods. Procedia Computer Science,213 pp. 391–399, 2022.

2. Гусев А.И. Растущий интерес российского private banking к кибербезопасности нуждается в осмыслении. ПЛАС, 3(311), 2024. https://plusworld.ru/journal/2024/plus-3-2024/rastushchiy-interes-rossiyskogo-private-banking-k-kiberbezopasnosti-nuzhdaetsya-v-osmyslenii/

УДК 004.056.5:004.89:005.334

Н.С. ИШНЯКОВА, В.С. КИРЕЕВ

Национальный исследовательский ядерный университет «МИФИ», Москва

ИНФОРМАЦИОННО-АНАЛИТИЧЕСКИЕ МЕТОДЫ ПОВЫШЕНИЯ УСТОЙЧИВОСТИ И БЕЗОПАСНОСТИ БЮДЖЕТИРОВАНИЯ НА МЕТАЛЛУРГИЧЕСКИХ ПРЕДПРИЯТИЯХ

В условиях цифровой трансформации и роста киберрисков важно создавать доверенные информационно-аналитические системы, обеспечивающие безопасность финансовых процессов. В работе рассмотрены подходы к автоматизации бюджетирования на металлургических предприятиях с применением ИИ, ERP, BI и RPA. Методы ICE, RICE и WSJF использованы для оценки влияния, рисков и эффективности решений. Результаты показывают, что интеграция ИИ в ERP повышает прозрачность, снижает ошибки и формирует основу защищённой аналитической среды предприятий критической инфраструктуры.

Актуальность ИИ в бюджетировании связана с высокой неопределённостью финансовых прогнозов. По данным PwC, 80% компаний сталкиваются с неточностями, что ведёт к рискам [1]. В металлургии, где цены на сырьё колеблются до 40% в год, точное планирование критично. Исследования McKinsey показывают, что ИИ снижает отклонения на 20–30%, а автоматизация с ERP, BI и RPA ускоряет согласование бюджета на 50% [2]. В условиях цифровой трансформации ИИ становится необходимым инструментом.

Цель работы – исследовать подходы к автоматизации бюджетирования и определить оптимальное решение с учетом методов ICE, RICE и WSJF.

Результаты помогут предприятиям выбирать эффективные способы автоматизации, снижать риски и повышать гибкость финансового планирования.

Для выбора оптимального подхода к внедрению ИИ в ERP, BI и RPA, в части согласования бюджета, необходимы обоснованные методы оценки. В исследовании применяются ICE, RICE и WSJF, позволяющие сравнить решения по влиянию, затратам и эффективности. Оценки, представленные в табл. 1, основаны на анализе систем, экспертном мнении автора и данных исследований PwC Digital IQ 2020, McKinsey и SAP [3]. В данной таблице все параметры (кроме Reach) оценены по субъективной шкале (1–10), а Reach – в процентах охвата числа пользователей. Также

приведено ранжирование по трём методикам для выявления сильных и слабых сторон каждого подхода.

Таблица 1. Оценка и сравнение решений по ключевым параметрам

Параметр\ Решения	ERP	RPA	BI	Спец. ПО
Impact (Влияние)	9	8	7	7
Confidence (Уверенность)	9	7	7	5
Ease (Легкость внедрения)	5	9	6	4
Reach (Охват пользовател.), %	100	50	80	60
Effort (Сложность)	5	5	7	8
Time Criticality (Срочность)	10	8	6	7
Risk Reduction (Снижение рисков)	9	7	6	6
Job Size (Размер задачи)	5	5	7	8
ICE (Impact × Confidence × Ease)	405	**504**	294	140
RICE ((Reach × Impact × Confidence) / Effort)	**1620**	560	560	262
WSJF ((Value + Time Criticality + Risk Reduction) / Job Size)	**5,6**	4,6	2,8	2,5

Анализ показывает, что ERP-системы лидируют по RICE и WSJF, подтверждая их стратегическую значимость. Они охватывают больше пользователей, снижают риски и повышают эффективность.

RPA-системы с наивысшим баллом по ICE оптимальны для быстрой автоматизации рутинных задач.

Однако наиболее эффективным решением для металлургических предприятий является внедрение ERP-систем с элементами искусственного интеллекта, обеспечивающих прозрачность, снижение рисков и интеграцию с аналитическими инструментами BI и RPA. Это формирует основу для создания устойчивой и безопасной информационно-аналитической среды управления финансами.

Список литературы

1. PwC. Digital IQ 2020 Russia. [Электронный ресурс]. – Режим доступа: https://www.pwc.ru (дата обращения: 21.10.2025).

2. Секреты успешного масштабирования аналитики [Электронный ресурс] // AnalytikaPlus. – URL: https://analytikaplus.ru/mckinsey-sekrety-uspeshnogo-masshtabirovaniya-analitiki/ (дата обращения: 21.10.2025).

3. SAP. Примеры использования AI и Big Data в металлургии. [Электронный ресурс]. – Режим доступа: https://www.sap.com (дата обращения: 21.10.2025).

УДК 004.056.5:004.8:553.49

А.Ф. КУКЕБАЕВ, В.С. КИРЕЕВ

Национальный исследовательский ядерный университет «МИФИ», Москва

ИНТЕЛЛЕКТУАЛЬНЫЕ МЕТОДЫ И ИНСТРУМЕНТЫ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ДЛЯ РЕИНЖИНИРИНГА ПРОЦЕССА ОЦЕНКИ ГЕОЛОГИЧЕСКИХ ЗАПАСОВ УРАНА

Рассматривается использование методов и инструментов искусственного интеллекта (ИИ) для повышения эффективности процесса оценки геологических запасов урана. Традиционные геостатистические подходы ограничены по точности и требуют значительных ресурсов. Внедрение ИИ-моделей, таких как Random Forest и сверточные нейронные сети, позволяет повысить точность прогнозов, сократить временные затраты и автоматизировать интерпретацию геофизических данных. Цель исследования – создание интегрированного подхода, объединяющего искусственный интеллект и традиционные методы геостатистики для оптимизации оценки запасов урана [1].

Оценка геологических запасов урана является ключевым элементом управления минерально-сырьевыми ресурсами и стратегического планирования в атомной отрасли. Традиционные методы (геостатистика, вариограммы, кригинг) сохраняют эффективность, однако требуют значительных объёмов данных и ручной интерпретации, что повышает риск ошибок при ограниченной разведанности месторождений [2]. Использование методов ИИ направлено на устранение этих ограничений и повышение точности оценки.

Эффективность внедрения ИИ подтверждена современными исследованиями. По данным W. Kong и соавт. (2024), применение алгоритма Random Forest при моделировании перспективных зон урана в бассейне Эрлиан (Китай) обеспечивает точность прогнозов до 92%, что существенно превосходит традиционные геостатистические методы (70–75%) (рис. 1) [3]. Обзоры Mahboob M.A. et al. (2022) и Jooshaki M. et al. (2021) подтверждают рост эффективности обработки геологических данных и высокую устойчивость ИИ-алгоритмов к шуму и неполноте данных по сравнению с кригингом [4]. Важным направлением реинжиниринга является интеграция аналитических и визуализационных инструментов в единую экосистему, обеспечивающую обновление геологических моделей на основе данных бурения, спутникового мониторинга и лабораторных анализов. Такой подход повышает

прозрачность и управляемость решений, снижая влияние человеческого фактора [5].

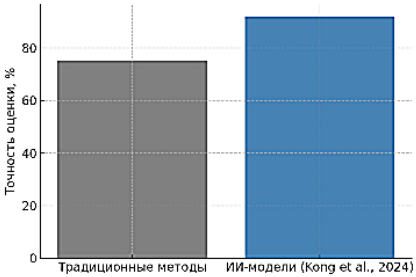


Рисунок 1. Сравнение точности методов оценки запасов урана [Электронный ресурс]. – URL: https://www.mdpi.com/2075-163X/14/2/128 (дата обращения: 23.10.2025)

Исследование представляет интегрированный подход, объединяющий методы искусственного интеллекта для реинжиниринга процесса оценки геологических запасов урана. Предложено использование интерпретируемых ИИ-моделей для анализа геолого-геофизических данных, что повышает точность, скорость и воспроизводимость результатов, а также снижает неопределённость и издержки оценки. Интеграция алгоритмов машинного обучения формирует основу интеллектуальной платформы поддержки решений в горнодобывающей отрасли. Дальнейшее развитие связано с внедрением облачных вычислений, квантовых сенсоров и AutoML-технологий для автоматизации построения и обновления геологических моделей [5, 6].

Список литературы

1. IAEA. Digital and AI Innovations in Mining for Sustainable Uranium Exploration [Электронный ресурс]. – Vienna: IAEA, 2022. – URL: https://www.iaea.org/publications (дата обращения: 23.10.2025).
2. Goodfellow I., Bengio Y., Courville A. Глубокое обучение. – MIT Press, 2016.
3. Kong W., Li Q., Liu X., et al. Machine Learning Based Uranium Prospectivity Mapping and Model Explainability Research // Minerals (MDPI). – 2024. – Т. 14, № 2. – С. 128. – URL: https://www.mdpi.com/2075-163X/14/2/128 (дата обращения: 23.10.2025).
4. Jooshaki M., Nad A., Michaux S. A Systematic Review on the Application of Machine Learning in Exploiting Mineralogical Data in Mining and Mineral Industry // Minerals (MDPI). – 2021. – Т. 11, № 8. – С. 816. – URL: https://www.mdpi.com/2075-163x/11/8/816 (дата обращения: 23.10.2025).
5. Johnson R., White D. Modernizing Mining Software: A Hybrid Approach // Mining Journal. – 2024. – Т. 22, № 1. – С. 89–94.
6. Mahboob M.A., Rahman M., Sadeghian A. Review of Machine Learning Based Mineral Resource Estimation // Natural Resources Research. – 2022. – Т. 31, № 6. – С. 2675–2690.

УДК 004.056

Д.Н. КАЛАШНИКОВ, Е.В. МАТРОСОВА

Национальный исследовательский ядерный университет «МИФИ», Москва

УСОВЕРШЕНСТВОВАНИЕ ПРОЦЕССА УЧЕТА ЗАКАЗОВ И ИССЛЕДОВАНИЙ ПРОБ УРАНА С ПРИМЕНЕНИЕМ МЕТОДОВ РАЗРАБОТКИ БЕЗОПАСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

В статье рассматривается подход к повышению безопасности и надежности системы учёта заказов и исследований рудных проб урана в химико-физической лаборатории. С учётом высокой степени конфиденциальности и критичности данных ядерного анализа предложена методология разработки безопасного программного обеспечения, основанная на принципах SSDLC (Secure Software Development Lifecycle).

Постановка задачи. Процесс обработки и хранения данных о пробах урана требует строгого соблюдения норм информационной и радиационной безопасности. На практике нередко наблюдаются проблемы, связанные с отсутствием системного контроля доступа, незащищёнными каналами передачи данных и рисками несанкционированного изменения результатов исследований [1]. Целью работы является усовершенствование системы учёта лабораторных заказов и результатов анализа проб урана с использованием принципов безопасной разработки программного обеспечения.

Пути решения. В качестве решения предложен комплексный подход, включающий следующие направления:

1. Анализ угроз и моделирование рисков – выявление уязвимостей на этапах регистрации, хранения и передачи данных между подразделениями лаборатории и смежными организациями.

2. Безопасное проектирование – реализация модульной архитектуры с разграничением прав пользователей (лаборант, аналитик, инженер, руководитель проекта), принципом минимальных привилегий и контролем критических операций.

3. Шифрование и защита данных — использование криптографических алгоритмов AES-256 и RSA-2048 для защиты данных проб и протоколов испытаний, а также внедрение безопасных каналов обмена (TLS 1.3).

4. Аутентификация и контроль доступа – применение многофакторной аутентификации и ролевой модели безопасности с журналированием всех действий пользователей.

5. Тестирование и аудит – использование инструментов статического анализа исходного кода (SonarQube, OWASP Dependency-Check) и регулярное проведение тестов на проникновение.

6. Мониторинг и инцидент-менеджмент – создание защищённого журнала аудита с функцией автоматического оповещения о подозрительных действиях и аномалиях.

Новые идеи и результаты. Разработанный прототип системы обеспечивает разграничение доступа на уровне заказов и данных исследований в среде химико-физической лаборатории, специализирующейся на исследовании проб урана. Система обеспечивает сквозное шифрование данных, автоматический контроль целостности записей и отслеживание цепочки действий пользователя. [2]. Реализованы сценарии для различных категорий пользователей – от операторов пробоподготовки до инженеров-аналитиков и руководителей подразделений. Такой подход позволил оптимизировать маршрутизацию данных и сократить время обработки заказов. Кроме того, интеграция с существующими лабораторными измерительными комплексами позволила автоматизировать передачу результатов анализов, снизив влияние человеческого фактора и минимизировав вероятность искажения данных.

Заключение

Интеграция методов безопасной разработки в систему учёта лабораторных заказов и исследований проб урана позволяет достичь высокого уровня информационной защиты, минимизировать человеческий фактор и обеспечить соответствие требованиям отраслевых стандартов по кибербезопасности. Выводы.

1. Применение SSDLC позволяет встроить контроль безопасности в каждый этап разработки и эксплуатации лабораторных систем.

2. Реализация шифрования, многофакторной аутентификации и разграничения прав доступа повышает доверие к результатам исследований.

3. Внедрение механизмов мониторинга и аудита способствует раннему выявлению инцидентов и минимизации последствий возможных атак.

4. Разработанный подход может быть масштабирован на другие виды лабораторий, работающих с чувствительными материалами.

Список литературы

1. OWASP Foundation. OWASP Secure Software Development Lifecycle Project, 2024.

2. ISO/IEC 27034-1:2023. Information technology – Security techniques – Application security.

УДК 004.056

Д.Т. ЖАКСЕЛЕКОВА
Научный руководитель – к.т.н., доцент В.Д. КОЛЫЧЕВ
Национальный исследовательский ядерный университет «МИФИ», Москва

ИНФОРМАЦИОННО-АНАЛИТИЧЕСКАЯ СИСТЕМА БЕЗОПАСНОСТИ НА БАЗЕ ИИ ДЛЯ УСТОЙЧИВОЙ ЭКСПЛУАТАЦИИ ЭНЕРГООБОРУДОВАНИЯ НА ПРИМЕРЕ АО «НАК «КАЗАТОМПРОМ»

Рассматривается информационно-аналитическая система безопасности (ИАСБ) на базе искусственного интеллекта для устойчивой эксплуатации энергооборудования. На примере АО «НАК «Казатомпром» показано, что интеграция ИИ-алгоритмов со SCADA системой и оснащение погружных насосных агрегатов частотно-регулируемыми приводами (ЧРП) позволяет снизить энергопотребление на 15–20%, сократить аварийные ремонты на 45% и обеспечить годовую экономию 3,58 млрд тг. Особое внимание уделено мерам киберустойчивости: сегментации сетей, контролю качества данных и переобучению моделей.

Постановка задачи

Цель исследования – разработка подхода к внедрению ИАСБ на базе ИИ для проекта по модернизации энергооборудования на уранодобывающих предприятий.

Задачи:

– интеграция предиктивных алгоритмов в систему управления насосным парком, оценка экономической эффективности;

– построение защищённого контура сбора и анализа данных;

– определение рисков и мер их снижения.

Методы

ИАСБ реализуется на базе непрерывного мониторинга параметров насосного парка (температура, вибрация, давление, расход, электропотребление). Данные собираются с IoT-датчиков и передаются через ПЛК в SCADA систему.

Для анализа используются алгоритмы машинного обучения: LSTM и RNN для оценки остаточного ресурса, автоэнкодеры для обнаружения аномалий, регрессионные модели для диагностики [2].

Кибербезопасность обеспечивается сегментацией сетей OT/IT, односторонними шлюзами, системой контроля доступа, процедурами data

governance. Для управления жизненным циклом моделей применяется MLOps, включающий контроль версий и регулярное переобучение [3].

Результаты

На примере модернизации насосного парка АО «НАК «Казатомпром» (4655 единиц) показано, что сочетание предиктивной аналитики насосного оборудования и ИАСБ обеспечивает снижение эксплуатационных затрат и повышает устойчивость работы ИИ-алгоритмов.

Экономические эффекты в результате реализации проекта по модернизации насосного оборудования:

– годовая экономия составила 3,58 млрд тг, включая 2,51 млрд тг за счёт снижения энергопотребления и 1,06 млрд тг за счёт сокращения ремонтов;

– NPV проекта при ставке дисконтирования 17% составила 4,68 млрд тг., ROI – 164%, срок окупаемости – 1,9 года.

Пилотные испытания на руднике «Западный Мынкудук» подтвердили рост энергоэффективности на 15–20% и сокращение аварийных простоев на 40%. ИАСБ обеспечило защиту каналов SCADA, контроль телеметрии и устойчивость прогнозных моделей, что снизило вероятность некорректных прогнозов и киберинцидентов.

Заключение

Интеграция предикативной аналитики и ИАСБ на базе ИИ позволяет достичь значимой экономии и повышения энергоэффективности при одновременном обеспечении киберустойчивости.

Проект модернизации насосного парка АО «НАК «Казатомпром» подтверждает, что снижение энергопотребления и сокращение ремонтов возможно при функционировании алгоритмов в защищённой цифровой среде. ИАСБ становится необходимым инструментом для устойчивой эксплуатации энергооборудования уранодобывающей отрасли.

Список литературы

1. АО «НАК «Казатомпром». Годовой отчет по цифровизации насосного оборудования. – Астана: Казатомпром, 2024. – 50 с.

2. US Department of Energy. Artificial Intelligence Strategy. – Washington: DOE, 2025. – 120 p.

3. NIST SP 800-82. Guide to Industrial Control Systems (ICS) Security. – Gaithersburg : NIST, 2022. – 250 p. DOI: 10.6028/NIST.SP.800-82r3.

УДК 004.056

Е.О. РОДИОНОВА, А.В. ФУРСЕНКО, Ю.Э. ПАВЛЕНКО

МИРЭА - Российский технологический университет», Москва

ТЕХНОЛОГИИ БОЛЬШИХ ДАННЫХ ДЛЯ КОРРЕЛЯЦИИ СОБЫТИЙ БЕЗОПАСНОСТИ НА ОСНОВЕ НЕЙРОННЫХ СЕТЕЙ

В статье рассматриваются современные подходы к применению технологий больших данных (Big Data) в задачах корреляции и анализа событий информационной безопасности с использованием нейронных сетей. Акцент сделан на преимуществах машинного обучения для выявления сложных закономерностей в больших объемах логов и событий, что существенно повышает эффективность обнаружения угроз и реагирования.

Введение

В условиях растущего объема киберугроз и усложнения атак традиционные методы анализа событий безопасности зачастую становятся недостаточно эффективными. Современные корпоративные ИБ-системы генерируют огромные потоки данных – журналы доступа, системные логи, сообщения об инцидентах, сетевой трафик [1]. Эффективный анализ и корреляция этих данных требуют применения технологий больших данных и интеллектуальных алгоритмов, способных выявлять скрытые взаимосвязи и аномалии [2].

Роль технологий больших данных в ИБ

Технологии Big Data обеспечивают масштабируемость хранения и обработки огромных объемов разнообразных данных в реальном времени. Платформы типа Hadoop, Spark, Kafka позволяют интегрировать данные из разнородных источников и выполнять комплексный анализ с минимальными задержками [1–2]. Это создаёт основу для построения системы корреляции событий, которая агрегирует и нормализует данные, подготавливая их для дальнейшего интеллектуального анализа [3].

Использование нейронных сетей для корреляции

Нейронные сети, особенно их глубинные архитектуры, успешно применяются для выявления сложных паттернов и аномалий в данных безопасности. Обучение на исторических данных позволяет нейросетям создавать модели нормального поведения и обнаруживать отклонения, характерные для атак или компрометаций [2].

В частности, рекуррентные нейронные сети (RNN) и их разновидности, такие как долгая краткосрочная память (LSTM), эффективны для анализа временных последовательностей событий. Свёрточные нейронные сети (CNN) применимы для извлечения признаков из структурированных логов и сетевых пакетов [2].

Корреляция с использованием нейросетей позволяет объединять связанные события из различных источников, повышая точность выявления сложных и целенаправленных атак.

Преимущества использования нейросетей и Big Data для корреляции безопасности:

1. Автоматизация выявления сложных угроз с минимальным вмешательством оператора.
2. Высокая адаптивность и способность обучаться на новых данных.
3. Возможность обработки разнородных и не консистентных данных.

В то же время вызовы включают необходимость большой обучающей выборки, высокую вычислительную нагрузку, сложность интерпретации решений и риски ложных срабатываний, что требует дополнительной настройки и верификации моделей [3].

Заключение

Интеграция технологий больших данных и нейронных сетей открывает новые горизонты в аналитике информационной безопасности. Современные решения позволяют значительно повысить эффективность корреляции событий, своевременно обнаруживать сложные атаки и минимизировать ущерб. Перспективы развития связаны с улучшением алгоритмов интерпретации, снижением вычислительных затрат и расширением возможностей автоматизации.

Список литературы

1. Котенко И.В., Федорченко А.В., Саенко И.Б., Кушнеревич А.Г. Технологии больших данных для корреляции событий безопасности на основе учёта типов связей. Вопросы кибербезопасности. 2017. № 5(24). с. 1–5. DOI: 10.21681/2311-3456-2017-5-2-16.

2. Макаров И.С., Райков А.В., Казанцев А.А., Нехаев М.В., Романов М.А. Применение нейросетей для анализа больших данных в реальном времени. Программные системы и вычислительные методы. 2025. № 2, с. 134–145. DOI: 10.7256/2454-0714.2025.2.73651 – EDN: DUSRKQ.

3. Новикова Е.С., Бекенева Я. А., Шоров А. В., Федотов Е. С. Обзор алгоритмов корреляции событий безопасности для обеспечения безопасности облачных вычислительных сред. Информационно-управляющие системы. 2017. № 5. с. 95–97. ISSN 1684-8853.2017.5.95. DOI: 10.15217.

УДК 004.056

В.А. РЫЧКОВ, А.Н. НИКИШИН,
Е.Е. ЧЕРВЯКОВ, А.М. КУТАРЁВ

Национальный исследовательский ядерный университет «МИФИ», Москва

ОБЗОР ПЕРСПЕКТИВНЫХ ТЕХНОЛОГИЙ ПОЛУЧЕНИЯ ЭНЕРГИИ ДЛЯ ПИТАНИЯ МАЛОГАБАРИТНЫХ НОСИМЫХ ЭЛЕКТРОННЫХ УСТРОЙСТВ

Цель данной работы привлечь внимание специалистов в области информационной безопасности к современному состоянию и перспективам развития средств технической разведки, как к важнейшему элементу ведения конкурентной разведки. В обзоре рассмотрены не только достижения ученых и инженеров в области беспроводной передачи электрической энергии, а также показаны демаскирующие признаки, сопутствующие использованию новых технологий.

В современном мире конкурентное противостояние достигает особой остроты и может приводить к использованию методов и средств промышленного шпионажа. Порой перспективы получения огромной прибыли или угроза потери бизнеса заставляют предпринимателей идти на отчаянные шаги, использовать незаконные методы получения информации. Такие методы подразумевают, в том числе, применение конкурирующими сторонами технических средств разведки (ТСР).

Как известно ни одно электронное устройство не обходится без источника электрической энергии.

В свою очередь, применение конкретного ТСР во многом зависит от планируемой продолжительности получения информации с использованием указанного средства, т.е. от типа разведки (рис. 1).

Планирование продолжительности ведения разведки определяется задачами основного бизнес процесса, что в конечном счете определяет необходимость использования того или иного источника питания для обеспечения соответствующей продолжительности работы ТСР.

Среди направлений получения электроэнергии, разрабатываемых в настоящее время в научных лабораториях мира, можно выделить следующие:

1) беспроводная передача энергии;
2) развитие химических источников тока многоразового действия;
3) преобразование тепла человеческого тела в электрическую энергию;
4) преобразование механической энергии в электрическую.

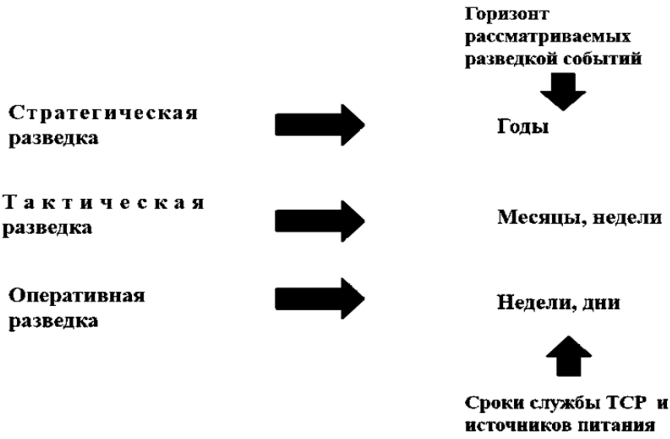


Рис. 1. Виды разведки

Каждому из приведённых выше направлений соответствуют определенные демаскирующие признаки получения и использования электрической энергии для работы ТСР.

Заключение

Мониторинг открытых источников информации позволяет следить за развитием науки и техники, выявляя те, которые потенциально могут быть использованы конкурентами.

Для успешного противодействия нечестной конкурентной борьбе, специалист по информационной безопасности должен знать демаскирующие признаки всех составляющих ТСР, в том числе основные параметры, принцип работы существующих и перспективных источников энергии.

Список литературы

1. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена заместителем директора ФСТЭК России 15 февраля 2008 г.

2. Меньшаков Ю.К. Теоретические основы технических разведок. Изд-во МГТУ им. Н.Э. Баумана, 2008. – 536 с.

УДК 004.056

В.А. РЫЧКОВ, А.Н. НИКИШИН,
Е.Е. ЧЕРВЯКОВ, А.М. КУТАРЁВ

Национальный исследовательский ядерный университет «МИФИ», Москва

ПЕРСПЕКТИВЫ РАЗВИТИЯ НОСИМЫХ ТЕХНИЧЕСКИХ СРЕДСТВ РАЗВЕДКИ НА ПРИМЕРЕ ГРАЖДАНСКОЙ ОДЕЖДЫ

В целях ознакомления специалистов по информационной безопасности, с потенциальными угрозами применения технических средств разведки, встроенных в высокотехнологичных моделях одежды, авторами был проведен мониторинг открытых источников информации. Ознакомление с представленными материалами даёт представление о возможных демаскирующих признаках технических средств разведки и позволит совершенствовать защиту информационной системы.

Одним из распространенных способов получения информации ограниченного доступа в ходе ведения конкурентной разведки является использование технических средств разведки (ТСР). Для реализации несанкционированного доступа к защищаемой информации применяется камуфлирование ТСР в предметы повседневного использования. ТСР представляет собой сложное электронное устройство. Структурная схема типичного ТСР представлена на рис. 1.

Рис. 1. Структурная схема типичного ТСР

В качестве датчиков физических полей могут быть использованы микрофоны, фото и видеокамеры [1], антенны [2]. Элемент питания – это различные по устройству источники электрической энергии. Блок накопления и сжатия информации представляет собой малогабаритное полупроводниковое устройство с малым потреблением энергии. [3] Устройство управления может быть реализовано в виде одной кнопки.

В настоящее время некоторые организации, в рамках противодействия угрозам информационной безопасности, вводят запрет на использование в служебных помещениях смартфонов и других высокотехнологичных устройств, имеющих признаки ТСР.

Однако противодействию угрозе использования ТСР, закамуфлированных в одежде [4], по нашему мнению, уделяется недостаточно внимания. В тоже время развитие микроэлектроники и легкой промышленности привело к появлению нового сектора экономики на стыке этих отраслей – создание одежды с интегрированными электронными устройствами, при этом на международном рынке уже доступен большой ассортимент «умной одежды», от очков Ray-Ban с прямой интеграцией искусственного интеллекта [5] до куртки с рукавами, который распознают каждый жест человека [6].

Технологии создания такой одежды, могут использоваться при создании экипировки с интегрированными в неё ТСР.

Заключение

Описанная угроза требует от сотрудников, ответственных за обеспечение информационной безопасности организации, соответствующих компетенций. В качестве средств выявления таких ТСР могут быть использованы рентгеновские и высокочастотные сканеры.

Список литературы

1. Intel показала умные очки, в которых изображение транслируется на сетчатку глаза [Электронный ресурс] https://habr.com/ru/post/410157/ (дата обращения: 14.10.2025)
2. Антенна, вшитая прямо в одежду [Электронный ресурс] URL: https://www.altsyn.com/energonovosti/168/antenna-v-odezhde (дата обращения: 14.10.2025)
3. Новые растяжимые литий-ионные батареи можно печатать на одежде [Электронный ресурс] https://scientificrussia.ru/articles/novye-rastazimye-litij-ionnye-batarei-mozno-pecatat-na-odezde (дата обращения: 14.10.2025)
4. Умная одежда будущего [Электронный ресурс] https://statusmen.ru/gear-tech/smart-clothes (дата обращения: 14.10.2025)
5. Ray-Ban Meta Glasses [Электронный ресурс] https://www.ray-ban.com/usa/ray-ban-meta-ai-glasses (дата обращения: 14.10.2025)
6. Meet the jacket that keeps you connected and on the move [Электронный ресурс] http://global.levi.com/jacquard/jacquard-with-buy-link.html (дата обращения: 14.10.2025)

УДК 004.056

В.А. РЫЧКОВ, Д.М. КАЗАНОВСКИЙ, П.С. УРЖУМОВ

Национальный исследовательский ядерный университет «МИФИ», Москва

СОВРЕМЕННЫЕ УГРОЗЫ УТЕЧКИ ИНФОРМАЦИИ ПО КАНАЛАМ ПОБОЧНЫХ ЭЛЕКТРОМАГНИТНЫХ ИЗЛУЧЕНИЙ

Статья систематизирует современные угрозы утечки информации по каналам побочных электромагнитных излучений (ПЭМИ). Проанализированы методы перехвата данных с видеодисплеев сверхвысокой четкости на расстоянии до 80 метров, идентификации процессов в смартфонах и IoT-устройствах, а также перехвата конфиденциального трафика через USB-интерфейсы.

Постановка задачи:

1. Провести анализ современных исследований, демонстрирующих возможности перехвата информации через каналы ПЭМИ.
2. Изучить методы восстановления данных с дисплеев UHD и Full HD, а также перехвата информации с USB-устройств.
3. Разработать рекомендации по защите от утечек через каналы ПЭМИ.

Современные электронные устройства, включая компьютеры, смартфоны и IoT-устройства, активно используются для обработки и передачи конфиденциальной информации. Однако они также являются источниками побочных электромагнитных излучений (ПЭМИ), которые могут быть перехвачены и использованы для восстановления обрабатываемых данных. Данная статья посвящена исследованию угроз, связанных с утечкой информации через каналы ПЭМИ, и анализу современных методов перехвата, включая восстановление изображений с дисплеев, идентификацию программных процессов и перехват данных с периферийных устройств.

Анализ современных исследований показал, что угрозы, связанные с ПЭМИ, эволюционируют. Если ранние работы демонстрировали возможность перехвата изображений с дисплеев на коротких расстояниях с помощью простого оборудования, то современные методы позволяют восстанавливать видеоинформацию с дисплеев UHD и Full HD на расстоянии до 80 метров в условиях городских помех.

Ключевые направления исследований включают:

– восстановление изображений с дисплеев с использованием направленных антенн и программно-определяемых радиоустройств (SDR);

– анализ электромагнитных излучений смартфонов и IoT-устройств для идентификации программных процессов с помощью машинного обучения;

– перехват данных с периферийных устройств, таких как USB-клавиатуры и кард-ридеры, через электромагнитные наводки.

Эксперименты подтвердили, что даже устройства с высоким уровнем защиты могут быть уязвимы. Например, перехват данных через перекрестные наводки в USB-концентраторах возможен даже при использовании кабелей без линий данных.

Заключение

Исследование показало, что угрозы, связанные с каналами ПЭМИ, остаются актуальными и требуют комплексного подхода к защите. Традиционные меры, такие как экранирование и фильтрация, не всегда эффективны. Для противодействия утечкам необходимо:

– разрабатывать стандартизированные методики оценки защищенности оборудования;

– внедрять аппаратно-программные решения, устойчивые к атакам через каналы ПЭМИ;

– использовать машинное обучение для мониторинга аномальных излучений и выявления скрытых закладок.

Дальнейшие исследования должны быть направлены на создание эффективных средств защиты, обеспечивающих конфиденциальность данных в условиях роста числа подключенных устройств и увеличения их производительности.

Список литературы

1. W van Eck, Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?, North-Holland Computers & Security 4 (1985) p. 269-286.

2. P. de Meulemeester, B. Scheers and G. A. E. Vandenbosch, "Eavesdropping a (Ultra-)High-Definition Video Display from an 80 Meter Distance Under Realistic Circumstances," 2020 IEEE International Symposium on Electromagnetic Compatibility & Signal/Power Int.

УДК 004.056

Н.С. НАУМОВА, В.А. РЫЧКОВ

Национальный исследовательский ядерный университет «МИФИ», Москва

МЕТОДЫ ПОИСКА ИНСАЙДЕРА В КОРПОРАТИВНЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

Целью работы является анализ и сравнение алгоритмов и моделей машинного обучения, применимых для выявления инсайдерских угроз. Результатом работы является постановка задачи для дальнейшего исследования.

Масштаб и актуальность угрозы инсайдера в крупных корпоративных ИС

Инсайдерские инциденты представляют собой одну из наиболее труднообнаруживаемых и финансово затратных категорий киберрисков. Ключевая особенность внутреннего нарушителя – злоупотребление легитимными правами доступа, что позволяет обходить традиционные периметровые системы защиты.

Согласно глобальным исследованиям, средняя стоимость инцидентов, связанных с инсайдерами, продолжает расти, достигая миллионов долларов на организацию в год. Наиболее частым сценарием является небрежность сотрудников, однако наиболее дорогостоящими - инциденты с компрометацией учетных записей через фишинг.

В российских исследованиях наблюдается дефицит публичных данных об инцидентах, однако аналитика показывает, что наиболее уязвимыми каналами утечки являются мессенджеры, электронная почта и съемные носители.

Постановка задачи

Задача поиска инсайдера сводится к задаче обнаружения аномалий в больших массивах телеметрии корпоративных систем.

Существуют две основные стратегии выявления аномалий:

- Обнаружение выбросов: Идентификация единичных объектов, резко отклоняющихся от общего набора данных. Эффективно для выявления разовых подозрительных событий.
- Обнаружение новизны: Распознавание ранее не встречавшихся паттернов поведения, не соответствующих модели «нормы», построенной на основе обучающих данных. Эффективно для выявления новых, неизвестных ранее сценариев угроз.

Обзор и сравнительная характеристика методов машинного обучения

Алгоритмы для обнаружения выбросов

Изолирующий лес. Быстрый и масштабируемый алгоритм, эффективно выявляющий редкие, многофакторные отклонения в активности пользователя.

Локальный уровень выброса. Оценивает аномальность объекта относительно его локального окружения, что полезно для анализа поведения в рамках отдельных ролей или отделов.

Методы для обнаружения новизны

Одноклассовый метод опорных векторов. Строит границу, отделяющую нормальное поведение от аномального. Чувствителен к настройкам и качеству обучающих данных.

Автокодировщик: Нейросетевая модель, выявляющая аномалии по высокой ошибке реконструкции данных. Способна находить сложные нелинейные зависимости.

Сеть долгой краткосрочной памяти. Анализирует временные последовательности, что позволяет выявлять не одиночные события, а подозрительные цепочки действий, развивающиеся во времени.

Трансформер. Современная архитектура на основе механизма внимания, способная улавливать сложные контекстные и долговременные зависимости в поведенческих последовательностях. Показывает высокую эффективность, но требует значительных вычислительных ресурсов.

Заключение

Выбор алгоритма зависит от конкретной задачи: для поиска разовых отклонений эффективны классические алгоритмы, а для выявления сложных поведенческих аномалий – модели глубокого обучения.

Наиболее перспективным направлением является разработка гибридных систем, которые комбинируют преимущества разных подходов, что позволяет повысить точность и снизить количество ложных срабатываний. Использование трансформеров открывает возможности анализа поведенческих паттернов с учётом контекста и корреляции между событиями.

В дальнейшем представляется целесообразным провести экспериментальную проверку эффективности указанных моделей на данных типа CERT r4.2, а также адаптацию трансформерных архитектур к специфике корпоративных сетей.

УДК 004.056

З.П. ГРАФОВ, Е.С. ПАНАРИН, К.Д. ПРЫГОВ

МИРЭА – Российский технологический университет, Москва

ПРОБЛЕМЫ АНАЛИТИКИ КИБЕРУЯЗВИМОСТЕЙ НА ПРИМЕРЕ СКАНЕРА ФСТЭК ScanOVAL

Исследование основных проблем автоматизированной аналитики кибер уязвимостей с использованием сканера ФСТЭК ScanOVAL. Выявлены ограничения в форматах отчетности, сложности интеграции с корпоративными системами управления инцидентами и недостатки автоматизации процессов сканирования. Предложены направления совершенствования методологии анализа уязвимостей и повышения эффективности аналитических процедур.

Введение

ScanOVAL – отечественный сканер уязвимостей, разработанный компанией «Алтэкс-Софт» по инициативе и при поддержке Федеральной службы по техническому и экспортному контролю России (ФСТЭК). Программа предназначена для автоматического обнаружения уязвимостей на рабочих станциях и серверах под управлением ОС Windows и Linux (Astra Linux и др.) посредством сравнения системных параметров с базой уязвимостей, описанных в формате OVAL (Open Vulnerability and Assessment Language) [1–3].

Ограниченность базы уязвимостей

ScanOVAL использует в качестве источника базы ФСТЭК (БДУ – Банк данных угроз), которые пока содержат ограниченное число записей (около 200 угроз и 43 тысячи уязвимостей) по сравнению с международными CVE-базами. Это снижает полноту обнаружения актуальных и новых уязвимостей, особенно в стороннем или модифицированном ПО [1, 3, 4].

Ограниченная поддержка операционных систем

Хотя для Windows сканер развивается более полно, версия для Linux находится в тестовом состоянии и покрывает ограниченный набор дистрибутивов (Astra Linux, Альт 9 и др.). Это снижает применение ScanOVAL в гетерогенных и масштабных инфраструктурах [1].

Трудоемкость ручной фильтрации результатов

Из-за большого объема выявленных уязвимостей (превышающего 200 на одном устройстве) аналитика и фильтрация для выделения реально критичных рисков требуют значительных усилий специалиста. В ScanOVAL отсутствуют развитые механизмы интеллектуальной

фильтрации и автоматической приоритизации на базе семантического анализа [3].

Ограничения в работе с пользовательскими описаниями

Хотя в описании заявлено, что ScanOVAL может использоваться для разработки и отладки собственных OVAL-описаний, на практике сканер принимает только защищённый ФСТЭК XML-контент. Попытки загрузить неподписанные или сторонние описания заканчиваются отказом, что ограничивает гибкость и расширяемость инструмента [3, 4].

Недостатки интерфейса и формата отчетности

Результаты сохранения доступны только в формате HTML, что требует дополнительной обработки для автоматизированного анализа данных. Несмотря на наличие XML-файлов с результатами, их обработка не является удобной и не интегрируется с большинством систем управления уязвимостями [3, 4].

Заключение

ScanOVAL демонстрирует высокий потенциал как отечественный инструмент для обнаружения уязвимостей, отвечающий требованиям импортозамещения. Однако ряд проблем – ограниченность базы уязвимостей, фрагментарная поддержка ОС, высокая трудоемкость аналитики, жесткие ограничения на работу с контентом и неудобство отчетности – сдерживают его широкое применение и требуют доработок для повышения эффективности аналитики кибер уязвимостей в сложных корпоративных и государственных инфраструктурах [3, 4].

Список литературы

1. Могилко И. А. Программное средство для анализа и мониторинга уязвимостей в соответствии с Банком данных угроз безопасности информации ФСТЭК РФ // Вестник науки. – 2025. – Т. 2. – № 7 (88). – С. 34–42.

2. Кучкарова Н. В. Разработка и исследование программного комплекса ScanOVAL для обнаружения уязвимостей в программном обеспечении : дис. ... канд. техн. наук / Н. В. Кучкарова. – М. : Министерство науки и высшего образования РФ, 2023. – 142 с.

3. Васильев В. И. Автоматизация анализа уязвимостей программного обеспечения на примере ScanOVAL // Информационная безопасность. – 2020. – С. 12–23.

4. Комаров В. В., Мезинова Н. А., Евдокимова Е. А. Анализ условий реализации угроз безопасности через эксплуатацию уязвимостей информационных активов // Вестник Санкт-Петербургского университета ГПС МЧС России. – 2024. – № 2. – С. 126–135. – DOI: 10.61260/2218-13X-2024-2-126-135.

УДК 004.056

В.Г. КАЛИНА

Национальный исследовательский ядерный университет «МИФИ», Москва

ОБНАРУЖЕНИЕ ЧУВСТВИТЕЛЬНЫХ ДАННЫХ В ПРОГРАММНОМ КОДЕ С ПОМОЩЬЮ LLM

В работе рассматривается проблема автоматического обнаружения чувствительных данных в программном коде с использованием больших языковых моделей. Задача формируется как токен-классификация и предлагается решение на основе архитектуры DeBERTa v3 в комбинации со сканером DeepSecrets. Модель обучена на данных публичных репозиториев. Экспериментальная оценка показала высокую эффективность F5-score=0.88. Результаты демонстрируют перспективность применения LLM для задач кибербезопасности.

Рост объемов программного кода в компаниях и увеличение числа участников процесса разработки создают серьезные риски для информационной безопасности организаций. Согласно исследованию IBM, компании, использующие методы автоматизации для обнаружения утечек, находят их почти на 100 дней быстрее [1]. Одной из наиболее критичных проблем является случайное включение чувствительных данных в исходный код - паролей к базам данных, API-ключей, токенов доступа и других секретных параметров. Традиционные сканеры безопасности, основанные на регулярных выражениях и заранее определенных правилах, генерируют большое количество ложных срабатываний, что создает значительную нагрузку на службы безопасности и замедляет процесс разработки.

Задача автоматического обнаружения чувствительных данных в программном коде может быть сформулирована как задача токен-классификации, известная также как Named Entity Recognition (NER) [2]. В отличие от классификации текста, где модель определяет категорию всего документа, токен-классификация требует присвоения метки каждому отдельному токену в последовательности. Для маркировки данных используется формат BIO (Beginning, Inner, Outer), где B обозначает начало чувствительной сущности, I – продолжение многотокенной сущности, а O – токены, не относящиеся к секретным данным.

Предлагаемое решение основано на применении трансформерной архитектуры DeBERTa v3 [3] в сочетании со специализированным сканером DeepSecrets, разработанным для первичного обнаружения

потенциально опасных фрагментов кода [4]. В качестве обучающих данных использовались публичные репозитории GitHub, содержащие файлы переменных окружения, в которых часто хранятся конфигурационные параметры и секретные ключи.

Архитектура модели включает предобученный DeBERTa v3, выход которого подается на полносвязный слой Dense для получения предсказаний на уровне токенов. Один из этапов является предобработка данных, включающая токенизацию с использованием DebertaV3Tokenizer и выравнивание меток токенов с метками слов, поскольку один токен может быть разбит на несколько подтокенов. В качестве функции потерь используется кросс-энтропия с игнорированием указанных классов, а метрикой качества служит F-beta score, придающим больший вес полноте обнаружения.

Экспериментальная оценка модели на тестовой выборке продемонстрировала значение F5-score равное 0.887 при величине функции потерь 0.0005, что свидетельствует о высокой точности классификации. Разработанный подход демонстрирует эффективность применения больших языковых моделей для задач кибербезопасности и открывает перспективы для дальнейших исследований в области автоматической оценки рисков, моделирования угроз и предсказания возможных сценариев атак на этапе проектирования систем.

Список литературы

1. IBM Security. Cost of a Data Breach Report 2024. [Электронный ресурс] URL: https://www.ibm.com/downloads/documents/us-en/107a02e94948f4ec (дата обращения: 15.10.2025).

2. Li J. et al. A Survey on Deep Learning for Named Entity Recognition // IEEE Transactions on Knowledge and Data Engineering. 2022.

3. He P. et al. DeBERTaV3: Improving DeBERTa using ELECTRA-Style Pre-Training with Gradient-Disentangled Embedding Sharing // arXiv preprint arXiv:2111.09543. 2021.

4. Secrets scanner that understands code. [Электронный ресурс] URL: https://github.com/ntoskernel/deepsecrets (дата обращения: 14.10.2025).

УДК 004.056

В.В. ВОЛОБУЕВ

Научный руководитель – к.т.н., доцент В.С. КИРЕЕВ

Национальный исследовательский ядерный университет «МИФИ», Москва

ВРЕМЕННЫЕ МЕТКИ В ГРАФАХ ЗНАНИЙ ДЛЯ АНАЛИЗА ИНЦИДЕНТОВ

Предложен подход к добавлению временных меток в графы знаний для анализа инцидентов. Разработана схема добавления временных атрибутов и алгоритм фильтрации событий. Практическая ценность работы заключается в создании механизма для обогащения графов знаний временной информацией.

Введение

Современные информационные системы генерируют множество событий, анализ которых требует учета времени их возникновения. Существующие подходы к работе с графами знаний часто не учитывают временные характеристики данных, что затрудняет анализ последовательности событий при расследовании инцидентов [1–3, 5]. Для построения исходного графа знаний из текстовых данных в данной работе используется подход, основанный на нейросетевой модели T5 [4], который был дополнен механизмом временных меток.

Цель работы

Целью работы является разработка подхода к добавлению временных меток в графы знаний для анализа инцидентов.

Объект и предмет исследования

Объектом исследования выступают графы знаний как способ представления информации о событиях. Предметом исследования является механизм присвоения и использования временных меток для анализа временных последовательностей.

Процесс исследования

Для достижения цели решены следующие задачи: изучены основные способы хранения временных данных в графах [6]; разработана схема добавления временных атрибутов к элементам графа; создан алгоритм фильтрации событий по временным интервалам; реализован прототип системы для демонстрации возможностей подхода.

Предложенный подход позволяет добавлять к сущностям и связям графа знаний временные метки, указывающие момент их регистрации. Разработанный алгоритм обеспечивает выборку событий за заданный период времени и построение временных последовательностей. Прототип системы наглядно демонстрирует возможность анализа хронологии событий и выявления связанных инцидентов в пределах заданного временного окна.

Заключение

Практическая ценность работы заключается в создании доступного и эффективного механизма для обогащения графов знаний временной информацией. Разработанный подход может быть успешно использован в системах мониторинга и анализа событий для исследования последовательности действий при расследовании инцидентов. Полученные результаты открывают перспективы для дальнейшего развития методов временного анализа в графах знаний.

Список литературы

1. Калинина А.Ю., Киреев В.С. Визуализация корпуса документов с помощью извлечения сущностей и связей предметной области на основе нейросетевой модели глубокого обучения T5 / А.Ю. Калинина, В.С. Киреев // XXV Международная научно-техническая конференция «Нейроинформатика-2023»: Сборник научных трудов.

2. Гринева Н.В. Применение графов для определения состояний нарушения безопасности активов [Электронный ресурс] / Н.В. Гринева // CyberLeninka. – 2024. – URL: https://cyberleninka.ru/article/n/primenenie-grafov-dlya-opredeleniya-sostoyaniy-narusheniya-bezopasnosti-aktivov (дата обращения: 22.09.2025)

3. Дойникова Е.В. Совершенствование графов атак для мониторинга кибербезопасности: оперирование неточностями, обработка циклов, отображение инцидентов и автоматический выбор защитных мер / Е.В. Дойникова // Программные продукты и системы. – 2018. – Т. 15, № 1. м С. 45–60.

4. Израилов К.Е. Метод обнаружения атак различного генеза на сложные объекты на основе интеллектуальной нечеткой графо-ориентированной модели / К.Е. Израилов // Вопросы кибербезопасности. – 2023. – № 3. – С. 90–100. – DOI: 10.21681/2311-3456-2023-3-90-100.

5. Косимова М.Ш. Приложения теории графов в компьютерной сетевой безопасности [Электронный ресурс] / М. Ш. Косимова // CyberLeninka. – 2024. – URL: https://cyberleninka.ru/article/n/prilozheniya-teorii-grafov-v-kompyuternoy-setevoy-bezopasnosti (дата обращения: 15.10.2025).

6. Манжосов А.В. Метод автоматизированного построения графа знаний связности формальных моделей норм и требований в области информационной безопасности / А. В. Манжосов, И. П. Болодурина // Методы и системы защиты информации. – 2022. – № 2(44). – С. 49–56. – DOI: 10.14529/secur220207.

УДК 004.89:004.41

А.А. САФОНОВА, В.Ю. РАДЫГИН

Национальный исследовательский ядерный университет «МИФИ», Москва

АВТОМАТИЗАЦИЯ УПРАВЛЕНИЯ НАУЧНЫМИ ИССЛЕДОВАНИЯМИ В УНИВЕРСИТЕТЕ С ПОМОЩЬЮ ML-АЛГОРИТМОВ

Аннотация: в условиях цифровой трансформации образования университеты сталкиваются с необходимостью внедрения современных инструментов для систематизации и анализа научной деятельности. Предлагаемая в статье платформа обеспечивает автоматическую теговую разметку публикаций и их классификацию по научным направлениям, что позволяет существенно повысить эффективность анализа научной деятельности университета.

Введение

На фоне развития цифрового мира университеты сталкиваются с необходимостью обработки растущих массивов научных данных, для чего традиционных методов уже недостаточно [1]. Решением этой проблемы становится внедрение алгоритмов машинного обучения, способных анализировать неструктурированную информацию и выявлять скрытые взаимосвязи [5–6]. В таких условиях создание не просто системы электронного архива документов, а комплексной аналитической платформы для стратегического управления исследованиями, позволяющая оценивать перспективность научных направлений и укреплять профиль университета, является актуальной задачей, решение которой было предложено в НИЯУ МИФИ.

Постановка задачи и методы решения

Разрабатываемая система должна обеспечивать автоматическую теговую разметку научных публикаций с использованием алгоритмов машинного обучения. Ключевыми задачами являются:

- создание механизма обработки больших массивов текстовых данных;
- разработка алгоритмов классификации публикаций по научным направлениям;
- формирование динамического облака тегов для визуализации исследовательских трендов.

Как пример действующий разработок для выполнения данной задачи были выбраны разработки Национального Университета Сингапура, ИТМО и МГУ им. Ломоносова [2–4]

Главное преимущество системы – объективность и масштабируемость, которые исключают субъективный фактор, обеспечивают точный анализ содержания научных работ, выявляют ключевые концепции и формируют динамическое облако тегов. [7]

Результаты и их значимость

Практическая апробация системы продемонстрировала значительные результаты: автоматически проанализировано более 1000 публикаций, включающих в себя, как научные статьи сотрудников и обучающихся, так и ВКР-выпускников ИФТЭБ НИЯУ МИФИ, из которых выделено и систематизировано более 30 ключевых терминов. Эти термины распределены по 6 ключевым научным направлениям на основе тематической классификации. Разработанная платформа не только систематизирует публикации, но и открывает новые возможности для стратегического планирования, позволяя отслеживать исследовательские тренды и оценивать продуктивность научных коллективов.

Заключение

Реализованная система – комплексное решение для управления научной деятельностью. Внедрение разработки повышает прозрачность научной деятельности, создаёт основу для развития аналитических инструментов и укрепляет позиции университета в глобальном научном пространстве.

Список литературы

1. Век информационных технологий – URL: http://smysl.info/novosti/vek-informatcionnykh-tekhnologii
2. National University of Singapore – URL: https://nus.edu.sg/nuslibraries
3. OpenBooks ITMO repository – URL: https://openbooks.itmo.ru/
4. ИСТИНА. Интеллектуальная Система Тематического Исследования НАукометрических данных – URL: https://istina.msu.ru/
5. Most Popular Backend Frameworks – 2012/2024. – URL: https://statisticsanddata.org/data/most-popular-backend-frameworks-2012-2024/
6. Научно-исследовательский инновационный портал как одно из условий развития в ВУЗе научно-исследовательской и инновационно-образовательной среды / Аверьянова Е.А. // Современные информационные технологии в образовательной деятельности – ст. 112-116
7. Облако ключевых слов // Адогий Глоссарий – URL: https://www.adogy.com/ru/terms/облако-ключевых-слов/

УДК 004.056

А.А. ЖУКОВ, О.А. КЛИМАНОВА

МИРЭА – Российский технологический университет, Москва

ПРИМЕНЕНИЕ ГЕНЕРАТИВНЫХ НЕЙРОСЕТЕЙ ДЛЯ СОЗДАНИЯ ЗАЩИТЫ ОТ ФИШИНГОВЫХ АТАК СОЦИАЛЬНЫХ ИНЖЕНЕРИЙ

Генеративные нейросети и технологии искусственного интеллекта (ИИ) становятся как мощным инструментом для злоумышленников, так и перспективным средством защиты от фишинга и социальной инженерии. В статье рассматриваются современные подходы к использованию генеративных моделей для построения систем, способных выявлять и противодействовать фишинговым атакам с высокой степенью адаптивности и автоматизации.

Введение

В последние годы фишинг и социальная инженерия стали одними из самых распространенных и эффективных методов киберпреступлений. Злоумышленники применяют ИИ и генеративные нейросети для создания высококачественных, персонализированных фишинговых сообщений, что значительно усложняет их обнаружение традиционными средствами. Однако эти же технологии могут использоваться для разработки инновационных систем защиты, способных анализировать коммуникации, выявлять подозрительные паттерны и предотвращать атаки.

Современные вызовы фишинга с применением ИИ

Согласно исследованиям и аналитике 2025 года, примерно 80% фишинговых атак используют ИИ для генерации высоко качественных писем и сообщений, которые максимально имитируют стиль и тональность корпоративной переписки, что дезориентирует пользователей и системы обнаружения. Кроме того, автоматизация и масштабирование рассылок через нейросетевые платформы увеличивают охват и эффективность атак [1, 2].

Роль генеративных нейросетей в защите

Генеративные модели применяются для создания обучающих и тестовых наборов данных, выявления аномалий и генерации паттернов, используемых для распознавания фишинговых сообщений. Они помогают создавать контрмеры, в том числе:

– Автоматический анализ текста и обнаружение скрытых намерений через методы обработки естественного языка (NLP).

– Имитирование фишинговых сценариев для обучения сотрудников методам защиты.

– Адаптивное выявление новых видов атак и автоматическое обновление защитных алгоритмов.

– Визуальный анализ писем и сайтов с использованием генеративных моделей для выявления дипфейков и подделок [3].

Практические реализации и примеры

Ведущие компании, такие как «Информзащита» и международные игроки на рынке, внедряют антифрод-системы с ИИ-модулями, которые позволяют автоматически идентифицировать и блокировать фишинговые письма. Регулярные тренинги с использованием сгенерированных ИИ фишинговых кейсов повышают осведомленность сотрудников и снижают риск успешных атак. Также развивается направление наступательной безопасности, с проактивным тестированием уязвимостей через атакующие симуляции, поддерживаемые ИИ [1, 4, 5].

Заключение

Генеративные нейросети – это двусторонний меч в сфере кибербезопасности: они усиливают как возможности атакующих, так и защитников. Разработка систем защиты с использованием генеративных моделей и обработкой естественного языка становится одним из ключевых направлений в борьбе с фишингом и социальной инженерией. Совмещение технических решений с обучением и повышением осведомленности пользователей создает комплексную и эффективную защиту.

Список литературы

1. Коваленко П.В. «Информзащита»: ИИ используется в 8 из 10 фишинговых атак: https://clck.ru/3PrCE5.

2. Сдобникова И.А. ИИ-фишинг: как защитить корпоративную почту в эпоху умных атак: https://clck.ru/3PrCGG.

3. Cyber IQ. Кибератаки на нейросети: как хакеры обманывают ИИ в 2025 году и что с этим делать российским компаниям: https://clck.ru/3PrCQx.

4. Сергеева М.А. Фишинг в корпоративной среде: как предотвратить атаки и защитить сотрудников от обмана: https://clck.ru/3PrCVz.

5. Positive Technologies: какие технологии станут целью атак хакеров в 2025 году: https://clck.ru/3PrCXs.

УДК 004.056

М.И. СИНЦОВ

РГУ нефти и газа (НИУ) им. И.М. Губкина, Москва

ВЕРОЯТНОСТЬ БЛОКИРОВКИ КЛЮЧЕВЫХ БИЗНЕС-ПРОЦЕССОВ ОРГАНИЗАЦИИ В РЕЗУЛЬТАТЕ ЛОЖНО-ПОЛОЖИТЕЛЬНОГО СРАБАТЫВАНИЯ ПРАВИЛ КОРРЕЛЯЦИИ

В статье рассмотрено влияние автоматического реагирования на блокировку бизнес-процессов организации при отсутствии реальной атаки. Проведен расчет значений вероятного простоя бизнес-процессов в результате такого реагирования. Осуществлено сравнение простоя в результате ложно-положительных сработок и реальной атаки.

В настоящее время [1, 2] остро стоит вопрос автоматического реагирования на действия злоумышленников, ввиду невозможности противостоять современным методам атаки с помощью ручного реагирования (например, внесении IP-адреса в черный список на средствах периметральной защиты или изоляция хоста средствами EDR (Endpoint Detection and Response). Разница в оперативности между ручным и автоматическим реагированием достигает десятки, а иногда и сотни раз. Вместе с тем, существует вероятность применения автоматического реагирования по результатам ложно-положительных сработок правил корреляции, что в свою очередь несет риски остановки бизнес-процессов организации наравне с атакой злоумышленников.

Оценим вероятность блокировки ключевых бизнес-процессов организации C по результатам изоляции сетевого сегмента средствами EDR в результате ложно-положительного срабатывания правила R на датасете сработок некоторого SOC за 365 дней.

Правило R срабатывало N раз, из которых у F сработок выставлен вердикт – ложно-положительная сработка. Если на сработку данного правила мы установим задачу по автоматическому реагированию в виде изоляции сетевого сегмента, то в $P=(100*F)$/N % бизнес-процессы будут остановлены без наличия явной угрозы со стороны злоумышленника. Каждая задача по разблокировке занимает в среднем R минут. Таким образом можно рассчитать общее время простоя бизнес-процессов в год от ложно-положительных сработок. Предположим данное значение будет $T_R=X$ минут.

Далее рассмотрим некую статистику реальных атак на предприятия сегмента организации С. В соответствии со статистическими данными предположим, что успешные атаки на организации сегмента компании С в среднем бывают 1 раз в 2 года. При этом по результатам такой атаки простой бизнес-процессов составляет $T_A = Y$ минут. Итого среднее значение простоя за год, в случае успешной атаки и отсутствия автоматического реагирования может составлять $T_{\text{срд}} = Z$ минут.

При расчете указанных выше показателей на основе датасета сработок некоторого SOC простой по результатам ложно-положительных сработок в разы меньше простоя, который либо был, либо могу быть возможен по результатам реальной атаки злоумышленника. При этом доработка правил корреляции в целях снижения ложно-положительных сработок приводит к пропуску действий злоумышленников, что в свою очередь увеличивает среднее количество реальных атак на организацию в течение года [3].

Таким образом, в целях снижения влияния ложно-положительных сработок на простои бизнес-процессов организациям необходимо применять автоматическое реагирование только на те правила корреляции, вероятность простоя при которых значительно ниже вероятности простоя в ходе реальной атаки, которая будет задетектирована данным правилом корреляции.

Список литературы

1. Сулейманова Д.О., Магомаев Т.Р. Когнитивная безопасность: исследование когнитивной науки в области кибербезопасности. Общество, Экономика, Управление. 2022, № 3, с. 58–65. DOI: 10.47475/2618-9852-2022-17310.

2. Autonomous AI hacking and the future of cybersecurity, URL: https://www.csoonline.com/article/4069075/autonomous-ai-hacking-and-the-future-of-cybersecurity.html (дата обращения: 15.10.2025).

3. Котенко И.В., Саенко И.Б., Лаута О.С., Васильев Н.А., Садовников В.Е. Атаки и методы защиты в системах машинного обучения: анализ современных исследований. Вопросы кибербезопасности. 2024, №1 (59), с. 24–37, DOI: 10.21681/2311-2024-1-24-37.

УДК 004.056

И.Д. КУЗЬМИН, А.В. КАШИРИН
Научный руководитель – В.А. РЫЧКОВ
Национальный исследовательский ядерный университет «МИФИ», Москва

ПРАКТИЧЕСКАЯ СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ: МОДЕЛИРОВАНИЕ УГРОЗЫ ДЛЯ ВЫЯВЛЕНИЯ БАНКОВСКИХ ДАННЫХ ЖЕРТВЫ НА ПЛАТФОРМАХ ОНЛАЙН-ЗНАКОМСТВ

В докладе рассматривается вопрос проектирования гибридного вредоносного программного обеспечения, созданного с целью выявления конфиденциальных данных (в том числе данные банковских карт) жертвы – не только техническими мерами, но и в том числе с применением высоко персонализированного подхода для повышения эффективности воздействия на целевой объект атаки.

Введение

В современном мире самый популярный способ нахождения пары [1], во многих странах мира, – используя социальные сети и сайты для знакомств, существует значимая перспектива реализации атаки для выявления конфиденциальной информации, от финансовых данных вплоть до государственной тайны – как и было в случае полковника ВС США Д. Слэйтера [2], раскрывшего засекреченную информацию «девушке из Украины» в приложении для знакомств в феврале 2022 г..

Основная часть

Текущие механизмы атак через этот вектор либо малоэффективные (без персонализации по отношению к цели атаки, и жертва быстро распознает злоумышленника), либо требуют постоянного внимания со стороны атакующего для фокуса на одной цели и не позволяет ему достичь большого охвата проведения операции. Разрабатываемый вариант модели вредоносного ПО (рис. 1) позволит сочетать лучшее из обоих подходов – добавить скорость распространения и процесс автоматизации, при этом сохранить эффективность атаки и высокую степень персонализации. В частном случае применения модели для выявления банковских данных, их у объекта можно будет выявлять не через дорогостоящую, долговременную операцию, а через хорошо выстроенный, автоматический процесс социальной инженерии.

Заключение

В итоге разработанная модель предлагает реализацию указанного гибридного подхода. Сохраняются многие факторы, которые необходимо учитывать в самой реализации ВПО перед запуском в сеть – культурные особенности целевой аудитории, специфику площадки. Тем не менее, если обе стороны учесть и достаточно подготовить техническую базу для атаки (в том числе создание качественной страницы для ввода банковских данных), схема достигает высокий потенциал успеха.

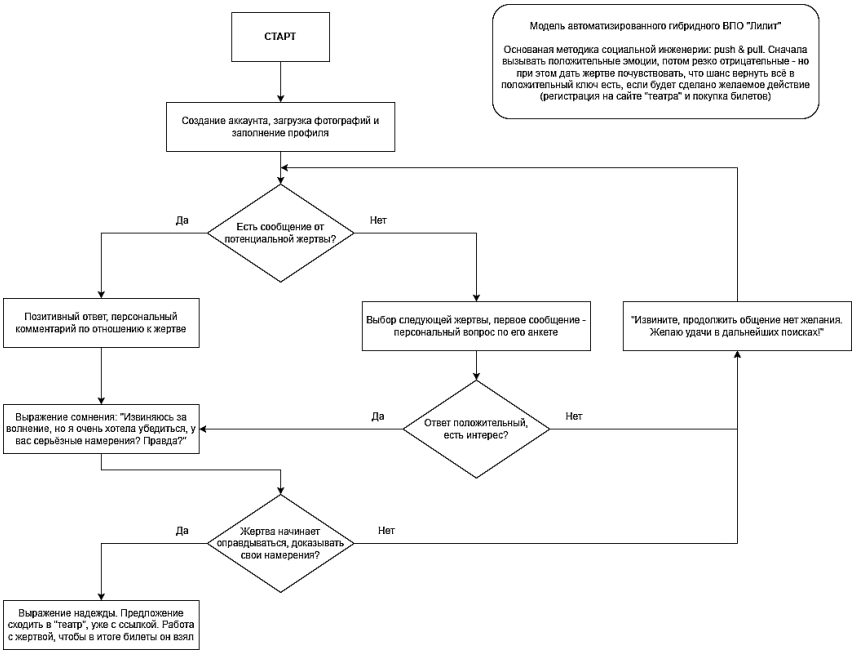


Рис. 1. Схема алгоритма ВПО

Список литературы

1. Michael Rosenfeld. Meeting online has become the most popular way U.S. couples connect, Stanford sociologist finds [Электронный ресурс] // URL: https://news.stanford.edu/stories/2019/08/online-dating-popular-way-u-s-couples-meet (дата обращения: 13.10.2025).

2. Danny Bradbury. Dating app scammer cons former US army colonel into leaking national secrets [Электронный ресурс] // URL: https://www.malwarebytes.com/blog/news/2025/07/dating-app-scammer-cons-former-us-army-colonel-into-leaking-national-secrets (дата обращения: 10.10.2025).

УДК 004.056

А.В. КАШИРИН, В.А. РЫЧКОВ, И.Д. КУЗЬМИН

Национальный исследовательский ядерный университет «МИФИ», Москва

НОВЫЕ ВЕКТОРЫ КИБЕРУГРОЗ НА ОСНОВЕ QR-КОДОВ: АНАЛИЗ И ЗАЩИТА

В работе исследуются современные методы кибератак, использующие QR-коды в качестве основного вектора компрометации. Рассматриваются два принципиально разных типа угроз: Unicode QR Code Phishing, обходящий email-фильтры за счёт текстового представления QR-кода, и стеганографическая атака через NPM-пакет fezbox с трёхслойной обфускацией. Целью исследования является выявление уязвимостей в современных системах аутентификации и цепочках поставок ПО, а также разработка рекомендаций по многоуровневой защите.

Постановка задачи

Массовое внедрение QR-кодов в корпоративные и пользовательские процессы – от аутентификации до документооборота – породило новые векторы атак, эксплуатирующие доверие пользователей и пробелы в защите. Особенно актуальны атаки [1], сочетающие социальную инженерию и техническую изощрённость: они обходят традиционные средства защиты, такие как антиспам-фильтры, антивирусы и системы анализа зависимостей. Задача работы – проанализировать механизмы атак QRLJacking, Unicode QR Phishing и стеганографической компрометации через NPM, оценить их опасность и предложить эффективные меры противодействия.

Пути решения и новые результаты

Первый тип угроз – Unicode QR Code Phishing – использует блочные символы Unicode (U+2580–U+259F) для визуального формирования QR-кода непосредственно в теле письма. Такой «код» распознаётся сканерами, но воспринимается email-системами как обычный текст, что позволяет обходить OCR-анализ и URL-фильтрацию. Эксперименты показали, что 92 % современных Secure Email Gateway не детектируют такие атаки [2].

Второй тип – стеганографическая атака fezbox – представляет собой supply chain-угрозу. Вредоносный NPM-пакет содержит QR-код в виде изображения, в пикселях которого скрыт Base64-закодированный JavaScript-код. Активация происходит через postinstall-хук с вероятностной задержкой и проверкой среды, что затрудняет анализ в песочницах. Атака успешно крадёт cookie, SSH-ключи и переменные окружения, экстрафильтрируя их через HTTPS [3].

Третий вектор – QRLJacking – направлен на перехват сессий в системах, использующих QR-аутентификацию (WhatsApp Web, Telegram и др.). Злоумышленник подменяет легитимный QR-код на фишинговом сайте; при

сканировании токен сессии отправляется на сервер атакующего, что даёт полный доступ к аккаунту без знания пароля [4].

Новые векторы киберугроз

Все три метода объединяет стеганографический принцип сокрытия и эксплуатация разрыва между данными и их визуальным представлением. Согласно методологии ФСТЭК, такие угрозы классифицируются как комбинированные с высокой актуальностью и критическим уровнем опасности [5].

Заключение

Проведённый анализ показывает, что QR-технологии, несмотря на удобство, создают новые слепые зоны в кибербезопасности. Традиционные сигнатурные и периметровые подходы неэффективны против описанных атак. Выводы

1. Необходимо внедрять поведенческий анализ на уровне email-шлюзов для детектирования аномальных Unicode-последовательностей.
2. Для защиты цепочек поставок ПО требуется обязательный анализ изображений в пакетах на наличие скрытых QR-кодов и использование приватных репозиториев с предварительной проверкой.
3. Системы QR-аутентификации должны включать визуальную верификацию, подтверждение на основном устройстве и ограничение времени жизни кода.
4. Рекомендуется актуализировать методологию ФСТЭК с включением специфических угроз QR-технологий и стеганографии.

Эффективная защита возможна только при сочетании технических мер, организационных политик и непрерывного обучения пользователей.

Список литературы

1. Каширин А. В. Актуальные уязвимости кибербезопасности при применении QR-кодов с помощью технических средств / А.В. Каширин, В.А. Рычков // Финансовая безопасность – новые горизонты: Материалы X Международной научно-практической конференции Международного сетевого института в сфере ПОД/ФТ, Москва, 19–20 ноября 2024 года. – М.: НИЯУ МИФИ, 2024. – С. 82–92. – EDN VSTAPH.
2. Kowski J.S. Unicode QR Code Phishing: A Novel Approach to Email-Based Social Engineering. Journal of Cybersecurity Research, 2024.
3. Socket Threat Research Team. Fezbox: Anatomy of a Sophisticated NPM Supply Chain Attack. Technical Report SR-2025-003, 2025.
4. Ezzat M., Elsobky A. QRLJacking: Hijacking Authentication via QR Codes. Black Hat Europe, 2016.
5. ФСТЭК России. Методика оценки ущерба от инцидентов ИБ. Приказ №31, 2021.

УДК 004.056

М.А. БАЕШОВ, А.Г. ЯРОВАЯ

Национальный исследовательский ядерный университет «МИФИ», Москва

КИБЕРБЕЗОПАСНОСТЬ ПРИ ЦИФРОВОЙ ТРАНСФОРМАЦИИ МАЛОГО И СРЕДНЕГО БИЗНЕСА

В современных условиях цифровая трансформация малого и среднего бизнеса сопровождается внедрением облачных сервисов, дистанционных каналов продаж и автоматизации управленческих процессов, что резко увеличивает значимость цифровых активов и одновременно расширяет поверхность потенциальных киберугроз. Задача заключается в разработке адаптируемой и экономически оправданной стратегии кибербезопасности для МСБ, которая обеспечивает конфиденциальность, целостность и доступность данных, устойчивость бизнес-процессов к инцидентам (включая атаки типа ransomware), соблюдение нормативных требований и минимизацию затрат через приоритизацию мер и использование управляемых/облачных сервисов. Российская подготовка специалистов в области кибербезопасности фокусируется на интеграции теории и практики, что создаёт предпосылки для прикладных решений в рамках задач МСБ. [1]

Решение проблемы предлагается реализовать на трёх взаимосвязанных уровнях: организационном, процедурном и техническом. На организационном уровне необходимо назначение ответственного за информационную безопасность (включая возможность аутсорсинга функции к MSSP), внедрение регламентов управления доступом и требований к поставщикам, а также формализация плана реагирования на инциденты. На процедурном уровне ключевыми элементами являются инвентаризация и классификация цифровых активов, регулярный патч-менеджмент, проверяемые резервные копии с определёнными RTO/RPO и регулярные упражнения по восстановлению. Технические меры включают внедрение многофакторной аутентификации, управление привилегиями по принципу минимальных прав, сегментацию сети, базовый мониторинг и защиту конечных точек (EDR) с возможностью подключения облачного SIEM или MSSP при росте нагрузки. Комплексный подход должен опираться на стандарты и лучшие практики, адаптированные под ресурсные ограничения МСБ. [1]

Предлагается концепция «модульной минимальной защиты» как лёгкого для внедрения набора взаимодополняющих модулей безопасности: модуль идентификации и классификации активов, модуль

аутентификации и управления доступом, модуль резервирования и восстановления, модуль обучения персонала с симуляциями фишинга и модуль мониторинга с опцией быстрого подключения MSSP. Такой модульный подход позволяет масштабировать защиту по мере роста компании и гармонизировать её с образовательными практиками и лабораторными наработками профильных программ подготовки. [2]

Кибербезопасность при цифровой трансформации МСБ должна рассматриваться как интегральная часть бизнес-стратегии, а не как внешняя ИТ-опция. Для достижения баланса между эффективностью защиты и ограниченными ресурсами МСБ необходимо применять модульный, поэтапный подход: быстрые и высокоэффективные меры дают заметный прирост устойчивости бизнеса, а постепенное подключение мониторинга и профессиональных сервисов позволяет наращивать зрелость безопасности. Образовательная среда и практические наработки ведущих профильных программ создают методическую базу для воспроизводимых решений и пилотных проектов, которые могут быть масштабированы в отраслевом контексте. [1]

Заключение

Разработанная модульная концепция обеспечивает воспроизводимый и экономически оправданный путь повышения киберустойчивости МСБ в условиях цифровой трансформации. Основные факторы успеха включают систематическую инвентаризацию активов, применение принципа минимальных привилегий, обязательное внедрение многофакторной аутентификации и проверяемые процедуры резервирования и восстановления. Пилотная реализация подтверждает, что даже при ограниченном бюджете МСБ могут достичь критического уровня защищённости, существенно снизив вероятность длительных простоев и репутационных потерь. Дальнейшие исследования целесообразно сосредоточить на адаптации модулей под отраслевые требования и экономическом моделировании возврата вложений в безопасность для типичных сегментов малого и среднего бизнеса. [1]

Список литературы

1. Абрамов В.И., Акулова Н.Л. – Цифровая трансформация экономики: учебное пособие. Москва: НИЯУ «МИФИ», 2020. – 77-91с.

2. ENISA. Good practices for SME cybersecurity м European Union Agency for Cybersecurity, руководства и рекомендации для малого и среднего бизнеса.

КИБ-2025

КИБЕРНЕТИКА
И ИНФОРМАЦИОННАЯ
БЕЗОПАСНОСТЬ

Направление

Проблемы информационной безопасности в системе Высшей школы

Руководитель секции – ТОЛСТОЙ А.И. к.т.н.,

заведующий кафедрой №44

УДК 004.056

Г.П. ГАВДАН, А.В. МАРЧЕНКО

Национальный исследовательский ядерный университет «МИФИ», Москва

ПОДГОТОВКА КАДРОВ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ ВЫСШЕЙ ШКОЛЫ

В работе исследуются вопросы совершенствования системы высшего образования (ВО) в контексте обеспечения информационной безопасности (ИБ). Проведен анализ современных вызовов и киберугроз, с которыми приходится сталкиваться сегодня образовательным организациям. На основе изучения научных публикаций и нормативно-правовых актов (НПА) выявлены системные проблемы в области защиты информационной инфраструктуры высшей школы (ВШ). По результатам исследования сформулированы рекомендации по обеспечению защищенности.

Введение

Обеспечение информационной безопасности (ИБ) в системе высшего образования является комплексной задачей, где ключевая роль отводится совершенствованию подготовки кадров Российской Федерации (РФ).

Актуальность данного направления обусловлена необходимостью формирования (отечественного) кадрового потенциала высшей школы (ВШ), способного противостоять современным угрозам.

Проблематика информационной безопасности в высшей школе может быть структурирована в трех взаимосвязанных аспектах:

Технический – создание защищенных систем хранения и обработки информации, включая разработку специализированного программного обеспечения;

Кадровый – организация системной подготовки и профессионального развития специалистов в области ИБ;

Организационно-правовой – формирование нормативной базы и регламентов функционирования информационной среды образовательных организаций.

Особое внимание уделяется кадровому аспекту, что подтверждается рассмотрением соответствующих вопросов на совещании у Президента Российской Федерации (РФ) с Советом Безопасности по проблемам ИБ.

Проведенный анализ выявил сохраняющиеся уязвимости в системе обеспечения ИБ ВШ, требующие комплексного решения, включая меры по координации деятельности между Министерством науки и высшего образования и профильными государственными службами (ФСТЭК России, ФСБ России).

Подготовки кадров в области ИБ: поиск и обучение талантов

Современные вызовы в области кибербезопасности обуславливают необходимость формирования эффективной системы подготовки кадров. Знаковым событием в этой сфере стала публикация Пентагоном «Плана реализации стратегии кибертрудовых ресурсов на 2023–2027 годы» [1], развивающего положения Стратегии кибербезопасности США на 2023–2027 гг. В данных документах идентифицированы ключевые проблемные зоны: отсутствие унифицированных критериев требований к киберкадрам; необходимость внедрения навыко-ориентированного отбора кандидатов; дефицит программ развития компетенций; профессиональное выгорание.

На основе системной работы осуществляется совершенствование подготовки кадров ВШ в области ИБ. Так, в соответствии с Указом Президента РФ от 12.05.2023 № 343 большинство профильных кафедр российских вузов реализуют новые основные образовательные программы (ООП) ВО и программы повышения квалификации (профессиональной переподготовки кадров) в области ИБ.

Для решения указанных проблем предложена система мер, структурированная вокруг четырех основных направлений: выявление, набор, развитие и удержание специалистов. Особого внимания заслуживает реализуемый подход к ранней профессионализации, предполагающий вовлечение учащихся детских учреждений и школ в изучение технологий, инженерии, математики и кибернетики [2].

Заключение

Необходимо продолжить обеспечивать поиск и обучение талантов. Разработанные сегодня программы позволяют использовать частное и государственное партнерство. Такое развитие кадрового потенциала с применением информационных технологий (ИТ) в области обеспечения ИБ позволяет решать такие задачи в образовательных учреждениях, где комбинирование различных ООП для специалистов разного уровня способствует повышению качества обучения, поскольку обеспечивает интеграцию практического опыта привлекаемых специалистов-практиков.

Список литературы

1. «DoD Cyber Workforce Strategy Implementation Plan 2023-2027» CLEARED For Open Publication (Jul 13, 2023) Department of Defense. Office of prepublication and security review. URL: https://media.defense.gov/2023/aug/03/2003274088/-1/-1/1/2023-2027-dod-cyber-workforce-strategy-implementation-plan.pdf (дата обращения: 19.08.2023).

2. «США не хватает сотен тысяч специалистов в области кибербеза». Эшелон в телеграм канале. URL: https://t.me/EchelonEyes/1834 (дата обращения: 19.08.2023).

УДК 004.056

Е.А. ТРОФИМОВ
Московский университет МВД России им. В.Я. Кикотя

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ КИИ ОРГАНАМИ ВНУТРЕННИХ ДЕЛ КАК ОБРАЗОВАТЕЛЬНАЯ ЗАДАЧА

В исследовании обосновывается наличие образовательной задачи, связанной с подготовкой кадров для органов внутренних дел по обеспечению безопасности объектов критической информационной инфраструктуры. Анализируются имеющиеся недостатки в подготовке специалистов по информационно-аналитическому обеспечению и делается вывод о необходимости развития программ подготовки данных специалистов в ведомственных высших учебных заведениях системы МВД России.

Цифровая трансформация затронула все сферы общественных отношений и привела к формированию качественно новой реальности, обусловленной тем, что нормальное функционирование государства и развитие общества находится в прямой зависимости от безопасности объектов критической информационной инфраструктуры (далее – КИИ).

Вместе с тем, в своем развитие не отстает и сфера преступности – с каждым годом растет количество киберугроз для указанных систем, источниками которых могут быть как и криминальные группы, так и группировки, спонсируемые недружественными государствами. В связи с этим обеспечение безопасности объектов КИИ в настоящий момент является вопросом национальной безопасности.

В первую очередь, данную деятельность связывают с технологическим развитием и разработкой новых технологий, однако немаловажным является кадровое обеспечение. Видится, что высокоразвитые системы защиты и эффективное нормативно-правовое регулирование не способны добиться необходимых результатов в отсутствии высококвалифицированных специалистов, способных грамотно применять их, проводить анализ возможных угроз и оперативно реагировать на возникающие инциденты.

Необходимо отметить, что особенное место в данной деятельности отводится органам внутренних дел (далее – ОВД), осуществляющим предупреждение, выявление и пресечение преступлений в рассматриваемой сфере, поэтому важной является подготовка вышеуказанных специалистов для нужд ОВД [1].

Основной проблемой здесь выступает системный разрыв между динамично изменяющимся состоянием информационной безопасности и информационной среды и достаточно статичной системой подготовки кадров. Говоря о подготовке специалистов по информационно-аналитическому обеспечению безопасности КИИ для ОВД, следует отметить ее вариативность:

1) Классическое образование в государственных высших учебных заведениях, характеризующейся высоким уровнем фундаментальных знаний по рассматриваемому профилю подготовки, но отсутствием специфики, связанной с деятельностью ОВД, обусловленной решением оперативно-служебных и следственных задач.

2) Ведомственное образование в высших учебных заведениях Министерства внутренних дел Российской Федерации (далее – МВД России), имеющее высокий уровень практической ориентированности, но, в некоторых случаях, отстающее в сфере внедрения и освоения современных технологический решений.

3) Программы повышения квалификации, характеризующиеся краткосрочностью, но, вместе с тем, недостаточностью фундаментальных и системных знаний [2].

Такая ситуация имеет свои негативные последствия для состояния защищенности объектов КИИ, поэтому, по нашему мнению, следует уделить особое внимание образовательной задаче, связанной с подготовкой специалистов по информационно-аналитическому обеспечению как важного компонента защиты КИИ ОВД в рамках ведомственного образования в высших учебных заведениях МВД России, позволяющего сочетать практико-ориентированных подход и достаточный уровень фундаментальных знаний, при должном дальнейшем развитии программ подготовки, внедрении и освоении современных технологий.

Список литературы

1. Осипенко А.Л. Об участии органов внутренних дел в системе обеспечения кибербезопасности Российской Федерации // Общество и право. 2018. №3 (65). с. 35-43.

2. Воронич В.В., Грачев М.И., Локнов А.И., Примакин А.И. Подготовка и переподготовка кадров в области информационной безопасности для правоохранительных органов. Региональная информатика и информационная безопасность: Сборник трудов, Санкт-Петербург, 26–28 октября 2016 года. Санкт-Петербургское общество информатики, вычислительной техники, систем связи и управления. Том Выпуск 2. Санкт-Петербург: Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления. 2016, с. 80–84. – EDN XEYLMF.

УДК 004.056

В.П. ИВАНОВ

Независимый эксперт, Краснодар

О ТЕОРИИ ЗАЩИТЫ ИНФОРМАЦИИ ПОСТНЕКЛАССИЧЕСКОГО ЭТАПА РАЗВИТИЯ НАУКИ

На основании анализа развития теоретической мысли в области защиты информации выявляются причины застоя в данной сфере и обосновывается необходимость перехода к мышлению постнеклассической стадии развития науки.

Введение

На рубеже II и III тысячелетия Мир вступил в полосу опасных информационных угроз, издания теоретической направленности по защите информации продолжают носить описательный характер, не хватает убедительности современного естествознания, что привело к написанию теории защиты информации в видении современного естествознания, истории и философии науки[1, 2].

Постановка задачи

Защита информации, как область науки относится к естествознанию. Как мировоззренческая парадигма она опирается на представления физики – базы объяснения реального физического мира. Как исторический феномен и область науки защита информации принадлежит научным эпохам развития науки, каждая из них имеет свои черты. Для решения задачи разработки научной теории на новых основаниях были поставлены задачи.

Определить:

– научную эпоху, в которой решается задача защиты информации в настоящее время;

– требования к научной теории в современном естествознании;

– структуру научной теории в современном естествознании;

– как строится современная теория в естествознании, что берется за образец;

– место аксиом и постулатов в естествознании;

– принципы, которыми руководствуются при создании научной теории;

– роль и место моделей в естествознании.

Результаты

В ходе исследования было установлено, что теория в защите информации продолжает «жить» в позитивистских нормах, что объясняет отставание теории от практики защиты информации, поскольку теории писались «успешно сдавшими кандидатский экзамен по Марксистско-Ленинской философии и в мышлении оставшимися в тех временах» [3], наука же ушла далеко вперед.

С целью решения поставленной в исследовании задачи были проанализированы изменения в науке к настоящему времени. Были выявлены в отношении науки постнеклассического этапа развития науки:

– требования к научной теории;

– характер структуры научной теории;

– осуществлен выбор образца для теории защиты информации;

– выявлены аксиомы и постулаты теории зашиты информации;

– выявлены принципы общей теории систем по отношению к теории защиты информации;

– был выявлен характер взаимодействия моделей в теории защиты информации;

– для демонстрации результативности (эффективности) разработанной теории защиты информации произведена оценка эффективности средства защиты информации по показателю эффективности – вероятность недопущения прочтения перехваченного злоумышленником текста на интервале времени, когда информация сохраняет ценность при использовании алгоритма ГОСТ 28147-89;

– высказана гипотеза о возможности существования в защите информации фундаментальных констант, в качестве таковой предложена постоянная Бреммерманна.

Список литературы

1. Степин В.С. Теоретическое знание. М. Прогресс-Традиция, 2003. – 744 с.

2. Степин В.С. История и философия науки. М. Академический проспект; Трикста, 2011. – 423 с.

3. Малюк А.А. Теория защиты информации. М. Горячая линия – Телеком, 2004. – 184 с.

УДК 378.047

И.А. РЕШЕТНИКОВ[1], И.М. КОМАРОВ[2]

[1]Институт кино и телевидения (ГИТР), Москва
[2]ООО «Газпром Информ», Москва

ФОРМИРОВАНИЕ КУЛЬТУРЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ВЫСШЕЙ ШКОЛЕ: ПОТЕНЦИАЛ ФОРМАТА ЭКРАННОЙ ИГРЫ

В докладе рассматривается проблема низкой осведомлённости студентов высшей школы в области информационной безопасности. На основе междисциплинарного подхода предлагается использование формата экранной игры для формирования соответствующих компетенций. На примере шоу «Киберарена» показано, как игровой формат преобразует теоретические правила цифровой гигиены в наглядные сценарии, повышая эффективность обучения.

Современная высшая школа сталкивается с необходимостью формирования у студентов не только профессиональных, но и цифровых компетенций, среди которых ключевое место занимает информационная безопасность. Однако традиционные методы обучения зачастую не способны обеспечить достаточный уровень вовлеченности, практического понимания угроз и знания методов борьбы с ними [1]. В этой связи возникает задача поиска инновационных педагогических подходов, способных помочь преодолеть пропасть между теоретическими знаниями и практическими навыками, смоделировать реальные угрозы в контролируемой и изолированной среде, обеспечить массовый охват аудитории благодаря зрелищности и соревновательной динамике.

Исследование опирается на междисциплинарный синтез двух областей знания – информационной безопасности (анализируются типичные угрозы, с которыми сталкивается студенческая среда) [2] и культурологии (а именно концепции Й. Хёйзинги, где игра рассматривается как фундаментальный фактор человеческой культуры) [3]. Термин «Экранная игра» определяется как агональное, зрелищное действо, обладающее четкой драматургией, правилами и ориентированное на внешнего зрителя [4]. В отличие от видеоигры, экранная игра коренится в реальности, что делает её релевантной для моделирования практических ситуаций.

Для иллюстрации потенциала формата был проанализирован проект «Киберарена» – российское интеллектуальное шоу, посвященное вопросам кибербезопасности. Соревнование состоит из нескольких раундов, в которых команды экспертов решают кейсы, основанные на

реальных инцидентах. Ответы команд оцениваются профессиональным жюри, которое комментирует решения, разбирает ошибки и предлагает оптимальные алгоритмы действий, что превращает шоу в наглядное учебное пособие [5].

На основе проведенного анализа предлагается концепция разработки и внедрения вузовской экранной игры по тематике информационной безопасности на основе актуальных для студентов кейсов (безопасность в социальных сетях, защита учебных аккаунтов, распознавание мошенничества). Формат может варьироваться от масштабных студийных съемок до более камерных трансляций из университетских медиастудий. Записи игр и разборы кейсов могут стать основой для практических занятий в курсах по информационной безопасности или цифровой грамотности.

Перспективой работы является детальная проработка пилотного сценария такой игры и его апробация в одной из учебных групп.

Список литературы

1. Костюченко К.Л., Мухачев С.В. Оценка осведомленности студентов в сфере информационных технологий и информационной безопасности // Вопросы безопасности. 2024. №2.

2. Итинсон К.С., Чиркова В.М. Обеспечение кибербезопасности в образовательных учреждениях: осведомленность, правила, стратегия // БГЖ. 2021. №4 (37).

3. Хёйзинга Й. Homo ludens. Человек играющий. – СПб.: Азбука, 2022. – 400 с.

4. Решетников И.А. Что такое «экранная игра» и как экранность и экран влияют на спортивные и интеллектуальные игры? // Культура и цивилизация. – 2025. – Т. 15, № 1-1. – С. 148–155.

5. Киберарена – новое интеллектуальное шоу об информационной безопасности // Отраслевой портал – информационная безопасность бизнеса URL: https://ib-bank.ru/bistv/video/1004 (дата обращения: 23.10.2025).

УДК 159.9: 37.013: 004

О.В. ЮСУПОВА

Самарский государственный технический университет

ЭТИЧЕСКИЕ РИСКИ ЦИФРОВОЙ ТРАНСФОРМАЦИИ ОБРАЗОВАНИЯ

В статье обозначен ряд деструктивных аспектов цифровой трансформации образования. Наиболее острой проблемой для образования сегодня названа проблема этических и моральных рисков привнесенных в повседневную образовательную практику технологий искусственного интеллекта, в том числе генеративного. Обозначены направления научных исследований, необходимых для создания технологий безопасности для образования в условиях бесконтрольного развития генеративного ИИ.

Начало XXI века характеризуется масштабным переходом общества от индустриального этапа к информационному. Образовательный сектор активно среагировал на изменения, используя достижения в области цифровизации и информационно-коммуникационных технологий: цифровизация в широком ее понимании неограниченно расширила информационное пространство, предоставила новые коммуникационные и организационные возможности, позволяя реализовать актуальные тренды развития образования: непрерывность, индивидуализацию, персонификацию и проч.

Отдельным этапом цифровизации, в том числе и образования, стало внедрение технологий искусственного интеллекта (ИИ). И если организационный потенциал ИИ очевидно полезен, то последствия применения в обучении генеративного ИИ: психологические, когнитивные, социальные, – еще предстоит оценить. Уже сейчас очевидно, что массовое внедрение технологий искусственного интеллекта в систему образования может оказать и дисфункциональное воздействие в виде таких последствий, как:

1. дегуманизация образовательного процесса – лишение его «человеческой» и этической составляющих, лишение образования своей миссии по улучшению и развитию личности;

2. нивелирование и фактическое уничтожение запроса на простые и умеренно сложные когнитивные операции;

3. усиление зависимости от технологий и роста цены возможных ошибок, допущенных искусственным интеллектом в организации образовательного процесса и другие.

Педагогическое сообщество активно обсуждает пути и средства сохранения когнитивных способностей нашей молодежи, ее психического здоровья и адекватной социализации, предлагая актуализацию традиционных методик и транслируя опыт внедрения новых авторских методик обучения и воспитания в цифровом мире.

Наименее исследованными и наиболее острыми для образования являются сегодня этические и моральные аспекты использования ИИ, в том числе и генеративного. Принятие Кодекса этики в сфере ИИ проблемы для образования не решает. И не только потому, что присоединение к нему имеет добровольный формат, а принципы и правила создания новых технологий – рекомендательный характер для компаний-разработчиков. Образование работает здесь и сейчас, каждый день в каждом классе и аудитории, и с уже существующими технологиями, которые врываются в нашу жизнь ежедневно и неконтролируемо.

В настоящее время необходимы технологические решения противостояния этическим и моральным рискам в сфере ИИ. Так, в Самарском государственном техническом университете специалисты в области проектирования интеллектуальных систем обеспечения информационной безопасности совместно с учеными в области гуманитарных наук и педагогами проводятся исследование этических проблем, связанных с технологиями искусственного интеллекта, и ищут пути их преодоления. Научные исследования включают развитие методологии гуманитарно-этической экспертизы технологических проектов с применением ИИ на различных медиаплатформах и в различных сферах его применения, в том числе в образовании; создание методик оценивания этических и моральных рисков генеративного ИИ на основе построение многоуровневой классификационной структуры; разработка платформенного решения обнаружения сгенерированного ИИ контента и этической оценки.

УДК 004

М.О. ГОРЛАНОВА, О.А. ТОЛПЫГИНА, М.Н. ОСИПОВ

Самарский национально-исследовательский университет им. С.П. Королева

ВНЕУЧЕБНАЯ АКТИВНОСТЬ СТУДЕНТОВ, ОБУЧАЮЩИХСЯ ПО НАПРАВЛЕНИЮ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Внеучебная активность является важным аспектом образовательного процесса, так как способствует расширению кругозора, установлению полезных контактов и получению нового опыта. Цель работы – выявить потребность студентов в мероприятиях, проводимых помимо учебной нагрузки.

Современное высшее образование направлено не только на формирование профессиональных компетенций, но и на развитие личности обучающегося, его социальной и профессиональной активности. Одним из важнейших факторов этого процесса выступает внеучебная деятельность, способствующая формированию навыков командной работы, развитию коммуникации, лидерских качеств и ответственности.

Особое значение внеучебная активность приобретает у студентов, обучающихся по направлению информационная безопасность. Это направление требуют постоянного профессионального развития, высоких коммуникационных навыков. Важно отметить, что данная сфера требует не только высоких технических навыков, но и высокой осознанности и чувства социальной ответственности.

Целью данного исследования является выявление потребностей и мотивационных факторов, определяющих участие студентов в мероприятиях вне учебного процесса. Для достижения поставленной цели были определены следующие задачи: оценить вовлеченность студентов во внеучебную жизнь университета, определить мотивацию/демотивацию и выявить каких мероприятий не хватает студентам.

Однако перед тем как преступить к исследованию важно выделить общие проблемы высший школы России, которые выделяют профильные специалисты. Согласно статье [1], посвященной вопросам системе высшего образования можно выделить следующие пункты: акцент на теоретическую подготовку, проблема трудоустройства выпускников, сокращение бюджета на образовательные программы, устаревающие учебные материалы и методы их подачи. Данный перечень можно считать обще известным, и он относятся к классическому процессу обучения.

Однако, не менее важной составляющей образовательной системы является внеучебные мероприятия, так как это обширное поле для реализации развития как самих студентов, так и образовательного учреждения.

Разработанная анкета содержала следующие группы вопросов: общие вопросы, вопросы о мотивации и демотивации, и группа вопросов о том какие мероприятия имеются и каких не хватает. В опросе приняли участие 108 студентов, обучающихся на 1–3 курсах по направлению информационная безопасность.

Исследование показало низкую вовлечённость студентов во внеучебные мероприятия об этом свидетельствуют следующие показатели: (36%) – не принимают участие и (40%) – принимают участие лишь иногда и наиболее предпочитаемая роль – наблюдатель. В ответах на вопрос о направленности мероприятий, в которых вы принимаете участие, лидирует вариант ответа «затрудняюсь ответить», это является дополнительным маркером очень низкой вовлеченности, далее выделяют следующие направления: творчество, спорт, волонтерство. Также фиксируется высокий спрос на следующие мероприятия: встречи с профессионалами и экспертами – (59%), мастер-классы и тренинги по специальности – (58%), мероприятия для развития личных и профессиональных навыков (soft skills) – (54%). Спрос на такого рода мероприятия может свидетельствовать о том, что студенты хотят видеть ВУЗ не как площадку для развлечений, а как перспективу профессионального роста.

Главные мотивационные факторы – новые знакомства – (44%) и возможность усиления резюме – (34%). Основные демотиваторы – высокая учебная нагрузка – (54%), отсутствие практической пользы от участия в некоторых внеучебных мероприятиях – (40%), малое количество внеучебных мероприятий предоставляемых ВУЗом в сфере профессиональной деятельности – (30%).

Результаты анкетирования показывают, что внеучебная жизнь университета не соответствует современным запросам студентов, что требует пересмотра форматов как образовательного процесса, так и организация внеучебной деятельности .

Список литературы

1. Тодис Л.М., Виноградова Т.В., Андронычева А.С. Современные проблемы высшего образования в России и возможные пути их решения. – 2022 – [Электронный ресурс] – https://cyberleninka.ru/article/n/sovremennye-problemy-vysshego-obrazovaniya-v-rossii-i-vozmozhnye-puti-ih-resheniya/viewer (дата обращения 20.09.2025)

УДК 004.056

А.А. ХОРЕВ

Национальный исследовательский университет «МИЭТ», Москва

ПОКАЗАТЕЛИ И КРИТЕРИИ ОЦЕНКИ НИРС

В соответствии с положением об открытом всероссийском конкурсе на лучшую НИРС оценка представленных работ проводится экспертами на основе 6 показателей. По каждому показателю оценка НИРС отражается экспертами в баллах от 1 до 5. Однако критерии выставления баллов по каждому показателю в положении отсутствуют. С целью повышения объективности оценки конкурсных работ экспертами предложены уточненные показатели оценки и критерии выставления от 1 до 5.

В соответствии с «Положением об открытом всероссийском конкурсе на НИРС» (далее – положением) оценка представленных конкурсных работ проводится экспертами на основе следующих показателей: 1) актуальность работы; 2) научный уровень работы; 3) обоснованность выводов и результатов работы; 4) степень достижения цели работы и полнота решения поставленной задачи; 5) перспективность использования результатов работы в практической деятельности; 6) грамотность изложения, качество оформления работы.

По каждому показателю оценка НИРС отражается экспертами в баллах от 1 до 5. Однако критерии выставления баллов по каждому показателю в положении отсутствуют, поэтому при проведении экспертизы НИРС большую роль играет субъективные факторы. Кроме этого, по некоторым показателям, например, «актуальность работы» довольно трудно обосновать критерии выставления баллов.

С целью повышения объективности оценки НИРС экспертами предложено оценку НИРС проводить по следующим показателям: 1) структура работы, качество ее оформления и грамотность изложения материала; 2) содержание работы; 3) научный уровень работы; 4) новизна выполненной работы; 5) практическое значение выполненной работы. По каждому показателю обоснованы критерии выставления баллов от 1 до 5.

В качестве примера далее приведены критерии начислении 5 баллов по каждому из показателей:

1. Структура работы, качество ее оформления и грамотность изложения материала: структура НИРС соответствует требованиям ГОСТ 7.32-2017 и содержит: титульный лист; реферат; содержание; термины и определения (при необходимости); перечень сокращений и

обозначений; введение; основную часть; заключение; список использованных источников; приложения (при необходимости). Основная часть содержит разделы (подразделы, пункты), каждый из которых отражает отдельный вопрос исследований. Работа написана технически грамотно, оформлена аккуратно. Имеются несущественные стилистические ошибки. Текст, чертежи, рисунки и схемы, формулы, список используемых источников соответствуют требованиям ГОСТ и ЕСКД

2. Содержание работы: содержание элементов НИРС полностью соответствует требованиям ГОСТ 7.32-2017. В работе описаны объект и предмет исследований. Предмет исследований относится к направлениям исследований паспорта научных специальностей 2.3.6 и 1.2.4. Сформулирована цель работы и вопросы исследований. В работе достаточно полно представлены все результаты исследований.

3. Научный уровень работы: корректно описаны объект и предмет исследований. Корректно сформулирована цель работы и вопросы исследований. Тема (наименование) работы отражает предмет и цель исследований. Описаны используемые методы исследований. Сформулированы полученные научные результаты и обоснована их новизна, достоверность и практическая значимость. Все предложения (решения, результаты) математически, логически или экспериментально обоснованы (доказаны). Математический аппарат применен корректно. Все выводы подтверждены результатами исследований. Список литературы отражает современное состояние работ в данной области исследований и содержит не менее 20 источников. Доля оригинального текста (включая самоцитирование) составляет не менее 75%. Все заимствованные материалы (тексты, формулы, рисунки, таблицы) приведены со ссылками на источники.

4. Новизна выполненной работы: основные результаты работы обладают новизной. Новизна полученных результатов подтверждена патентом на изобретение или проведено сравнение полученных результатов с результатами исследований других авторов и обоснована их новизна. Результаты работы докладывались авторами на Международных или Всероссийских научных конференциях, по результатам которых выпущены сборники докладов (трудов), включенных в РИНЦ.

5. Практическое значение выполненной работы: основные результаты работы имеют практическое значение и реализованы. Результаты реализации подтверждены актами внедрения, содержащими сведения об объекте внедрения и роли соискателя в разработке данного объекта.

УДК 004.056

А.А. ХОРЕВ

Национальный исследовательский университет «МИЭТ», Москва

О ТЕРМИНОЛОГИИ В ОБЛАСТИ КИБЕРБЕЗОПАСНОСТИ

Используемые в научных публикациях в области кибербезопасности основные термины и определения имеют неоднозначную трактовку, что вызывает значительные трудности в понимании их сущности. В данной статье предприняты попытки систематизации и уточнения формулировок основных терминов, используемых в области кибербезопасности.

Используемые в научных публикациях в области кибербезопасности основные термины и определения имеют неоднозначную трактовку, что вызывает значительные трудности в понимании их сущности. Приведу лишь два совершенно разных определений самого термина «кибербезопасность»:

Кибербезопасность (киберзащита) – действия, необходимые для предотвращения неавторизованного использования, отказа в обслуживании, преобразования, рассекречивания, потери прибыли, или повреждения критических систем или информационных объектов. Кибербезопасность включает в себя понятия идентификации, аутентификации, отслеживаемости, авторизации, доступности и приватности [1].

Кибербезопасность (КБ) – это состояние защищенности активов объекта КБ от деструктивного воздействия опасностей на объект КБ в сфере КБ, при котором возможный ущерб активам объекта КБ не будет превышать допустимый уровень [2].

В данной статье предприняты попытки систематизации и уточнения формулировок основных терминов, используемых в области кибербезопасности.

Информационная инфраструктура – совокупность систем, средств и технологий обработки информации.

К системам обработки информации относятся:

Автоматизированная система – система, состоящая из комплекса технических средств, осуществляющих обработку информации в соответствие с заданной информационной технологией, и персонала, обеспечивающего его функционирование.

Информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств и систем.

Компьютерная сеть – сеть, узлы которой состоят из компьютеров и аппаратуры передачи данных, а ветви которой являются линиями передачи данных.

Телекоммуникационная система – технологическая система, предназначенная для передачи информации по линиям связи

Обработка информации – совокупность операций сбора, накопления, ввода, вывода, приема, передачи, записи, хранения, регистрации, преобразования, отображения и уничтожения информации.

Информационные технологи – методы, процессы и алгоритмы обработки информации и способы их осуществления.

Угроза безопасности информации – совокупность явлений, действий или процессов (в том числе воздействие программных или программно-аппаратных средств), результатом которых может быть нарушение безопасности информации.

Киберугроза – угроза воздействия программных и (или) программно-аппаратных средств на объекты информационной инфраструктуры с целью нарушения их функционирования и (или) нарушения безопасности информации, обрабатываемой такими объектами.

Кибератака (**компьютерная атака)** – целенаправленное воздействие программных и (или) программно-аппаратных средств на объекты информационной инфраструктуры с целью нарушения их функционирования и (или) создания угрозы безопасности информации, обрабатываемой такими объектами.

Кибербезопасность – состояние защищенности объектов информационной инфраструктуры от киберугроз.

Киберустойчивость – способность объектов информационной инфраструктуры функционировать в условиях кибератак.

Список литературы

1. ГОСТ Р 56205-2014. Сети коммуникационные промышленные Защищенность (кибербезопасность) сети и системы. Часть 1-1. Терминология, концептуальные положения и модели. – М.: Стандартинформ, 2014. – 76 с.

2. Толстой А.И. Таксономия понятий в области кибербезопасности. Безопасность информационных технологий. – М.: – 2024. – Т. 31, № 2(56) – С. 158–175. URL:https://bit.spels.ru/index.php/bit/article/view/1614.

УДК 004.056

А.И. ТОЛСТОЙ

Национальный исследовательский ядерный университет «МИФИ», Москва

КАТЕГОРИРОВАНИЕ ПОНЯТИЙ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Рассматриваются результаты категорирования понятий, отнесенных к области информационной безопасности. Определена совокупность понятий (терминов, представляющих понятия), которые могут быть использованы при построении системы понятий на основе использования принципов таксономии (систематики).

Введение

Современная область профессиональной деятельности (ОПД), относящейся к информационной безопасности (ИБ), имеет обширную терминологическую базу [1]. В настоящее время актуальным является построение научно-обоснованной системы понятий, которая бы позволила, с одной стороны, уточнить определения терминов, представляющих соответствующие понятия, а с другой – обосновано выбрать термины и определения для новых понятий, появляющихся как результат развития рассматриваемой ОПД.

Постановка задачи

Анализ результатов, полученных при реализации первой попытки создания такой системы понятий [2] показал невозможность построения научно обоснованной системы понятий в области ИБ, структура которой обладала бы базовыми признаками применимости принципов таксономии (теории классификации и систематизации сложно организованных областей действительности). Причины: (1) нарушение требований однозначности между понятием и термином, его представляющим; (2) присутствие среди используемых на практике понятий, которые не могут быть отнесены к известным категориям понятий. Была поставлена задача исследовать категории понятий в области ИБ, которые могут быть использованы при их систематизации.

Результаты

При систематизации понятий выделяют следующие наиболее общие категории понятий [2, 3]:

- категорию предметов (объектов): материальные физические (технические устройство, система); нефизические (логический объект,

процесс, система); человек; социотехнические системы; информация, представленная в определенных формах (сообщение, данные);

- категорию процессов (действий во времени);
- категорию свойств (качественные признаки и количественные характеристики предметов (объектов) и процессов).

В таблице определены категории понятий, представленных соответствующими терминами, относящиеся к области ИБ.

Термин	Объект	Процесс	Свойство
Информационная безопасность	-	-	-
Информационная безопасность объекта	-	-	+
Актив объекта	+	-	-
Свойство актива объекта	-	-	+
Опасность (источник опасности)	+	-	-
Угроза	-	-	-
Информационные сфера, пространство, среда	+	-	-
Ущерб	-	-	+
Риск	-	-	+
Обеспечение ИБ объекта	-	+	-
Система обеспечения ИБ объекта	+	-	-
Информации	+	-	-
Человек	+	-	-

Анализ данных показывает, что понятия «информационная безопасность» и «угроза» не поддаются категорированию. Поэтому систематизация понятий возможна только для области «информационная безопасность объекта» и замены понятия «угроза», например, на «источник опасности» или «источник угрозы».

Список литературы

1. Попов С.В., Рачкова Е.В., Черемушкин А.В. Информационная безопасность. Глоссарий. Под ред. С. Пазизина. – М.: Медиа группа «Авангард», 2025. – 366 с.

2. Толстой, Александр И. Систематика понятий в области информационной безопасности. Безопасность информационных технологий, [S.1], т. 30, № 1, с.130-148, 2023.

3. «Рекомендации по основным принципам и методам стандартизации терминологии». Рекомендации по межгосударственной стандартизации РМГ 19-96. Введены в действие с 1 июля 1998 г. (Постановление Госстандарта России от 21 апреля 1998 г. № 135).

ИМЕННОЙ УКАЗАТЕЛЬ АВТОРОВ СТАТЕЙ

Третья Всероссийская научно-техническая конференция «Кибернетика и информационная безопасность»

«КИБ-2025»

Сборник научных трудов

Том 2

Ответственный редактор И.М. Ядыкин

Подписано в печать 20.11.2025. Формат 60x84 1/16.
Печ. л. 12,75. Уч.-изд. 12,75. Тираж 160 экз.
Изд. №024-2. Заказ № 55

Национальный исследовательский ядерный университет «МИФИ»
Типография МИФИ
115409, Москва, Каширское ш. 31