МТУСИ

ФУМО ВО ИБ

СОВРЕМЕННЫЕ ТЕНДЕНЦИИ РАЗВИТИЯ МЕТОДОВ И ТЕХНОЛОГИИ ЗАЩИТЫ ИНФОРМАЦИИ

Сборник научных трудов
по материалам III Всероссийской
научной школы-семинара

МОСКВА 2023

МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ
Ордена Трудового Красного Знамени федеральное государственное бюджетное образовательное учреждение высшего образования
«Московский технический университет связи и информатики»
(МТУСИ)

Федеральное учебно-методическое объединение в сфере высшего образования по УГСНП 10.00.00 «Информационная безопасность»
(ФУМО ВО ИБ)

25-27 октября 2023 г.

III ВСЕРОССИЙСКАЯ НАУЧНАЯ ШКОЛА-СЕМИНАР

СОВРЕМЕННЫЕ ТЕНДЕНЦИИ РАЗВИТИЯ МЕТОДОВ И ТЕХНОЛОГИЙ ЗАЩИТЫ ИНФОРМАЦИИ

СБОРНИК ТРУДОВ

Москва – 2023

УДК 004.056(082)
ББК 16.8я43
Т33

Сборник трудов III Всероссийской научной школы-семинара «Современные тенденции развития методов и технологий защиты информации». Москва, МТУСИ, 25-27 октября 2023 г. – М., 2023. – 332 с.

ПРОГРАММНЫЙ КОМИТЕТ:

ISBN 978–5–6050465–6–1

УДК 004.056(082)
ББК 16.8я43
Т33

СОДЕРЖАНИЕ

РАЗДЕЛ 4. НАУЧНЫЕ ДОКЛАДЫ ГРАНТОПОЛУЧАТЕЛЕЙ 2023 ГОДА – СОИСКАТЕЛЕЙ УЧЁНОЙ СТЕПЕНИ КАНДИДАТА НАУК

РАЗДЕЛ 1. НАУЧНЫЕ ДОКЛАДЫ ГРАНТОПОЛУЧАТЕЛЕЙ 2022 ГОДА – СОИСКАТЕЛЕЙ УЧЁНОЙ СТЕПЕНИ ДОКТОРА НАУК

Золотарев В.В.
Сибирский государственный университет науки и технологий им. акад. М.Ф. Решетнева,
заведующий кафедрой, к.т.н., доц.,
zolotorev@sibsau.ru

О ПРОБЛЕМАХ И ЗАДАЧАХ ЗАЩИТЫ ИНФОРМАЦИИ ДЛЯ ПЕРЕХОДНЫХ СОСТОЯНИЙ ЦИФРОВОЙ ТРАНСФОРМАЦИИ ТЕХНОЛОГИЧЕСКИХ ПРОЦЕССОВ

Аннотация: Проблемы защиты информации в переходных состояниях цифровой трансформации – следствие разрыва между исходным (и, вполне вероятно, защищенным состоянием) технологического процесса и прогнозируемыми или случайными переходными состояниями, возникающими в процессе цифровой трансформации.

Основными проблемами, рассмотренными ниже, являются децентрализация (временная или реализованная как технология), эксфильтрация данных, отсутствие регламентов работы с новыми функциональными элементами (на примере цифровых двойников), недостатки применимых к управлению данными и управлению знаниями политик безопасности.

В работе кратко представлена концепция, объединяющая четыре уровня управления информационной безопасностью, проблемы переходных состояний цифровой трансформации технологического процесса и некоторые возможные пути их решения.

Схема, предложенная в работе, основана на изучении практических ситуаций и может быть применяться в задачах экспертной оценки, моделирования или развертывания систем защиты информации в переходных состояниях цифровой трансформации технологических процессов.

***Ключевые слова*:** управление информационной безопасностью, децентрализация, эксфильтрация данных, переходное состояние, цифровая трансформация.

Введение. Актуальность темы исследования определяется следующими исходными позициями:

1. Управление информационной безопасностью в целом должно рассматриваться как сложный многоуровневый процесс, который часто не воспринимается как единая система и как следствие теряет часть эффективности или не может быть интегрирован в основные технологические или бизнес-процессы организации. Кроме того, существует недооценка сложности этого процесса, его увязки со зрелостью процессов организации; из-за этого эффективность управления информационной безопасностью также может быть снижена.

2. По-видимому в настоящий момент классические подходы к управлению информационной безопасностью должны быть дополнены, поскольку в реальных производственных, образовательных и иных системах появились новые функциональные элементы. К примеру, создание и использование тестового контура или цифрового двойника, внедрение управления на основе данных или систем управления знаниями неизбежно меняет

ландшафт угроз и не может (не должно) игнорироваться службой информационной безопасности организации.

3. На уровне концепции необходимо целостное видение управления информационной безопасности как набора требований, распространяющихся на все смежные вопросы для реализации систем защиты информации – от развертывания инфраструктуры технологических или бизнес-процессов (информационной, технологической) до поиска и анализа случаев эксфильтрации чувствительной информации.

При этом можно отметить, что целевой моделью организации с позиций цифровой трансформации является формирование единого цифрового пространства, базиса для реализации основных процессов [1]. Это означает как другой уровень взаимодействия между процессами внутри единого пространства, так и другой уровень контроля и управления безопасностью в нем (в том числе для новых функциональных элементов).

Степень проработанности темы:

Следовательно, переход организации любого типа к целевой модели цифровой трансформации – не обычная транспортная задача, поскольку генерируемые изменения содержат качественные переходы для отдельных процессов и организации в целом. При этом, как указывают авторы связанных работ, нормой является конфликт интересов, дублирование задач, снижение эффективности использования ресурсов [2].

Проблемы и задачи защиты информации переходных процессов, подобных анализируемым в настоящем исследовании, встречаются в различных областях деятельности. В частности, для образовательных систем характерны проблемы защиты информации при управлении на основе данных [3-5], в том числе с элементами использования цифровых двойников; для индустриальных систем – проблема интеграции новых элементов в управляющие процессы и формирования систем управления информационной безопасностью в целом [6]. На уровне подобных работ интересно рассмотрение типовых информационных потоков и наборов мер контроля информационной безопасности. Большой областью исследований является стандартизация для управления информационной безопасностью. Не смотря на то, что стандарты в этой области приняты и активно применяются, их активное улучшение продолжается и сейчас, в частности [7] проводится анализ стандартов безопасности, различных политик безопасности, стандартов и руководств, применимых к задаче защиты информации.

Ранее исследовались оптимизационные задачи различного типа, решение которых применимо к модели управления информационной безопасностью. В частности, в работе [8], формируя модель управления информационной безопасностью, сосредоточились на оптимизационной задаче, отталкиваясь от ограниченности ресурсов. Подход авторов статьи заключается в возможности многоуровневой (отличающейся по сложности и ресурсоемкости) системы защиты и риск-ориентированном порядке действий.

Новые функциональные элементы, реализуемые при цифровой трансформации, также изучаются в различных аспектах их применения. Можно отметить, к примеру, сервис-ориентированные платформы [9].

Также, по-видимому, важное значение имеет и будет иметь работа с дестабилизирующими факторами, особенно в условиях неопределенности, что характерно для переходных состояний. В частности, существуют исследования подобного типа для управляющих механизмов безопасности информационной среды [10].

Активно изучается также и проблема оценки уровня зрелости, упомянутая выше [11].

Целью исследования, результаты которого приведены ниже, является решение следующей задачи: предложить алгоритмы и модель управления информационной безопасностью с учетом требований к новым функциональным элементам цифровой среды, контролю эксфильтрации данных и переходным состояниям цифровой трансформации бизнес-процессов.

Новыми результатами исследования, представленными ниже, стали:

1. Предложенная и детализированная четырехуровневая модель управления информационной безопасностью, включающей слои управления данными и управления знаниями, для описания процессов управления информационной безопасностью, затрагивающих несколько уровней этой модели;

2. Формирование новых устойчивых связей поддерживающих процессов управления информационной безопасностью на уровне отдельных задач с учетом четырехуровневой модели с акцентом на уровень данных.

Примеры переходных состояний цифровой трансформации процесса. При реализации переходных процессов цифровой трансформации важным ограничивающим параметром является время. Кроме того, поскольку задачи имеют сложные взаимные связи, то решение отдельной задачи должно быть увязано по времени с последующими и предыдущими, для достижения заданных эффектов в общем плане (табл. 1).

Табл. 1. Примеры задач управления информационной безопасностью в переходных состояниях цифровой трансформации

Задача	**Возможность моделирования времени перехода**	**Возможность формализации процесса перехода**	**Возможность привязки к смежным задачам**
Обеспечение закупочной деятельности, контрактования и поставок	Подзадачи (пример): Расчет времени оценки выполнения требований ИБ	Подзадачи (пример): Моделирование процессов управления требованиями	Подзадачи (пример): Мониторинг цепи поставок
Формирование организационно-распорядительной документации в области управления данными	Подзадачи (пример): Расчет времени проверки данных на конфиденциальность	Подзадачи (пример): Разработка регламента работы с данными	-

Все задачи информационной безопасности должны быть интегрированы (наиболее применимо – в виде управления рисками) в технологические и бизнес-процессы организации. Управление рисками на уровне технологии и информационных систем дает возможность контроля эффективности процесса и количественной оценки его характеристик, результатов, промежуточных (переходных) состояний.

Такие способы интеграции могут существовать на уровне процессов управления организацией, управления информационной безопасностью, обеспечивающих и основных процессов.

Децентрализованные системы. Одной из основных проблем переходных состояний является децентрализация и асинхронность функционирования основных защищаемых систем организации. При этом адаптивность требований информационной безопасности должна быть достаточной для реализации применимых политик информационной безопасности и

достижения необходимого уровня риска для любого переходного типа децентрализованной системы, поскольку на практике переходные состояния систем или их элементов могут предполагать децентрализованное управление в достаточно больших интервалах времени или постоянно.

Такие задачи возникают в системах управления событиями, управления инцидентами, центров обработки данных по компьютерным атакам, управления информационной безопасностью в целом [12].

Для систем с децентрализованным управлением возникает отдельная задача синтеза систем защиты информации на основе комплексного подхода. Кроме того, усложняется задача управления ресурсами и активами, обнаружения угроз, в том числе динамического, а также взаимодействия между центрами принятия решений в подобной системе. Для переходных состояний, предполагающих децентрализованное управление, возможно применять элементы интеллектуальных технологий [13, 14].

Проблемы защиты информации для управления на основе данных. При реализации отдельных концепций, лежащих в основе цифровой трансформации процессов организации, неизбежно возникают новые проблемы защиты информации и необходимость генерации новых способов их решения. Одной из таких проблем является управление на основе данных [15].

Краткое рассмотрение проблем управления на основе данных сводит проблематику защиты информации к минимум трем основным моментам:

1. Агрегация данных, валидация и верификация данных предполагают, что возникает задача создания безопасных алгоритмов, реализующих протоколы доступа к данным, в том числе для аналитических задач, задач обработки больших данных, задач обезличивания и пр. Таким задачам не уделяется достаточного внимания как для переходных процессов цифровой трансформации, так и для основных бизнес-процессов, реализованных в единой цифровой среде, что является причиной утечек данных и других инцидентов информационной безопасности.

2. Управление на основе данных предполагает, что формируется способ или технология контроля над данными, что является отдельной задачей для службы информационной безопасности и смежных структур. Примером применения такой технологии контроля является, к примеру, работа с поставщиками услуг в части передачи клиентской информации.

3. Неконтролируемое распространение данных автоматическими алгоритмами сбора и анализа данных (далее – эксфильтрация данных). Эта проблема может возникать как для случая неумышленного (ошибочного) распространения, так и для случая умышленного извлечения данных. Должны существовать протоколы контроля эксфильтрации данных, постоянно применяемые в ситуациях автоматического или автоматизированного сбора и анализа данных.

Некоторые способы решения указанных проблем приведены на основе существующих и применимых мер контроля ниже (рис. 1).

При этом в существующих моделях управления информационной безопасностью данные процессы на практике либо не реализуются, либо реализуются, но эффективность их остается низкой.

В данной задаче важным аспектом исследования является то, что применение алгоритмов управления информационной безопасностью должно учитывать не только

инфраструктурные и процессные требования, но и опираться на разработанные ранее (при достаточном уровне зрелости организации) регламенты работы с данными. На уровне концепции для определенных типов организаций (организаций с распределенной сетью филиалов, например) это требование является обязательным.

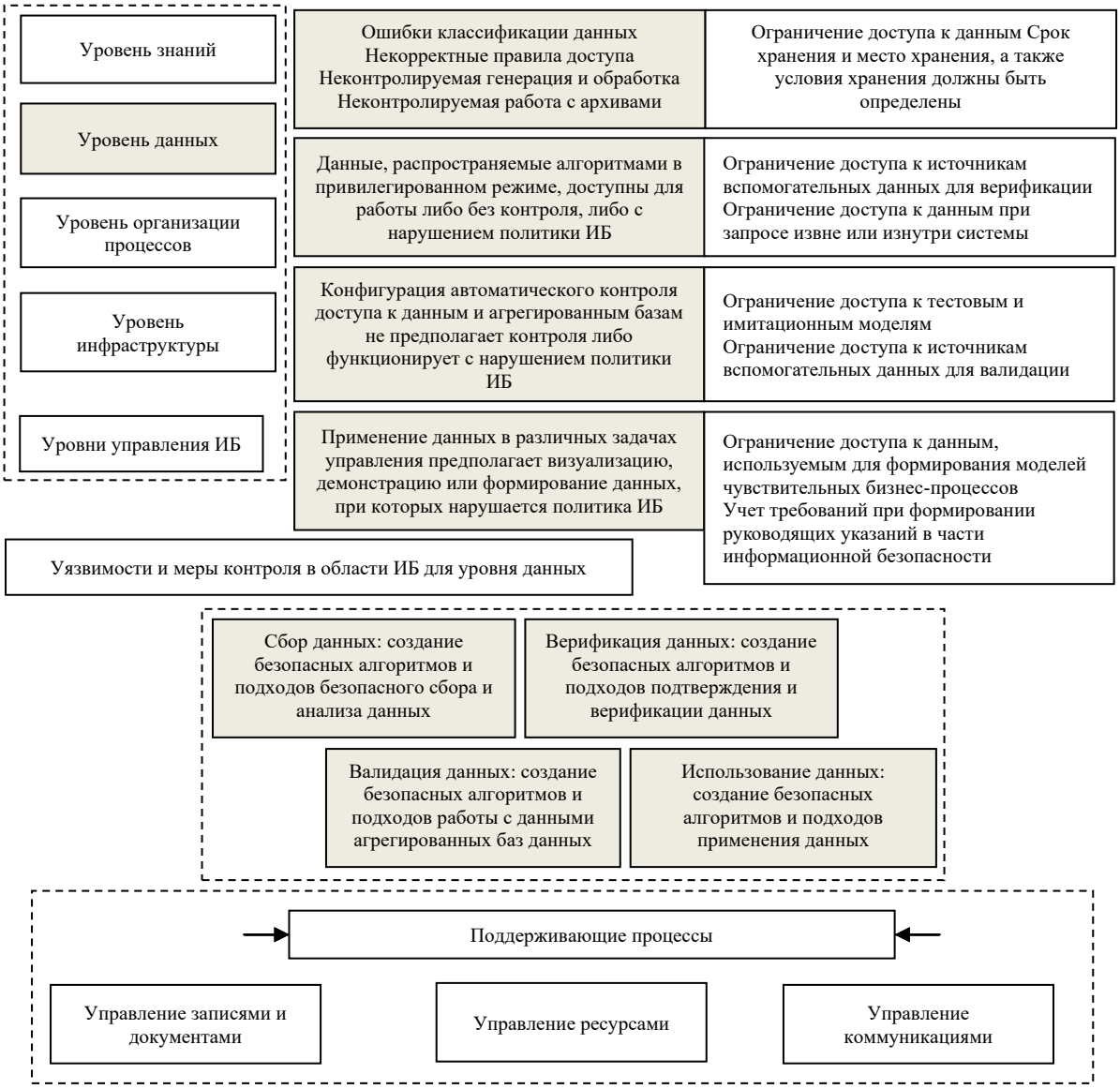


Рис. 1. Решение проблем защиты информации для управления на основе данных

При этом должны быть учтены и сложные моменты идентификации чувствительных данных, к примеру, в рамках повторной верификации и для работы с неполными (поврежденными, остаточными) данными.

Важный момент для уровня данных – это работа с непомеченными данными, потенциально требующими разграничения доступа. Часто для таких данных существует трудность выявления, связанная с ошибками контентного анализа, недостатка или невозможности сформировать шаблоны для сравнения, сложности автоматического тегирования (или маркировки).

Известны решения по поиску и тегированию конфиденциальной информации, к примеру, в патентах [16-17] и ряде смежных работ предполагается следующий результат

подобного поиска – повышение точности классификации конфиденциальной информации за счет обработки полученных данных с помощью ансамбля нейронных сетей, в ходе которой данным в каждой ячейке таблицы присваивается тег, соответствующий заданному типу конфиденциальной информации. При этом предобработка текстовой информации предполагает приведение ее к виду, пригодному для анализа, в частности векторного представления [18].

Очевидно, что в этой области исследований требуется совершенствование алгоритмов контроля над данными, в том числе и для нетегированной информации, потенциально чувствительной для организации. В исследовании в рамках тестирования алгоритмов применялись алгоритмы контроля на основе анализа метаданных.

Также при реализации управления на основе данных возникает (и должна решаться) задача контроля автоматизированных и автоматических коммуникаций процессов и технологических элементов, таких как программные роботы или коннекторы источников данных.

Эти коммуникации могут быть либо не полностью контролируемыми с позиций распространения конфиденциальной информации (или иных типов информации, контроль над которыми может представлять интерес для организации), либо находиться в состоянии неполного контроля в определенных переходных состояниях организационных и информационных систем.

Исследование предполагает анализ и фиксацию задач по управлению информационной безопасностью автоматических и автоматизированных коммуникаций, а также рекомендации по внедрению алгоритмов контроля, по введению строгих и слабых (основанных на риск-ориентированном подходе) требований к контролю эксфильтрации данных, что придает гибкость задачам управления безопасностью и работы с информационными ресурсами организации.

Управление знаниями в информационной безопасности. Здесь, на уровне концепции, возникает проблема следующего вида: на уровне управления знаниями существует необходимость получить доступ к как можно большему количеству источников для сбора, анализа и верификации информации; с точки зрения информационной безопасности это будет нарушением принципа минимизации полномочий и локализации объектов защиты информации в инфраструктуре организации. Если говорить о причинах такого противоречия, то даже на уровне основополагающих стандартов поясняется, что «управление знаниями направлено на то, чтобы заинтересованные стороны получали нужную информацию в надлежащем формате, на нужном уровне и в нужное время, в соответствии с их уровнем доступа и другими применимыми политиками. Для этого необходима процедура приобретения знаний, включающая в себя формирование, сбор и сохранение неструктурированных знаний, как формальных, документированных, так и неформальных, неявных» [19].

Управление знаниями может быть рассмотрено и как задача, связанная с упомянутыми выше новыми функциональными элементами, интегрируемыми в систему в ходе цифровой трансформации процессов. В частности, в исследовании рассматривается на экспериментальных примерах работа с различными типами цифровых двойников, тестовых контуров и исследовательских стендов, формирующих сценарии и тактики управления информационной безопасностью.

Даже задача изменения ландшафта атак с учетом применения цифровых двойников в образовании имеет множество интересных измерений, не говоря уже о ее приложениях к упомянутым выше, но мало рассматриваемым в литературе слоям управления данными и управления знаниями.

Ниже (рис. 2) на основе [20] показаны частные задачи управления информационной безопасностью цифрового двойника на указанных уровнях.

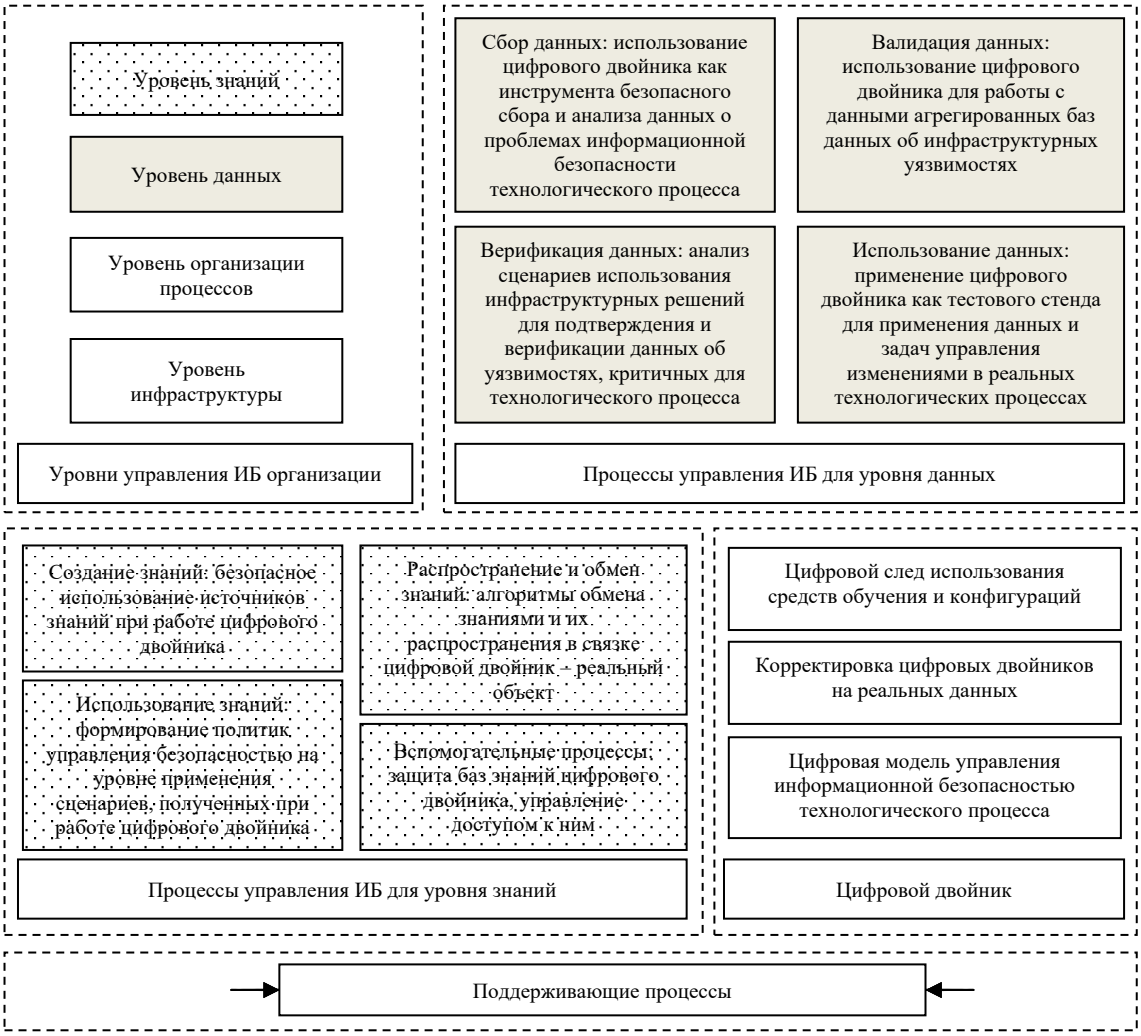


Рис. 2. Решение проблем защиты информации для управления на знаний (на примере использования цифрового двойника)

Подобное расширение может быть полезно при развертывании разных типов экспертных и советующих систем, систем поддержки принятия решений, ситуационных центров и особенно интересно для задач управления знаниями, опирающихся на описанный уровень данных, которые рассмотрены в отдельных исследованиях. На уровне концепции предполагается, что уровень знаний и уровень данных должны быть на постоянной основе интегрированы в процессы управления информационной безопасности (с соответствующими применимыми политиками информационной безопасности) и функционировать для любого типа новых функциональных элементов, реализуемых на различных этапах, в том числе в переходных состояниях, цифровой трансформации технологических и бизнес-процессов организации.

Выводы и перспективы исследования. Исследование сосредоточено на формировании пригодных в практике рекомендаций по построению концепции и процессных моделей управления информационной безопасности, учитывающей как традиционно рассматриваемые уровни управления инфраструктурой информационной системы и управления организационными процессами, так и новые, расширяющие модель уровень данных и уровень знаний.

В том числе, с практической точки зрения, исследование затрагивает вопросы неконтролируемого распространения (эксфильтрации) данных, поиска нетегированных (неразмеченных) конфиденциальных данных в открытых базах данных в том случае, если данные не поддаются эффективному контентному анализу. В исследовании также анализируются на уровне концепции и процессной модели задачи управления информационной безопасностью новых функциональных элементов (как пример: цифровые двойники, тестовые контуры, регламенты и автоматизированные (автоматические) алгоритмы работы с данными).

Основным результатом работы является детализованная четырехуровневая модель управления информационной безопасностью, основанная на концепции расширенного управления информационной безопасностью, включающего уровень данных и уровень знаний, а также новые функциональные элементы, реализуемые в переходных и итоговых состояниях цифровой трансформации, а также особенности переходных состояний цифровой трансформации.

В настоящей работе представлены некоторые примеры проведенных исследований.

СПИСОК ЛИТЕРАТУРЫ

1. Стратегия цифровой трансформации Сибирского государственного университета науки и технологий – Красноярск, 2021. – 117 с.

2. Офицеров, А.И. Концептуальные основы обеспечения комплексной безопасности критически важных объектов / А.И. Офицеров, О.О. Басов, С.С. Бачурин // Экономика. Информатика 2020. Том 47, № 1.

3. Кунц, Е.Ю. Использование компетентностной модели образовательной программы для принятия управленческих решений в образовательной организации / Е.Ю. Кунц, П.С. Ложников // Прикаспийский журнал: управление и высокие технологии. – 2022. – №2. – с. 27-34.

4. Попов, А.М., Золотарев В.В., Кунц Е.Ю. Проблема управления информационной безопасностью при создании цифрового двойника дисциплины / А.М. Попов, В.В. Золотарев, Е.Ю. Кунц // Прикаспийский журнал: управление и высокие технологии. – 2022. – №2. – с. 109-118.

5. Золотарев, В. В. Модель и алгоритм управления информационной безопасностью образовательной организации высшего образования с учетом требований управления на основе данных / В. В. Золотарев, М. А. Лапина // Прикаспийский журнал: управление и высокие технологии. – 2022. – № 4(60). – С. 107-118.

6. Park, S. Advanced Approach to Information Security Management System Model for Industrial Control System / S. Park, K. Lee // The Scientific World Journal – 2014 – vol. 2014, Article ID 348305, p. 1-13.

7. Toapanta, S. Analysis for the adoption of security standards to improve the management of securities in public organizations / S. Toapanta, M. Ronquillo, L. Gallegos, A.

Zezzatti // 2020 International Conference on Machine Learning and Intelligent Systems, MLIS-2020, Frontiers in Artificial Intelligence and Applications – 2020 – vol. 332, pp. 310 – 321.

8. Фомченкова, Л.В. Модель управления информационной безопасностью / Л.В. Фомченкова, А.В. Леонов // Journal of Economy and Business - 2019 - vol. 12-3 (58).

9. Wilk, J. Information security management model for integration platforms / J. Wilk // 2015 Forth International Conference on e-Technologies and Networks for Development (ICeND) – 2015 – pp. 1-6.

10. Зырянова, Т. Ю. Модель системы управления информационной безопасностью в условиях неопределенности воздействия дестабилизирующих факторов / Т. Ю. Зырянова // Автореферат диссертации на соискание ученой степени кандидата технических наук по специальность: 05.13.19 – Методы и системы защиты информации. – Томск, 2008.

11. Osamah, M. Adopting security maturity model to the organizations' capability model / M. Osamah, M. Iman, M. Sherif, E. Mazen // Egyptian Informatics Journal – 2021 – vol. 22, Issue 2, - pp. 193-199.

12. Дилигенская, А. Н. Модель и алгоритм управления информационной безопасностью образовательной организации высшего образования с учетом требований управления на основе данных / А. Н. Дилигенская, В. В. Золотарев, Н. Е. Карпова, С. В. Селигеев // Прикаспийский журнал: управление и высокие технологии. – 2023. – № 2(62). – С. 42-50.

13. Mukhin, V. Adaptive security system based on intelligent agents for distributed computer systems / V. Mukhin // Int. Conf. on Development and Application Systems (DAS) – 2016 (Suceava).

14. Zhang, B.-Y. Research on virus detection technique based on ensemble neural network and SVM / B.-Y. Zhang, J.-P. Yin, S.-L. Wang, X.-A. Yan // Neurocomputing – 2014 – Vol. 137 – pp. 24–33.

15. Трофимов, В.В. О концепции управления на основе данных в условиях цифровой трансформации / В.В. Трофимов, Л.А. Трофимова // Петербургский экономический журнал. 2021. №4.

16. Способ и система классификации данных для выявления конфиденциальной информации / Патент RU 2 759 786 C1. Владелец патента: Публичное акционерное общество "Сбербанк России" (ПАО Сбербанк) (RU) Автор: Теренин Алексей Алексеевич (RU) Начало действия: 2019.07.05 Публикация: 2021.11.17 Подача: 2019.07.05.

17. Способ и система классификации данных для выявления конфиденциальной информации в тексте / Патент RU 755 606 C2 Владелец патента: Публичное акционерное общество "Сбербанк России" (ПАО Сбербанк) (RU) Автор: Теренин Алексей Алексеевич (RU) Начало действия: 2019.10.16 Публикация: 2021.09.17 Подача: 2019.10.16.

18. Способ и система получения векторного представления электронного текстового документа для классификации по категориям конфиденциальной информации / Патент RU 2 775 358 C1 Владелец патента: Публичное акционерное общество "Сбербанк России" (ПАО Сбербанк) (RU) Автор: Вышегородцев Кирилл Евгеньевич (RU) Начало действия: 2021.09.24 Публикация: 2022.06.29 Подача: 2021.09.24

19. ITIL 4 Edition, ed. 2019. ISBN 9780113316076. – p. 5.1.4. Управление знаниями.

20. Использование цифрового двойника в задачах управления информационной безопасностью / А. Р. Касимова, В. В. Золотарев, Л. Х. Сафиуллина, А. С. Балыбердин // Прикаспийский журнал: управление и высокие технологии. – 2023. – № 1(61). – С. 48-58.

Иванов Д.В.
Самарский национальный исследовательский университет имени академика С.П. Королева,
доцент кафедры безопасности информационных систем, к.ф.-м.н., доц.,
dvi85@list.ru

ВЫЯВЛЕНИЯ АНОМАЛИЙ ТРАФИКА КОМПЬЮТЕРНЫХ СЕТЕЙ НА ОСНОВЕ МОДЕЛЕЙ С РАЗНОСТЬЮ ДРОБНОГО ПОРЯДКА

Аннотация: В докладе исследования предлагается комплекс моделей трафика компьютерных сетей на основе уравнений с разностями дробного порядка. Разработаны методы структурно-параметрической идентификации моделей трафика компьютерных сетей с длинной памятью при наличии ошибок в переменных на основе генетических алгоритмов, позволяющие выявлять аномалии трафика.

Ключевые слова: Моделирование трафика компьютерных сетей, аномалии трафика, временные ряды с длинной памятью, разности дробного порядка, ошибки в переменных, генетические алгоритмы.

.

Актуальность темы исследования. Обеспечение надлежащего уровня безопасности сетевых ресурсов и инфраструктур является в настоящее время эта проблема интенсивно исследуется и разрабатывается, а число новых атак растет, их глобальный охват и степень сложности требуют динамичного развития систем сетевой защиты.

Степень ее разработанности. Длинная память– это свойство, которое описывает корреляционную структуру высокого порядка временного ряда. В случае, если ряд характеризуется длинной памятью, то зависимость существует даже между далеко отдаленными друг от друга во времени наблюдениями. Поскольку длинная память создает в модели для среднего уровня ряда нелинейную зависимость в первые моменты распределения, то она генерирует в динамике ряда потенциально полезный для прогнозирования компонент.

Автокорреляции ряда с длинной памятью удовлетворяют такое соотношение: $\rho_k \approx c \cdot k^{-\alpha}$ при k $\to \infty$. Таким образом, убывание автокорреляций происходит по гиперболе. Это гиперболическое убывание автокорреляций противопоставляется экспоненциальному, характерному для процессов с короткой памятью (ARMA): $\rho_k \leq \cdot k^{-\alpha}$ где c – положительная константа и $0 < \alpha < 1$. В связи с тем, что длинная память является особой формой нелинейной динамики, она ставит под вопрос линейное моделирование и требует разработки на теоретическом уровне новых нелинейных моделей оценки поведения временных рядов, у которых идентифицируется наличие длинной памяти. В работах, где анализируют нестационарные временные ряды, уделяется внимание порядку интегрированности ряда, речь идет о значении параметра d процесса ARIMA (p, d, q)). Как правило, авторы ограничиваются выбором между d равным 0 и 1. Случай d = 0 отвечает короткой памяти ряда, тогда как при d = 1 можно сделать вывод о бесконечной памяти.

С другой стороны, существование короткой памяти означает, что следствия шока исчезнут достаточно быстро, при этом из поля зрения исследователей исчезает промежуточная ситуация, когда следствия шока окажутся временными, но продолжительными (то есть случай длинной памяти, или персистентности). Для решения этой проблемы Гренджер [1,2] предложил новый класс моделей ARFIMA (p, d, q), что допускает возможность использования нецелого параметра d .

Примером временных рядов с длинной памятью является трафик в компьютерных сетях [3-5].

Обзор методов по выявлению аномалий трафика приведен в статье [7]. Как следует из обзора для выявления аномалий трафика на сегодняшний день используются только модели ARFIMA и GARMA [8,9].

Цели и задачи работы. Целью работы является повышение защищенности информационных систем с помощью увеличения точности выявления аномалий трафика. Работа посвящена решению этой актуальной проблемы, связанные с этим направлением вопросы разработки соответствующего математического аппарата нуждаются в теоретической и практической проработке.

Научная новизна.

1. Разработаны методы структурно-параметрической идентификации линейных и нелинейных моделей с длинной памятью, описываемых уравнениями с разностями дробного порядка при наличии ошибок в переменных, которые сочетали бы в себе высокую точность оценивания параметров с требованиями малой априорной информации;

2. Разработаны критерии для идентификации ARX (autoregression with exogenous input, авторегрессионных с экзогенными входными данными) систем, описываемых уравнениями с разностями дробного порядка, при наличии помех наблюдений класса мартингал-разность. Разработаны критерии для различных частных случаев данных систем и помех. Доказана сильная состоятельность получаемых оценок параметров при применении критериев.

3. Разработаны критерии для идентификации ARX систем, описываемых уравнениями с разностями дробного порядка, при наличии коррелированных помех. Разработаны критерии для различных частных случаев данных систем и помех. Доказана сильная состоятельность получаемых оценок параметров при применении критериев.

4. Разработаны критерии для идентификации ARX систем, описываемых уравнениями с разностями дробного порядка, при отсутствующей или неполной информации об автокорреляционной функции помех. Доказана сильная состоятельность получаемых оценок параметров при применении критериев.

5. Разработаны критерии для идентификации нелинейных систем различных классов (класса Гаммерштейна, Винера, билинейных систем), описываемых уравнениями с разностями дробного порядка, наличии помех наблюдений. Доказана сильная состоятельность получаемых оценок параметров при применении критериев.

6. Разработаны эффективные численные реализации алгоритмов идентификации.

7. Разработана методология выявления аномалий трафика на моделях с длинной памятью, построенных по экспериментальным данным.

8. На основе разработанных алгоритмов прикладного программного обеспечения, исследование эффективности представленных в диссертации методов, алгоритмов и программ с помощью тестового статистического моделирования и на реальных реализациях трафика компьютерных сетей.

Теоретическая и практическую значимость работы. Теоретическая значимость заключается в том, что предложен единый подход для идентификации линейных и нелинейных систем различных классов, описываемых уравнениями с разностями дробного порядка при наличии помех наблюдений. На основе предложенного подхода построены и реализованы алгоритмы идентификации для различных классов помех, в том числе

нестационарных. Доказана сильная состоятельность оценок параметров для предложенных рекуррентных и нерекуррентных алгоритмов идентификации.

Практическая значимость диссертации заключается в том, что полученные алгоритмы и созданное на их основе программное обеспечение могут применяться для выявления аномалий трафика, а при решении практических задач в самых разных областях науки и техники, таких как: химия, эконометрика, машиностроение, экология, геофизические исследования, системы передачи информации, анализ временных рядов, автоматизированные системы управления технологическими процессами.

Методология и методы исследования. Методы исследования. В работе использованы: теория вероятностей, в том числе теория оценивания, математическая статистика, теория оптимизации, теория матриц, линейная алгебра, прикладное программирование.

Положения, выносимые на защиту.

1. Критерий для идентификации ARX систем, описываемых уравнениями с разностями дробного порядка, а также их рекуррентные, при наличии помех наблюдений класса мартингал-разность. Критерии для различных частных случаев данных систем и помех. Доказательство сильной состоятельности получаемых оценок параметров при применении критериев;

2. Критерий для идентификации ARX систем, описываемых уравнениями с разностями дробного порядка, при наличии коррелированных помех. Критерии для различных частных случаев данных систем и помех. Доказательство сильной состоятельности получаемых оценок параметров при применении критериев;

3. Критерии для идентификации многомерных ARX систем, описываемых уравнениями с разностями дробного порядка, при отсутствующей или неполной информации об автокорреляционной функции помех. Доказательство сильной состоятельности получаемых оценок параметров при применении критериев.

4. Критерии для идентификации многомерных нелинейных систем различных классов (класса Гаммерштейна, Винера, Вольтерра, билинейных систем), описываемых уравнениями с разностями дробного порядка, наличии помех наблюдений. Доказательство сильной состоятельности получаемых оценок параметров при применении критериев.

6. Численные реализации рекуррентных и нерекуррентных алгоритмов идентификации.

7. Прикладное ПО на основе предложенных алгоритмов. С помощью разработанных алгоритмов и программного обеспечения разработаны алгоритмы выявления аномалий трафика.

Степень достоверности и апробация работы. Достоверность и обоснованность результатов обоснована представленными математическими доказательствами теоретических результатов. Теоретические положения подтверждены результатами вычислительных экспериментов. Результаты работы были представлены на всероссийских и международных конференциях.

Краткое содержание диссертации с упором на результаты, полученные за период реализации научного проекта в рамках гранта

Рассматривается многомерная стационарная устойчивая ARX (autoregression with exogenous input, авторегрессия с экзогенными входными данными) система с дискретным временем ($i = \ldots, -1, 0, 1 \ldots$), описываемая следующим уравнениями с разностями дробного порядка:

$$z_i = \sum_{m=1}^{\bar{r}} b^{(m)} \Delta^{\beta^{(m)}} z_{i-1}^{(l)} + \sum_{m=1}^{r} a^{(m)} \Delta^{\beta^{(m)}} x_i + \varsigma_i \quad y_i = z_i + \xi_i,\ w_i = x_i + \zeta_i \tag{1}$$

где $\Delta^{\alpha^{(m)}} z_i = \sum_{j=0}^{i} \binom{\alpha^{(m)}}{j} z_{i-j}$, $\Delta^{\beta^{(m)}} x_i = \sum_{j=0}^{i} \binom{\beta^{(m)}}{j} x_{i-j}$,

$$\binom{\alpha^{(m)}}{j} = \frac{(-1)^j \Gamma\left(\alpha^{(m)} + 1\right)}{\Gamma(j+1)\Gamma\left(\alpha^{(m)} - j + 1\right)}, \quad \binom{\beta^{(m)}}{j} = \frac{(-1)^j \Gamma\left(\beta^{(m)} + 1\right)}{\Gamma(j+1)\Gamma\left(\beta^{(m)} - j + 1\right)}.$$

$$0 < \alpha^{(1)} \ldots < \alpha^{(\bar{r})},\ 0 < \beta^{(1)} \ldots < \beta^{(r)},\ \Gamma(\alpha) = \int_0^{\infty} e^{-t} t^{\alpha-1} dt.$$

z_i, y_i – ненаблюдаемая и наблюдаемая выходные переменные в выходном сигнале; x_i, w_i – ненаблюдаемая и наблюдаемая переменные во входном сигнале; ξ_i – помеха наблюдения в выходном сигнале; ζ_i – помехи наблюдения соответственно во входном сигнале. ς_i – ошибка в уравнении;

Для доказательства свойства состоятельности оценок будем предполагать, что для системы, входных сигналов и помех выполнены следующие неограничительные условия:

1. Множество $\tilde{\mathrm{B}}$, которому априорно принадлежат истинные значения параметров устойчивой линейной системы, является компактным.

2. Вектор входных переменных и истинные значения параметров удовлетворяет условию

$$\lim_{N\to\infty} \frac{1}{N} \sum_{i=1}^{N} \left(\varphi^{(i)}\right)\left(\varphi^{(i)}\right)^T = H \text{ п.н.},$$

где $\varphi^{(i)} = \left(\varphi_z^{(i)} \vdots \varphi_x^{(i)}\right)^T$, $\varphi_z^{(i)} = \left(\Delta^{\alpha^{(1)}} z_{i-1}, \ldots, \Delta^{\alpha^{(\bar{r})}} z_{i-1}\right)$, $\varphi_x^{(i)} = \left(\Delta^{\beta^{(1)}} x_i, \ldots, \Delta^{\beta^{(r)}} x_i\right)$,

H – положительно определенная матрица.

3. Случайные последовательности $\{\xi_i\}, \{\varsigma_i\}, \{\zeta_i\}$, удовлетворяющие условиям:

$E\left(\xi_{i+1} / F_\xi^{(i)}\right) = 0$, $E\left(\varsigma_{i+1} / F_\varsigma^{(i)}\right) = 0$, $E\left(\zeta_{i+1} / F_\zeta^{(i)}\right) = 0$ п.н.; $E\left(\xi_{i+1}^2 / F_\xi^{(i)}\right) < W_\xi$,

$E\left(\varsigma_{i+1}^2 / F_\varsigma^{(i)}\right) < W_\varsigma$, $E\left(\zeta_{i+1}^2 / F_\zeta^{(i)}\right) < W_\zeta$ п.н, $E\left(\varsigma_{i+1}^2\right) < \infty$, $E\left(\xi_{i+1}^2\right)^2 < \infty$, $E\left(\zeta_{i+1}^2\right) < \infty$ п.н.

где $F_\varsigma^{(i)}, F_\xi^{(i)}, F_\zeta^{(i)}$ – σ-алгебры, индуцированные семействами случайных величин $\{\varsigma_t, \xi_t, \zeta_t, t \in T_i\}$, $T_i = \{t; t \le i, t \in \mathrm{Z}_c$-множество целых чисел$\}$; $W_\varsigma, W_\xi, W_\zeta$ – случайные величины, $E\left(W_\varsigma\right) < \infty$, $E\left(W_\xi\right) < \infty$, $E\left(W_\zeta\right) < \infty$ п.н.

4. $\{x_i\}$ статистически не зависят от $\{\xi_i\}$, $\{\varsigma_i\}, \{\zeta_i\}$;

5. Помехи $\{\xi_i\}$, $\{\varsigma_i\}, \{\zeta_i\}$ и параметры системы $\alpha^{(m)}$, $\beta^{(m)}$, удовлетворяют условиям

$$\lim_{N\to\infty} \frac{1}{N} \sum_{i=1}^{N} \left(\varphi_{\xi\zeta}^{(i)}\right)\left(\varphi_{\xi\zeta}^{(i)}\right)^T = \lim_{N\to\infty} \frac{1}{N} \left[E \sum_{i=1}^{N} \varphi_{\xi\zeta}^{(i)} \left(\varphi_{\xi\zeta}^{(i)}\right)^T \right] = H_{\xi\zeta} \text{ п.н.},$$

$$H_{\xi\zeta}=\left(\begin{array}{c|c} H_\xi & 0 \\ \hline 0 & H_\zeta \end{array}\right), h_\xi^{(mm')}=\lim_{N\to\infty}\frac{1}{N}\sum_{j=0}^{N-1}\sum_{i=j}^{N-1}\binom{\alpha^{(m)}}{j}\binom{\alpha^{(m')}}{j}\xi_{i-j-1}\xi_{i-j-1},$$

$$h_\zeta^{(mm')}=\lim_{N\to\infty}\frac{1}{N}\sum_{j=0}^{N-1}\sum_{i=j}^{N-1}\binom{\beta^{(m)}}{j}\binom{\beta^{(m')}}{j}\zeta_{i-j}\zeta_{i-j},$$

причем H_ξ, H_ζ положительно определены.

Требуется определять оценки неизвестных коэффициентов динамической системы описываемой уравнением (1) по наблюдаемым последовательностям z_i, x_i при известных порядках $\overline{r}, r, \alpha^{(m)}, \beta^{(m)}$.

Будем искать оценки параметров в ввиде минимума нелинейной функции, числитель которой представляется сумму квадратов ошибок, а знаменатель дисперсию невязки:

$$\min_{\theta\in\tilde{\mathrm{B}}}\frac{\left\|Y-\Phi\theta\right\|_2^2}{\bar{\sigma}_\xi^2+\bar{\sigma}_\zeta^2+\theta^T H_{\xi\zeta}\theta} \tag{2}$$

где $\tilde{\varphi}^{(i)}=\left(\varphi_y^{(i)} \mid \varphi_w^{(i)}\right)^T$, $\theta=\left(b \mid a\right)^T$, $Y=\left(y_1,\ldots y_N\right)^T$, $\Phi=\left(\tilde{\varphi}^{(1)}, \ \ldots, \ \tilde{\varphi}^{(N)}\right)^T$.

Теорема 1. Пусть некоторый случайный процесс $\{y_i, i=\ldots-1,0,1,\ldots\}$ *описывается уравнением (1) с начальными нулевыми условиями и выполняются предположения 1-5. Тогда оценки* $\hat{\theta}(N)$*, определяемая выражением (2) с вероятностью 1 при* $N\to\infty$*, существует, единственная и является сильно состоятельной оценкой, т.е.* $\hat{\theta}(N)\xrightarrow[N\to\infty]{\text{П.Н.}}\hat{\theta}$.

Критерий путем замены переменных может быть сведен к задаче полных наименьших квадратов

$$\min_{\theta'\in\tilde{\mathrm{B}}'}\frac{\left\|Y'-\Phi'\theta'\right\|_2^2}{1+\theta'^T H'\theta'}. \tag{3}$$

Существует несколько подходов к минимизации полных наименьших квадратов (ПМНК). Первый подход основан на том, что решение задачи (ПМНК) требует вычисления минимального сингулярного числа расширенной матрицы $\left(\Phi', Y'\right)$ и соответствующего этому числу правого сингулярного вектора.

Проблема поиска сингулярного вектора является нелинейной векторной задачей. Ее численное решение сопряжено со значительными трудностями, связанными с устойчивостью алгоритмов поиска, вопросами сходимости, высокой вычислительной сложностью.

Второй подход основан на решении смещенной нормальной системы. что если выполняется условие

$$\left(\Phi'^T\Phi'-\sigma^2 I\right)\theta'=\Phi'^T Y. \tag{4}$$

При решении системы (4), нелинейной остается лишь скалярная задача поиска минимального сингулярного числа $\sigma=\sigma_{\min}\left(\Phi', Y'\right)$. Данная задача всегда хорошо обусловлена всегда хорошо обусловлена. Однако система (4) имеет значительно большее число обусловленности, чем решение задачи на основе правого сингулярного вектора

$$\kappa_2\left(\Phi'^T\Phi' - \sigma^2 I\right) = \frac{\sigma^2_{\max}\left(\Phi'\right) - \sigma^2 I}{\sigma^2_{\min}\left(\Phi'\right) - \sigma^2 I}$$

В работе предложена расширенная эквивалентная смещенной нормальной системе:

$$\left(\begin{array}{c|c} \sigma I & \Phi' \\ \hline \Phi'^T & \sigma I \end{array}\right)\left(\begin{array}{c} \sigma^{-1}\varepsilon \\ \hline \theta' \end{array}\right) = \left(\begin{array}{c} Y' \\ \hline 0 \end{array}\right), \tag{5}$$

где $\varepsilon = Y - \Phi'\theta$.

Теорема 2. Спектральное число обусловленности системы уравнений (4) определяется как

$$\kappa_2 = \frac{\sigma_{\max}\left(\Phi'\right) + \sigma}{\sigma_{\min}\left(\Phi'\right) - \sigma}. \tag{6}$$

Разработанные алгоритмы и программное обеспечение используются для усовершенствования алгоритмов обнаружения DDOS атак.

Известно, что трафик компьютерных сетей имеет свойства самоподобия и длинной памяти [3]. Для моделирования этих свойств трафика широко используются дробные разности и в частности модели ARFIMA (autoregressive fractionally integrated moving average) [4,5]. Применение модели ARFIMA сопряжено с рядом сложностей:

1. Предполагается, что на первом шаге точно, оценивается порядок дробного интегрирования. После чего может быть оценена целочисленная ARMA модель. В случае погрешности, оценки параметра дробного интегрирования ARMA модель может иметь длинную память, что обычно не учитывается и может сильно искажать модель.
2. Оценивание даже целочисленной модели ARMA на много сложнее чем оценивание авторегрессий высокого порядка.
3. Из классов моделей ARMA, авторегрессии, авторегрессия с аддитивным шумом, наилучшей разрешающей способностью для в задачах спектрального анализа в задачах спектрального анализа обладает авторегрессия с аддитивным шумом [10, 11].

Исходя из сказанного выше было использовано следующие семейство моделей.

1. Авторегрессии, описываемой уравнениями с разностями дробного порядка с помехой наблюдения в выходном сигнале

$$z_i = \sum_{m=1}^{r} b^{(m)}\Delta^{\alpha_m} z_{i-1} + \varepsilon_i, \;\; y_i = z_i + \xi_i. \tag{7}$$

2. FAR (Fractional differencing autoregressive) с помехой наблюдения в выходном сигнале

$$\Delta^{\alpha}\left(z_i - \sum_{m=1}^{r} b_0^{(m)} z_{i-m}\right) = \varepsilon_i, \;\; y_i = z_i + \xi_i. \tag{8}$$

4. GAR (Gegenbauer autoregressive) с помехой наблюдения в выходном сигнале

$$\Delta^{\alpha}\left(z_i - \sum_{m=1}^{r} b_0^{(m)} z_{i-m}\right) = \varepsilon_i, \;\; y_i = z_i + \xi_i, \tag{9}$$

где $\nabla_{\nu}^{\alpha} \equiv \left(1 - 2\nu q^{-1} + q^{-2}\right)^{\alpha}$ - разность Гэгенбаура, $0 < \alpha, \;\; 0 < \nu \le 1$ оператор сдвига назад $q^{-1} z_i = z_{i-1}$, которая представима в виде линейного фильтра

$$\nabla_{\nu}^{\alpha} z_i = \sum_{j=0}^{i} C_j^{\alpha}(\nu) z_{i-j},$$

$$C_j^{\alpha}(\nu) = \sum_{k=0}^{[j/2]} (-1)^k \Gamma(\alpha + j - k) \frac{(2\nu)^{j-2k}}{\Gamma(\alpha)\Gamma(k+1)\Gamma(j-2k+1)}.$$

Параметры идентифицированных моделей применяются в семействе детекторов использующих:

1. Ошибку прогнозирования процесса.
2. Порядок дробной разности, связанный с показателем Херста как $\alpha = H - 0.5$.
3. Спектральное представление полученное на основе оцененной авторегрессии.

Высокая точность разработанных методов оценивания авторегрессий с разностями дробного порядка позволяет улучшить показатели распознавания различных DDOS атак в компьютерных сетях.

Рекомендации и перспективы дальнейшей разработки темы. Разработанные алгоритмы и программы могут быть внедрены в существующие системы безопасности.

СПИСОК ЛИТЕРАТУРЫ

1. Granger, C.W., Joyeux, R.: An introduction to long-memory time series models and fractional differencing. J. Time Ser. Anal. 1(1), 15–29 (1980).

2. Hosking, J.R.M. Fractional differencing. Biometrika 1981, 68, 165–176.

3. Grossglauser M. On the relevance of long-range dependence in network traffic/Grossglauser M., Bolot J.C. –FRR.: Wapszawa, 1996. – 109 p.

4. Leland W.E., Taqqu M.S., Willinger W., and Wilson D.V. On the self-similarnature of ethernet traffic // IEEE/ACM Transactions of Networking, 2(1), 1994. P. 1–15.

5. Цыбаков Б.С. Модель телетрафика на основе самоподобного случайного процесса // Радиотехника. 1999.- № 5.С. 24–31.

6. Шелухин О.И., Осин А. В., Смольский С.М. Самоподобие и фракталы. Телекоммуникационные приложения. / Под ред. О. И. Шелухина. — М.: ФИЗМАТЛИТ, 2008. — 368 с. — ISBN 978-5-9221-0949-9.

7. M. Husák, J. Komárková, E. Bou-Harb and P. Čeleda, "Survey of Attack Projection, Prediction, and Forecasting in Cyber Security," in IEEE Communications Surveys & Tutorials, vol. 21, no. 1, pp. 640-660, Firstquarter 2019, doi: 10.1109/COMST.2018.2871866.

8. A. B. Abdullah, T. R. Pillai, and L. Z. Cai, “Intrusion detection forecasting using time series for improving cyber defence,” International Journal of Intelligent Systems and Applications in Engineering, vol. 3, no. 1, pp. 28–33, 2015.

9. T. R. Pillai, S. Palaniappan, A. Abdullah, and H. M. Imran, “Predictive modeling for intrusions in communication systems using GARMA and ARMA models,” in 2015 5th National Symposium on Information Technology: Towards New Smart World (NSITNSW), Feb 2015.

10. Guidorzi, R.; Diversi, R.; Vincenzi, L.; Mazzotti, C.; Simioli, V. Structural monitoring of a tower by means of MEMS-based sensing and enhanced autoregressive models. Eur. J. Control. 2014, 20, 4–13.

11. Guidorzi, R.; Diversi, R.; Vincenzi, L.; Simioli, V. AR+ noise versus AR and ARMA models in SHM-oriented identification. In Proceedings of the 23rd Mediterranean Conference on Control and Automation (MED), Torremolinos, Spain, 16–19 June 2015; pp. 809–814.

Когос К.Г.
НИЯУ МИФИ, доцент, зам. директора, к.т.н.,
kgkogos@mephi.ru

МЕТОД ОГРАНИЧЕНИЯ ПРОПУСКНОЙ СПОСОБНОСТИ ПУТЕМ ЗАШУМЛЕНИЯ ТРАФИКА

Аннотация: Данная статья посвящена разработке и исследованию метода противодействия утечке информации по скрытым каналам путем зашумления канала передачи информации. Были рассмотрены способы противодействия утечке информации путем случайного увеличения длин передаваемых пакетов, введения случайных задержек пакетов и генерации фиктивного трафика. Для рассмотренных способов противодействия были получены выражения для оценки максимальной остаточной пропускной способности скрытого канала в условиях противодействия.

Ключевые слова: СКРЫТЫЕ КАНАЛЫ, ПРОПУСКНАЯ СПОСОБНОСТЬ, УТЕЧКА ИНФОРМАЦИИ, ЗАЩИТА ИНФОРМАЦИИ, ЗАШУМЛЕНИЕ КАНАЛА

Пусть длины пакетов принимают значения на множестве $N_{l_{фикс}+n-1} \setminus N_{l_{фикс}-1}$, $l_{фикс}$, $L \in N$, где N_x — множество натуральных чисел, не превосходящих x. Предложен следующий способ увеличения длин передаваемых пакетов: длина каждого пакета, подлежащего отправке, увеличивается на количество битов, определяемое значениями случайной величины, равновероятно принимающей целочисленные значения на множестве $N_{\alpha-1} \bigcup \{0\}$, где α — параметр метода противодействия. Равномерное распределение представляет наибольшую неопределенность в распознавании получателем переданного по скрытому каналу символа, выбор множества значений случайной величины продиктован минимизацией дополнительной нагрузки на канал связи.

Заметим, что длина пакета не может стать больше максимально допустимой $n_{макс}$ (в нашем случае – $n_{макс} = 1500$ байт). В связи с этим для пакетов с длиной, превышающей $n_{макс} - \alpha + 1$, необходимо изменить алгоритм случайного увеличения длины, уменьшив значение параметра для таких случаев. Так что в случае получения пакета с длиной l, такой что $l > n_{макс} - \alpha + 1$, его длина увеличивается случайно на количество битов, определяемое значениями случайной величины, равновероятно принимающей целочисленные значения на множестве $N_{n_{макс}-l} \bigcup \{0\}$. В крайнем случае, когда $l = n_{макс}$, длина пакета вообще не может быть увеличена.

Дополнительная нагрузка на канал вычисляется с учетом вероятностей длин пакетов в исходном трафике $p(i)$. Выражение для вычисления дополнительной нагрузки на канал связи d:

$$d = \frac{\alpha - 1}{2} \sum_{i=1}^{n_{макс}-\alpha+1} p(i) + \sum_{i=n_{макс}-\alpha+2}^{n_{макс}} \frac{n_{макс} - i}{2} p(i). \quad (1)$$

Эффективная пропускная способность канала связи при введении данного метода противодействия равна

$$\beta' = \frac{\beta E(L)}{E(L)+d} = \frac{\beta E(L)}{E(L)+\frac{\alpha-1}{2}\sum_{i=1}^{n_{макс}-\alpha+1} p(i)+\sum_{i=n_{макс}-\alpha+2}^{n_{макс}} \frac{n_{макс}-i}{2} p(i)}, \quad (2)$$

где $E(L)$ — средняя длина передаваемых пакетов.

Из-за случайного изменения длин пакетов введение данного метода противодействия не приводит к рассинхронизации отправителя и получателя скрытого канала, однако становится возможной передача данных лишь по таким скрытым каналам, где символам скрытно передаваемого сообщения соответствуют построенные по определенным правилам множества длин пакетов. Далее исследована остаточная пропускная способность нескольких типов таких скрытых каналов.

Заметим, что при введении описанного метода противодействия мощность выходного алфавита увеличивается: если до введения противодействия в скрытом канале использовался алфавит $\{1,...,n\}$, то после случайного увеличения длин имеем алфавит $\{1,...,\min(n+\alpha-1, n_{макс}-l_{фикс}+1)\}$. Соответственно, для оценки остаточной пропускной способности скрытого канала необходимо привести в соответствие эти два алфавита. Для этого расширим алфавит скрытого канала до $\{1,...,\min(n+\alpha-1, n_{макс}-l_{фикс}+1)\}$ с условием, что символы $\{\min(n+1, n_{макс}-l_{фикс}+1),...,\min(n+\alpha-1, n_{макс}-l_{фикс}+1)\}$ отправляются с нулевой вероятностью.

При предложенном способе противодействия может быть целесообразно использовать видоизмененный набор входных символов для скрытого канала по памяти. Для передачи символа «i» отправитель посылает пакет длины $l_{фикс}+(i-1)b$, где $i \in N_{n_{факт}}$, b — параметр скрытого канала, принимающий целочисленные значения на отрезке $[1,\alpha]$. Величина $n_{факт}$ определяет фактическую мощность алфавита в скрытом канале, построенном на основе пакетов с длинами до $l_{фикс}+n-1$ с учетом величины шага b: $n_{факт}=\left\lfloor \frac{n-1}{b} \right\rfloor+1$. Таким образом, при $b=1$ имеем исходную схему построения скрытого канала, при которой средняя длина пакета минимальна. При $b=\alpha$ значении построенный скрытый канал является каналом без ошибок, поскольку длина пакета не может быть увеличена более чем на $\alpha-1$ бит.

Таким образом, входное распределение $L_{СК}$ в скрытом канале имеет следующий вид:

$$L_{СК}=\begin{pmatrix} l_{фикс} & l_{фикс}+1 & \cdots & l_{фикс}+b & \cdots & l_{фикс}+(n_{макс}-1)b & \cdots & l_{фикс}+n_{СК}-1 & \cdots & \min(l_{фикс}+n_{СК}+\alpha-2, n_{макс}) \\ p_{СК}(1) & 0 & 0 & p_{СК}(2) & \cdots & p_{СК}(n_{макс}) & \cdots & 0 & 0 & 0 \end{pmatrix}. \quad (3)$$

Численно будет оценен скрытый канал с равномерным распределением по памяти и по времени. В таком случае $L_{СК}$ выглядит так:

$$L_{СК}=\begin{pmatrix} l_{фикс} & l_{фикс}+1 & \cdots & l_{фикс}+b & \cdots & l_{фикс}+(n_{макс}-1)b & \cdots & l_{фикс}+n_{СК}-1 & \cdots & \min(l_{фикс}+n_{СК}+\alpha-2, n_{макс}) \\ \frac{1}{n_{макс}} & 0 & 0 & \frac{1}{n_{макс}} & \cdots & \frac{1}{n_{макс}} & \cdots & 0 & 0 & 0 \end{pmatrix}. \quad (4)$$

Сначала рассмотрим частный случай, при котором мы не учитываем ограничение на максимальную длину пакета, то есть теоретический случай. В таком случае каждый пришедший пакет может быть увеличен на $\alpha - 1$ бит, следовательно, нет необходимости учитывать особые условия противодействия для пакетов с длиной, близкой к максимальной.

В таком случае дополнительная нагрузка на канал связи заключается в отправке, в среднем, $(\alpha - 1)/2$ фиктивных бит на пакет. С другой стороны, эффективная пропускная способность канала связи при введении данного метода противодействия равна

$$\beta' = \frac{\beta E(L)}{E(L) + (\alpha - 1)/2}, \tag{5}$$

где $E(L)$ — средняя длина передаваемых пакетов.

При равномерном распределении по памяти и по времени пропускная способность принимает следующий вид:

$$\nu = \max_{n,b,m} \left\{ \frac{H(L_{вых}) - H(L_{вых} \mid L_{вх}) + \log_2 m - H(T_{вых} \mid T_{вх})}{\frac{E(L_{вых})}{\beta} + T\frac{m+1}{2}} \right\}. \tag{6}$$

На рисунке 1 приведена зависимость пропускной способности скрытого канала от параметра n и больших значений параметра b при значении $\alpha = 3000$. Более того, оценивается скрытый канал только по памяти, то есть $m = 1$ и $T = \tau$.

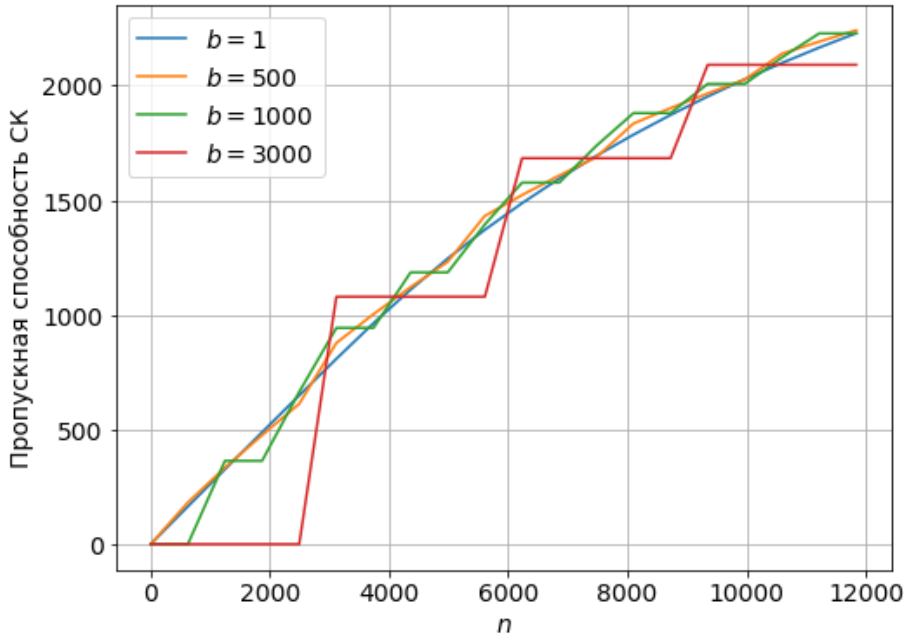


Рисунок 1 — Зависимость пропускной способности скрытого канала от параметра n и больших значений параметра b при значении $\alpha = 3000$

С ростом параметра α увеличивается и величина параметра n. Еще заметим, что при $b = \alpha$ выходное распределение получается практически равномерным (только для части последних символов вероятность их получения равна нулю). Количество таких символов

равно $(n-1)\bmod b$ - это связано с тем, что наибольший символ в скрытом канале, отправляемый с ненулевой вероятностью $p_{СК}$ равен $n-(n-1)\bmod b$.

При больших значениях параметра n отличие $n_{реал}$ от n перестает вносить ощутимый вклад в величину энтропии. Это объясняется тем, что величина $(n-1)\bmod b$ становится значительно меньше n (разумеется, что это при разумном и не очень большом значении α, а следовательно и b).

Раз мы выяснили, что $n_{реал} \approx n$ при больших n, то подумаем, какие значения b наиболее выгодно брать? Явно нужно постараться взять b кратное α. Если берем $b=\alpha$, то получаем канал без ошибок. Если берем $b=\left\lceil \frac{\alpha}{2} \right\rceil$, то может быть только два варианта символа «i», в который может быть преобразован изначально отправленный символ «j». И так далее.

После того, как был подробно рассмотрен частный случай, при котором при введении противодействия не делалась поправка на максимальную длину пакета, перейдем к общему случаю.

Чтобы найти значение величины $H\left(L_{вых} \mid L_{СК}\right)$, необходимо определить условные вероятности декодировать символ «i» при условии отправки символа «j». Вероятности символов в выходном распределении $p_{вых}(i)$, энтропия $H(L_{вых})$ и пропускная способность ν находятся аналогично рассмотренному ранее частному случаю. При расчетах берем $T=\tau$

На графике приведена зависимость пропускной способности скрытого канала от параметров n и b при значении $\alpha=3000$ (рисунок 2). Более того, оценивается скрытый канал только по памяти.

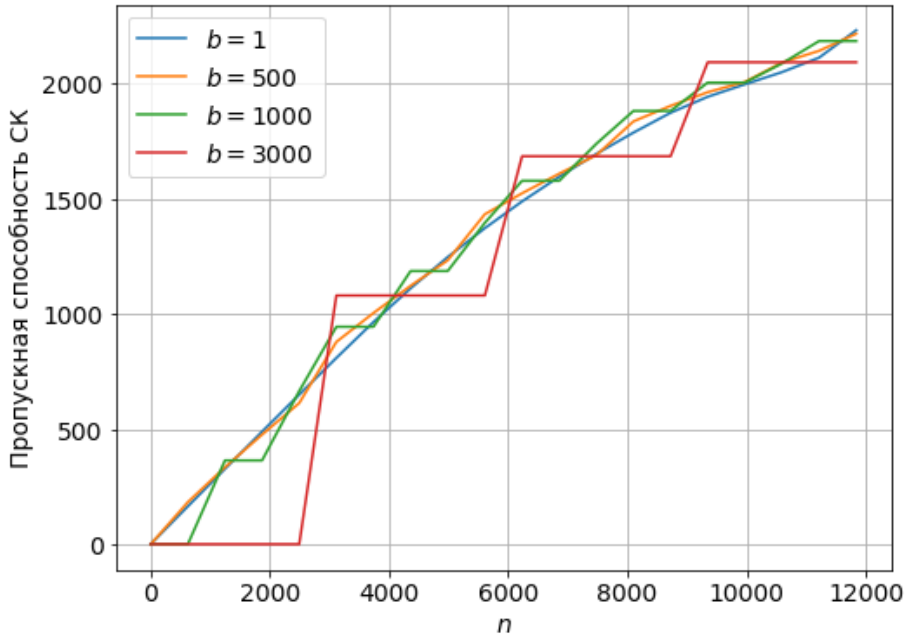


Рисунок 2 — Зависимость пропускной способности скрытого канала от параметров n и b при значении $\alpha=3000$

Заметим, что как для больших ($\alpha=3000$) значений параметра α оптимально выбирать максимально допустимую величину параметра n.

Отдельно рассмотрим разницу, которая появляется при переходе от рассмотренного ранее частного случая к общему случаю, учитывающему ограничение на максимально возможную длину пакета. На рисунке 3 приведена зависимость остаточной пропускной способности скрытого канала от параметра n при $b=1$ и $\alpha=1000$ для двух разных схем (без ограничения на длину минус 1; с ограничением на длину минус 2).

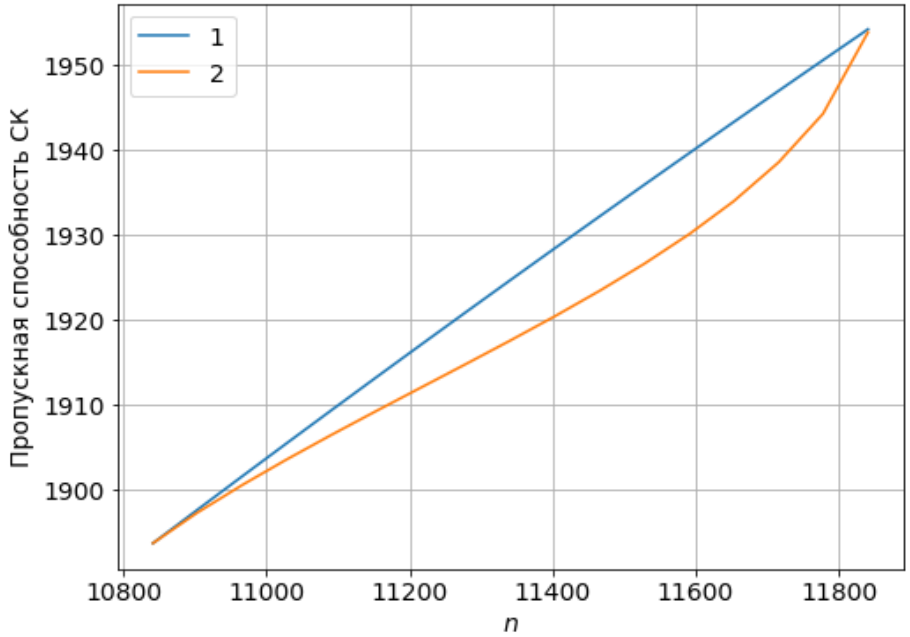


Рисунок 3 — Зависимость остаточной пропускной способности скрытого канала от параметра n при $b=1$ и $\alpha=1000$

Можно заметить, что при оптимальном $n=n_{макс}-l_{фикс}+1$ оба метода дают одинаковые результаты, поэтому выгоднее брать общий метод, так как при нем получается чуть выше эффективная пропускная способность канала связи.

Также видно, что простой способ оценить остаточную пропускную способность скрытого канала при введении противодействия – это оценить пропускную способность скрытого канала без ошибок для случая $b=\alpha$ без учета какого-либо противодействия (просто взять логарифм фактического значения $n_{факт}=\left\lfloor \frac{n-1}{b} \right\rfloor+1$, и т. д.).

Случай блочного шифрования трафика аналогичен рассмотренному ранее поточному шифрованию. Необходимо внести только несколько изменений. Если раньше мы отправляли символы в скрытом канале с шагом b, начиная с $l_{фикс}$, то сейчас минимально возможная длина пакета равна $\left\lceil \frac{l_{фикс}}{l_ш} \right\rceil l_ш$. И пакеты в скрытый канал мы можем брать только с шагом b, кратным размеру блока $l_ш$. То есть $b=kl_ш$, где k - натуральное. Также логично брать величину α тоже кратной $l_ш$, то есть $\alpha=rl_ш$, где r - натуральное.

Поскольку на выходе могут быть только пакеты с длинами, кратными длине блока $l_ш$, необходимо немного изменить выражение для вычисления условной вероятности $P_{вых\_блочн}\left(i\middle|j\right)$ для блочного шифрования трафика. Можно просто считать, что $P_{вых\_блочн}\left(i\middle|j\right)$

агрегирует все вероятности $P_{вых}\left(i\middle|j\right)$ (взятые из случая для поточного шифрования) только в символах, кратных $l_ш$:

$$P_{вых\_блочн}\left(i\middle|j\right)=\begin{cases}\sum\limits_{k=i-l_ш+1}^{i} P_{вых}\left(k\middle|j\right), \ i \ кратно \ l_ш \\ 0, \ иначе\end{cases}. \quad (3)$$

Заметим, что такое изменение в вычислении условной вероятности $P_{вых\_блочн}\left(i\middle|j\right)$ не вносит значительных изменений в значение условной энтропии, как ранее не вносили больших изменений разные значения параметра b.

В целом, результаты не должны отличаться от тех, которые были получены при поточном шифровании трафика, так как мы показали, что величина параметра b практически не влияет на остаточную пропускную способность скрытого канала. А непосредственное влияние на пропускную способность оказывает как раз параметр α. Поэтому приходим к выводу, что и для разных параметров $l_ш$ при фиксированном α пропускная способность скрытого канала будет практически неизменной.

СПИСОК ЛИТЕРАТУРЫ

1. Popescu, A. On Kleinrock's Independence Assumption / Network Performance Engineering. Lecture Notes in Computer Science. — 2011.
2. Архангельская, А.В. Характеристики области эффективного применения методов поточного шифрования для защиты трафика в телекоммуникационных системах / Информационное противодействие угрозам терроризма. — 2005.
3. Hernandez, A. One-way delay measurement and characterization / Proceedings of the International Conference on Networking and Services. — 2007.
4. Sagatov, E.S. Composite distribution for one-way packet delay in the global network / Proceedings of the 24th Telecommunications Forum. — 2016.
5. Sukhov, A. Generating function for network delay / Journal of High Speed Networks. — 2016.
6. Грушо, А.А. Статистические скрытые каналы / Материалы XVII Общероссийской научной конференции «Методы и технические средства обеспечения безопасности информации». — 2008.
7. Cabuk, S. IP covert timing channels: design and detection / Proceedings of the eleventh ACM conference on computer and communications security. — 2004.
8. Shah, G. Keyboards and Covert Channels / Proceedings of The15th USENIX Security Symposium. — 2009.
9. Sellke, S.H. Covert TCP/IP timing channels: theory to implementation / Proceedings of the twenty-eighth conference on computer communications. — 2009.
10. Armitage, G.J. Stealthier inter-packet timing covert channels / G/ Proceedings of 10th International IFIP TC 6 Networking Conference. — 2011.

Частикова В.А.
ФГБОУ ВО «Кубанский государственный технологический университет», доцент кафедры кибербезопасности и защиты информации, канд. техн. наук, доцент,
chastikova_va@mail.ru

МЕТОДОЛОГИЯ ПОСТРОЕНИЯ СИСТЕМ АНАЛИЗА ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ РАСПРЕДЕЛЁННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

Аннотация: в статье изложено построение методологии интеллектуального анализа событий безопасности, предназначенной для мониторинга распределённых информационных систем и содержащей совокупность подходов, использующих различные методы машинного обучения, а именно: методы глубокого обучения, искусственные иммунные систем, алгоритмы роевого интеллекта, генетические алгоритмы, экспертные системы. Основу методологии составляет принцип гибридизации данных интеллектуальных методов в контексте подмодулей системы анализа событий для решения специализированных задач. В исследовании представлены анализ современного состояния исследований в области, новизна предлагаемой методологии и ожидаемые научные результаты реализации проекта.

Ключевые слова: система обнаружения вторжений, сетевая атака, модифицированный генетический алгоритм дуэлей, глубокое обучение, искусственная иммунная система, нейроиммунный подход.

Ключевой целью исследования является разработка методологии анализа событий информационной безопасности в распределенных системах. Значимость и актуальность связана с острой необходимостью обеспечения сетевой безопасности информационных систем средних и крупных организаций, хранящих и обрабатывающих существенный объем конфиденциальных сведений, требующий регулярного контроля и защиты. Для мониторинга безопасности специалисты применяют различные продукты, предоставляющие инструменты контроля за состоянием среды по ключевым показателям, логам инцидентов, сетевому трафику. Но для таких систем остаётся актуальным вопрос эффективности механизмов, обеспечивающих автоматический анализ событий. Она определяется адаптивностью алгоритмов под новые схемы атак, цепочек инцидентов для своевременного и системного выявления действий злоумышленников с минимальной нагрузкой на операторов системы безопасности. Данные инструментальные комплексы требуют регулярной поддержки баз сигнатур, настройки, используют классические подходы, основанные на методах сигнатурного анализа, статистической вероятности, экспертных систем, которые характеризуются малой гибкостью, адаптивностью, в отличие от методов машинного обучения. Предложенная методология предполагает построение комплексной системы анализа инцидентов безопасности (САИБ), выполняющей множество разнородных функций. Для неё требуется определение перечня ключевых модулей, решаемых ими задач и подходов их реализации.

В качестве основных задач исследования необходимо провести анализ интеллектуальных подходов построения систем обнаружения и анализа инцидентов, разработать методики построения систем обнаружения вторжений, анализа инцидентов биометрической идентификации и аутентификации в распределенных средах, анализа и

корреляции событий безопасности, модуля агрегации и визуализации данных, а также модуля сжатия данных. Разработка комплекса программных продуктов, реализующих предложенные методики для распределенных систем различных объектов экономической инфраструктуры.

Наиболее распространёнными методами анализа событий являются классические экспертные системы, сигнатурные методы, методы статистического анализа, зарекомендовавшие себя благодаря стабильности, эффективности при определении известных инцидентов [1]. Системы, основанные на подходах машинного обучения, несмотря на высокую гибкость и эффективность в прикладных задачах [2, 3], ещё не получили широкого распространения в современных комплексах мониторинга безопасности, т.к. менее исследованы и отработаны. Но в связи с высокими перспективами систем, адаптивных к малознакомым схемам инцидентов, многие корпорации заинтересованы развиваться в направлении внедрения нейронных сетей и иных интеллектуальных методов [4]. Это связано и с сложностью формирования специалистами для классических систем баз сигнатур, требующих регулярного обновления.

Помимо названных недостатков, в данный момент всё большее распространение получают системы биометрической аутентификации, которые характеризуются рядом особенностей, в силу чего инциденты, связанные с их эксплуатацией могут быть нетипичными для классических методов идентификации личности [5] и требуют отдельного подхода к анализу.

Таким образом, методы машинного обучения являются перспективным направлением развития современных САИБ, т.к. их комплексное применение с классическими подходами способно обеспечить одновременно и устойчивость, и адаптивность идентификации угроз.

Главной задачей САИБ является анализ и корреляция событий ИБ, для чего проводится агрегация, нормализация, фильтрация, классификация, корреляция и приоритезация событий.

Результаты формируются в виде настраиваемых графических отчетов и предупреждений, облегчающих мониторинг инфраструктуры распределённой системы путём выявления отклонений ключевых показателей по выбранным критериям [6, 7].

В основу модулей системы САИБ вошли наиболее перспективные, активно развивающиеся и демонстрирующие эффективность интеллектуальные методы машинного обучения различных классов: нейросетевые методы глубокого обучения, искусственные иммунные системы, генетические алгоритмы эволюционной имитации, метаэвристические алгоритмы роевого интеллекта, а также классические экспертные системы [8].

Современные архитектуры нейронных сетей характеризуются высокой гибкостью, адаптивностью, поэтому они повсеместно применяются для решения различных видов прикладных задач, в том числе и для распознавания образов атак в информационных системах [9, 10]. В качестве глубоких нейронных сетей в разработанной САИБ применяются архитектуры свёрточных сетей. В свою очередь, иммунные системы также являются перспективным направлением в рамках решения задачи обнаружения вторжений в виду основных принципов иммунологии [11, 12]. В качестве ИИС используется гибридная искусственная иммунная система (ГИИС), представляющая слияние классического клонального типа ИИС и модифицированного генетического метода дуэлей (МГАД), также применяемого для настройки гиперпараметров систем САИБ.

Подход гибридизации архитектур данных методов для построения модулей САИБ был именован нейроиммунным подходом, являющимся основой исследования, обеспечившей повышение эффективности целевой системы анализа инцидентов [8].

Для описания методики обнаружения, анализа и корреляции инцидентов информационной безопасности, в том числе обусловленных применением систем биометрической аутентификации, в комплексной системе анализа распределённых инцидентов предлагается использовать следующие основные функциональные модули САИБ: сенсорный модуль и сеть сбора данных с узлов; модуль генерации и обучения детекторов; модуль сжатия и хранения данных; модуль анализа и корреляции; административный модуль управления [13].

Соответственно, в системе анализа инцидентов ИБ можно выделить несколько основных подсистем, модулей, обеспечивающих её функциональность и изображённых на рисунке 1.

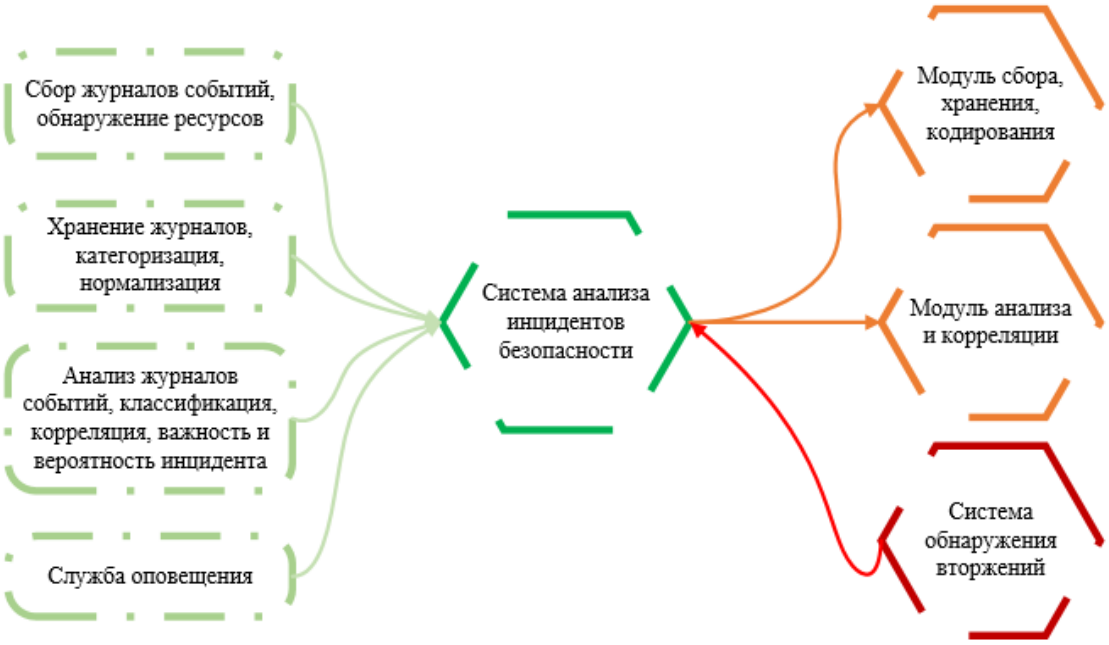


Рисунок 1 – Компоненты и функции САИБ

Предлагаемая методика анализа инцидентов ИБ и обнаружения сетевых атак САИБ объединяет такие интеллектуальные подходы, как: методы глубокого обучения в виде искусственных нейронных сетей, демонстрирующих высокие показатели эффективности в задачах кибербезопасности [13, 5]; системы, основанные на правилах [14]; искусственные иммунные системы (ИИС), также обладающие высоким потенциалом, гибкостью и адаптивностью в соответствии с рядом исследований [1, 15]; метаэвристические алгоритмы, являющиеся современным неотъемлемым инструментом при решении задач оптимизации [3, 4].

В качестве глубоких нейронных сетей применяются архитектуры свёрточных сетей [14]. В качестве ИИС используется гибридная искусственная иммунная система (ГИИС), объединяющая классический клональный вариант ИИС [6] и модифицированный генетический метод дуэлей (МГАД). Основные положения ГИИС и МГАД были описаны в рамках предыдущих исследований [7, 8].

Объединение данных интеллектуальных методов позволило обеспечить эффективность целевой системы анализа инцидентов.

Общий алгоритм работы нейроиммунной системы анализа инцидентов ИБ распределённых систем следующий: для обучения нейроиммунных модулей формируется репрезентативная выборка инцидентов ИБ, которые предоставляются системе защиты для

формирования базы антител-распознавателей угроз по выделенным признакам. Далее обученная нейроиммунная система вводится в узлах в режиме распознавания и при обнаружении инцидентов в анализируемой среде формирует уведомление об обнаруженной проблеме, лог события.

Для построения нейроиммунной системы применяются свёрточная нейронная сеть как метод глубокого обучения и гибридная искусственная иммунная система, объединяющая свойства генетического алгоритма, иммунной системы типа клональной селекции и модифицированного генетического алгоритма.

Ключевой особенностью разрабатываемой системы является применение гибридных интеллектуальных методов, подходов для решения задачи анализа и корреляции, а также внедрения в САИБ интеллектуального модуля системы обнаружения вторжений (СОВ).

Общий принцип работы систем анализа инцидентов ИБ, обнаружения вторжений на базе нейроиммунной системы представляется следующим образом: для обучения нейроиммунной системы формируется репрезентативная выборка известных инцидентов ИБ, образов сетевых атак, которые предоставляется системе защиты для формирования базы антител-распознавателей опасных объектов, исчерпывающе описывающих каждый из заданных типов атак в случае СОВ или корреляционные связи между событиями, составляющими инциденты, в случае САИБ. После чего обученная нейроиммунная система вводится в узлах в режиме распознавания. Соответственно, при возникновении угрозы, идентификации опасного поведения в анализируемой сети формируется уведомление об обнаруженной проблеме, поступающее администратору.

В рамках данной работы обучение и тестирование нейроиммунной системы проводится на наборе данных «Intrusion Detection Evaluation Dataset» CIC-IDS2017 (Канадский институт кибербезопасности). Выбранный набор является одним из наиболее актуальных и изученных, т.к. существует ряд исследований, описывающих недостатки датасета и предлагающих решения по их устранению, балансировке, сокращению карты признаков путём поиска корреляций, избыточности в записях. При этом датасет обладает достаточно большой выборкой, вариативностью представленных классов атак.

Новизна исследования заключается в предлагаемой методологии анализа инцидентов безопасности распределённых систем на основе разработанного нейроиммунного подхода, реализованного и исследованного с использованием гибридизации структур интеллектуальных методов машинного обучения. В работе предпринята попытка использовать преимущества каждого из подходов для решения своей специализированной подзадачи. Предложенное решение способно обеспечить повышение надёжности, гибкости, комплексной эффективности современных систем анализа событий.

Архитектура применяемой в нейроиммунном подходе свёрточной сети представлена далее (Рисунок 2) и включает входной слой приёма образа атаки, две пары слоёв свёртки и субдискретизации с последующим выходом на полносвязную сеть – персептрон, содержащий пару скрытых слоёв. Для компенсации потери значимости признаков, соответствующих угловым зонам карты образа, к исходной карте и после первого слоя субдискретизации применяется техника same padding, заключающаяся в дополнении по периметру обрабатываемых карт нулевых пикселей. В свою очередь, пулинговые слои реализуют подход max pooling, в соответствии с которым субдискретизация заключается в выборе наибольшего элемента в пределах позиции смещающегося окна (ядра или фильтра), где на первом этапе пулинга при размере ядра 2x2 параметр stride, описывающий шаг смещения ядра, равен 2, что

сокращает размер карты в 2 раза. На втором этапе пулинга смещение stride равняется 1. В качестве активационной применяется функции ReLu, алгоритмом обучения сети является гибридная искусственная иммунная система.

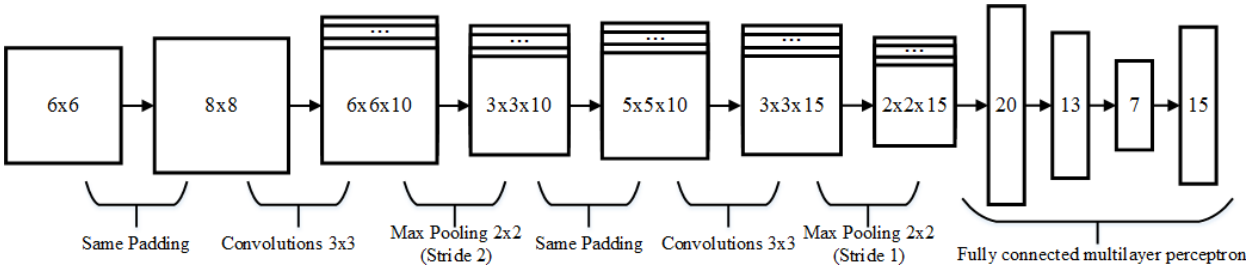


Рисунок 2 – Архитектура свёрточной нейронной сети нейроиммунной системы обнаружения сетевых атак

На рисунках ниже (Рисунок 3, Рисунок 4) представлены алгоритмы обучения и функционирования системы обнаружения сетевых атак на основе нейроиммунного подхода, образованного сочетанием архитектур гибридной искусственной иммунной системы и свёрточной нейронной сети.

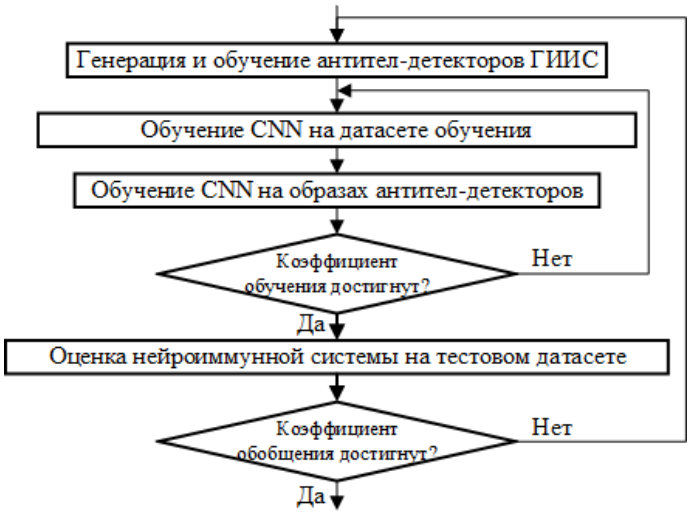


Рисунок 3 – Алгоритм обучения системы обнаружения сетевых атак на основе нейроиммунного подхода

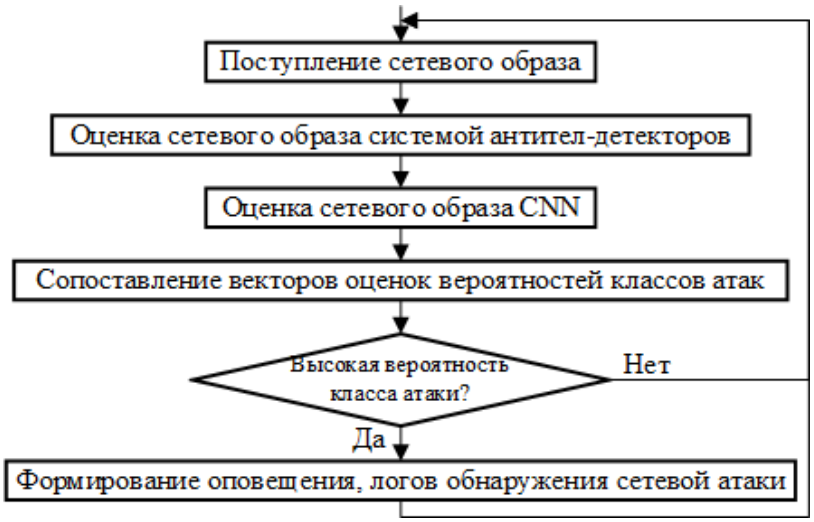


Рисунок 4 – Алгоритм функционирования системы обнаружения сетевых атак на основе нейроиммунного подхода

В рамках исследования подхода анализа уникальных событий биометрической идентификации и аутентификации личности получены 3 патента на изобретения: «Способ опознавания личности по радужной оболочке глаза» (RU 2672279 C1), «Способ опознавания личности по рисунку вен ладони» (RU 2761776 C1) и «Способ опознавания личности по рисунку вен ладони» (RU 2761776 C1) .

Научными результатами являются: формирование методов построения надёжных и точных систем анализа событий информационной безопасности, повышение защищенности распределенных систем от различных видов угроз, включая сетевые атаки, вредоносное программное обеспечение, взлом учетных записей, атаки на системы аутентификации, в том числе биометрические.

Полученные теоретические и практические результаты использованы в лекционном, лабораторном и практическом курсах дисциплины «Технологии искусственного интеллекта в области безопасности и защиты информации» для студентов специальностей 10.05.01 Компьютерная безопасность, 10.05.03 Информационная безопасность автоматизированных систем и магистров направления подготовки 10.04.01 Информационная безопасность кафедры кибербезопасности и защиты информации КубГТУ.

СПИСОК ЛИТЕРАТУРЫ

1. Andress, J. The basics of information security: understanding the fundamentals of InfoSec in theory and practice / J. Andress // Syngress. — 2014. — 190.
2. Kahraman, K. Anomaly Detection in Networks Using Machine Learning / K. Kahraman // School of Computer Science and Electronic Engineering University of Essex. — 2018. — 71.
3. Alfredo, C. An Analysis of Deep Neural Network Models for Practical Applications / C. Alfredo, P. Adam, C. Eugenio // ArXiv:1605.07678v4. — 2017. — 1-6.
4. Poltavtseva, M.A. Modeling big data management systems in information security / M.A. Poltavtseva, M.O. Kalinina //Automatic Control and Computer Sciences. — 2019. — №53(8). — 895-902.
5. Gernot, T. Biometric Masterkeys / T. Gernot, P. Lacharme // Comput. Secur. — 2022. — №116. — 102642.
6. Berdibayev, R. A concept of the architecture and creation for SIEM system in critical infrastructure / R. Berdibayev, S. Gnatyuk, Y. Yevchenko, V. Kishchenko // Systems, Decision and Control in Energy II. — 2021. — 221-242.
7. Сухов, В.Е. Система обнаружения аномалий сетевого трафика на основе искусственных иммунных систем и нейросетевых детекторов / В.Е. Сухов // Вестник рязанского государственного радиотехнического университета. — 2015. — №54(1). — 84-90.
8. Частикова, В.А. Методика построения системы анализа инцидентов информационной безопасности на основе нейроиммунного подхода / В.А. Частикова, А.И. Митюгов // Электронный сетевой политематический журнал "Научные труды КубГТУ". — 2022. — №1. — 98-105.
9. Alfredo, C. An Analysis of Deep Neural Network Models for Practical Applications / C. Alfredo, P. Adam, C. Eugenio // ArXiv:1605.07678v4. — 2017. — 1-6.
10. Матвеев, М.Г. Модели и методы искусственного интеллекта. Применение в экономике / М.Г. Матвеев, А.С. Свиридов // Издательский дом «ИНФРА-М». — 2014. — 316-324.

11. Васильев, В.И. Распределенная система обнаружения атак на основе механизмов иммунной системы / В.И. Васильев, Р.Р. Шамсутдинов // Информационные технологии интеллектуальной поддержки принятия решений (ITIDS 2018), Труды VI Всероссийской конференции (с приглашением зарубежных ученых). — 2018. — 237-244.
12. Gallais-Jimenez, M., Nguyen, H.A., Saied, M.A., Nguyen, T.N., & Sahraoui, H.A. (2020). API Misuse Detection An Immune System inspired Approach / M. Gallais-Jimenez, H.A. Nguyen, M.A. Saied, T.N. Nguyen, H.A. Sahraoui // ArXiv:abs/2012.14078. — 2012. — 2-4.
13. Miller, D. Security information and event management (SIEM) implementation / D. Miller // New York: McGraw-Hill. — 2011.
14. Atymtayeva L., Kozhakhmet K., Bortsova G. Building a knowledge base for expert system in information security. Conference: Soft Computing in Artificial Intelligence book, Advances in Intelligent Systems and Computing series, 2014, vol. 270, p. 20.

Штеренберг С.И.
Ордена Трудового Красного Знамени федеральное государственное бюджетное образовательное учреждение высшего образования «Московский технический университет связи и информатики», доцент, к.т.н.,
stas.shterenberg.89@mail.ru

СИСТЕМЫ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ДЛЯ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ В РАСПРЕДЕЛЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

Аннотация: Разработка технологии защищенной интеллектуальной системы обнаружения вторжений (далее – СОВ) на основе квазибиологической парадигмы является ключевым направлением деятельности в рамках работы с проектом гранта, а именно системами искусственного интеллекта (далее – ИИ) для обнаружения вторжений в распределенных информационных системах (далее - РИС). Актуальность выбранного направления исследований и разработок обусловлена тем, что имеются тенденции и процессы синхронизации знаний о автоматизированных, роботизированных и интеллектуальных системах. В ходе исследования выделяются критерии/проблемы значимости, а именно: глобальные (сохранение веток развития Индустрии 4.0 [1, 2], повсеместное внедрение интернета вещей (IoT) [3], развитие кибернетики и кибербезопасности), частные (структурность машинного и глубокого обучения, мультиагентный подход и метод роя частиц (далее - МРЧ), развитие SIEM & IDS), ключевые (комплексная защита РИС от атак, направленных на нарушение целостности программного обеспечения (далее - ПО), защита пакентно-нейросетевых программ (далее - ПНП) при помощи других нейронных сетей (далее – НС)), перспективные (технологии Больших данных, развитие иммунных систем, генетические алгоритмы). На основе выбранных векторов исследований, автор выделяет следующие противоречия в науке которые будут озвучены в данном докладе, подчеркнутые актуальностью: квазибиологическая парадигма – как ключевой подход к формированию интеллектуальных СОВ, технологическая сингулярность – стремление для развития систем защиты информации (далее - СЗИ) на основе иммунных систем.

Ключевые слова: Большие данные, нейронные сети, SIEM, системы обнаружения вторжений, искусственный интеллект, квазибиологическая парадигма, машинное обучение, глубокое обучение, программный агент.

Постановка задачи, степень разработанности темы

Как и во всей теме проекта, так и в данном докладе будет подробно рассмотрена возможность установления неизвестных ранее объективно существующих закономерностей квазибиологических свойств и явлений для материальных СЗИ с целью повышения устойчивости архитектуры отдельно взятого ПО. Соответственно интеллектуальная СОВ и свойств ПНП входящих в ее состав будут являются ключевым объектом исследования, а показатели устойчивости архитектуры интеллектуальной СОВ в условиях атак, направленных на нарушения целостности – предметом исследований.

Необходимо достичь следующей цели, а именно, уменьшения количества ложных срабатываний для повышения надежности интеллектуальных СОВ за счет переобучения ПНП, в том числе с использованием принципов автоматической пересборки и саморепликации. Такая цель будет достигаться возможностями:

1. провести теоретические мультидисциплинарные исследования существующих методов обнаружения угроз безопасности и защиты от них, обосновать и выбрать направления исследований на основе анализа информационных источников и результатов патентных исследований;

2. произвести моделирование устойчивой к компьютерным атакам ассимиляционную память в среде обработки Больших данных РИС с использованием ИИ;

3. построить самоорганизующуюся карту НС, действующую в составе интеллектуальной СОВ для мониторинга всех компонентов ПНП;

4. обеспечить работоспособность децентрализованных рассинхронизированных ПНП в РИС, ранее сопряженных в едином ПО;

5. разработать архитектуру интеллектуальной СОВ на основе квазибиологической парадигмы для управления всем комплексом ПНП в составе РИС;

6. определить эффективность разработанной архитектуры интеллектуальной СОВ и основных научных результатов.

Моделирование защиты ассимиляционной памяти в среде обработки Больших данных РИС с использованием ИИ

Известно, что технологию Больших данных может быть использованы для многих целей, включая системы защиты информации. Ассоциативная память в интеллектуальной системе обнаружения вторжений служит важным инструментом для быстрого и эффективного СОВ. Для улучшения результативности предсказательного моделирования ассимиляционной памяти стоит сделать ставку на несбалансированные данные [4]. В особенности квазибиологической парадигмы, стоит привести следующие понятия:

1. Понижающий отбор. Если у вас достаточно данных, как в случае с данными о ссудах, одно из решений состоит в понижающем отборе (недоотборе) преобладающего класса, чтобы моделируемые данные были сбалансированнее между нулями и единицами.

2. Повышающий отбор и повышающая/понижающая перевесовка. Одно из критических замечаний по поводу метода понижающего отбора состоит в том, что он (способ) отбрасывает данные и не использует всю имеющуюся под рукой информацию.

3. Генерация данных. Вариацией повышающего отбора посредством бутстрапирования является генерация данных путем перестановки существующих записей для создания новых записей.

4. Предвзятые данные [5, стр. 396]. По иным направлениям также существует возможность, что ваши алгоритмы могут кодировать фактические предвзятости (смещения), которые существуют в мире.

Известные примеры РИС [6] могут обрабатывать Большие данные благодаря моделированию без потерь, т.к. имеется процесс информационно-управляющей системы (далее – ИУС) [7]. Однако, модель еще не может являться до конца приспособленной к работе в крупный РИС с Большими данными. В ассоциативной памяти устанавливается необходимый базис для работы. В таком виде система может выполнять все стандартные функции по обработке событий безопасности (рис. 1): - Сбор; - Нормализация; - Агрегация; - Обогащение; - Хранение; - Уведомление. Приведем пример нескольких возможных базовых настроек правил для обработки событий безопасности:

1) Простой фильтр – каждому событию безопасности присваивается приоритет, таким образом могут появляться события, которые требуют быстрого реагирования. Такие события могут не нуждаться в агрегации или фильтрации (рис. 2);

2) Агрегация (по временному отрезку или количеству прошедших событий) – накопление однотипных событий безопасности, а при превышении их количества отправка уведомления об инциденте (рис. 3);
3) Шаблоны (по временному отрезку или количеству прошедших событий) – заданный набор, следующих друг за другом событий на определенном промежутке времени или за некоторое количество событий (рис. 4).

Правила и фильтры для выявления инцидентов могут конфигурироваться напрямую, для этого составляются непосредственно сами правила для конвейеров обработки данных.

Рис. 1. Стандартный поток по обработке данных SIEM-системой

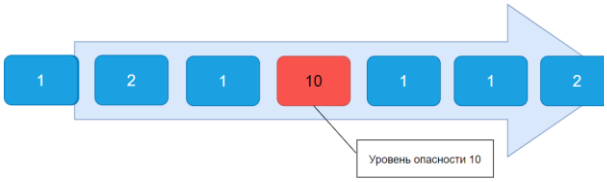


Рис. 2. Обнаружение события с высоким уровнем опасности в потоке (простой фильтр)

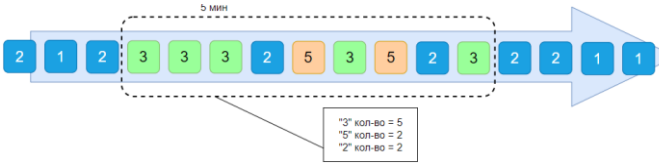


Рис. 3. Обнаружение набора событий с одинаковыми приоритетами (агрегация)

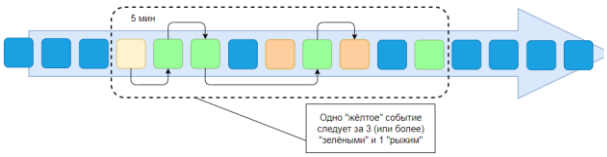


Рис. 4. Обнаружение определенной последовательности событий (шаблон)

Разработка методики построения самоорганизующейся карты НС, действующей в составе интеллектуальной СОВ, для мониторинга поведения искусственного интеллекта

Автоматический сборщик мониторинга и аудита для интеллектуальной системы обнаружения вторжений может состоять из следующих компонентов:

1. Агенты мониторинга - небольшие программы, установленные на каждом устройстве в сети, которые собирают информацию о событиях в режиме реального времени и отправляют ее на центральный сервер.

2. Центральный сервер - программа, которая принимает данные от всех агентов мониторинга, агрегирует и обрабатывает их, и сохраняет в базу данных.

3. Система анализа данных - набор алгоритмов и правил, которые используются для обнаружения аномальных событий и потенциальных угроз безопасности.

4. Интерфейс пользователя - приложение, доступное для управления системой. Он позволяет пользователям просматривать данные о событиях, создавать и настраивать правила анализа, и управлять параметрами системы.

5. Модуль генерации отчетов - система, которая создает автоматические отчеты, основанные на данных, собранных системой мониторинга и анализа.

6. Модуль управления угрозами - система, которая предлагает рекомендации по управлению угрозами, выявленными системой анализа данных.

7. Система уведомлений - модуль, который уведомляет администраторов системы о появлении новых событий и угроз безопасности.

Помимо этого, важно предусмотреть регулярное обновление системы безопасности, а также обучение пользователей работе в сети и рекомендации по безопасности.

Детализированная настройка правил корреляции позволяет сократить количество ложных срабатываний, что снижает нагрузку на СОВ, связанную с рассмотрением событий, ошибочно признанных инцидентами (Рис. 6). При разработке научно обоснованного решения всегда возникает потребность в оценке его эффективности и применимости в реальных условиях. Из-за ограниченной распространенности данной темы, некоторые методы оценки эффективности не могут быть применены [8].

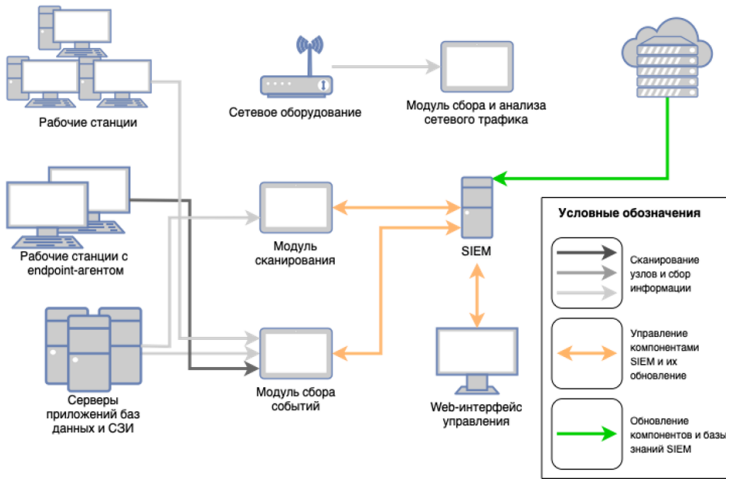


Рис. 5. Общая схема работы СОВ схожая с SIEM

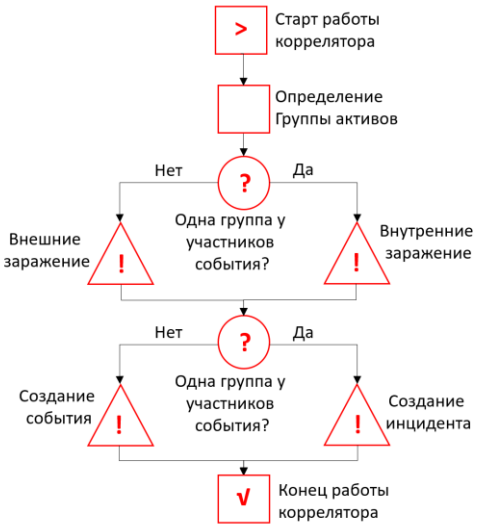


Рис. 6. Алгоритм правил корреляции, определяющего тип заражения вредоносным ПО

Для оценки эффективности разработанной методики необходимо сравнить эффективность проведения мониторинга при ее использовании и без, т.е. сравнить процесс проведение мониторинга с использованием SIEM и полностью ручной. В этом сравнении следует учесть ключевые факторы, оказывающие существенное влияние на качество и эффективность мониторинга.

Обеспечение работоспособности децентрализованных рассинхронизированных ПНП в РИС

Для обеспечения работоспособности децентрализованных, рассинхронных, пакетно-нейросетивых программ необходимо учитывать следующие факторы:

1. Синхронизация пакетов: пакеты должны быть синхронизированы между всеми участниками сети с помощью специальных протоколов.

2. Надежность: пакеты должны передаваться надежно, чтобы избежать потери данных. Для этого можно использовать механизмы повторной передачи и контроля ошибок.

3. Безопасность: пакеты должны быть защищены от несанкционированного доступа. Для этого используются криптографические алгоритмы и механизмы аутентификации.

4. Масштабируемость: сеть должна быть способна обрабатывать большое количество пакетов без снижения производительности.

5. Гибкость: сеть должна иметь возможность адаптироваться к изменяющимся условиям работы.

6. Эффективность: сеть должна работать быстро и эффективно, чтобы обеспечить высокую производительность.

7. Поддержка различных протоколов: сеть должна поддерживать различные протоколы передачи данных, чтобы обеспечить совместимость с различными устройствами и приложениями.

Табл. 1. Значения частных показателей для расчета значений эффективности

Факторы, влияющие на эффективность		Степень значимости коэффициента	Частный показатель стандартных способов проведения мониторинга	Частный показатель разработанной методики
1	Временные затраты на сбор исходных данных для проверки выполнения требований	0,5	0,1	1
2	Временные затраты на обработку собранной информации	0,2	0,5	1
3	Временные затраты на актуализацию информации	0,1	0,9	1
4	Временные затраты на анализ полученных результатов	0,1	0,5	1
5	Временные затраты на принятие решения о соответствии	0,1	0,3	1
Итоговый коэффициент эффективности			**0,32**	**1**

СОВ может иметь два режима работы: централизованный и децентрализованный. В централизованном режиме все управление и мониторинг системы осуществляется из единого центра, что повышает контроль и обеспечивает централизованный механизм принятия решений. В децентрализованном режиме каждый компонент системы имеет свою автономность и может автономно обрабатывать и защищать информацию, без единой точки управления [8].

Архитектура интеллектуальной СОВ на основе квазибиологической парадигмы

Архитектура интеллектуальной системы обнаружения вторжений может быть построена на основе квазибиологической парадигмы. Ниже представлена общая архитектура такой системы:

1. Сбор данных: система собирает данные о сетевой активности, включая информацию о трафике, сетевых пакетах и других событиях. Данные могут быть получены из различных источников, например, сетевых устройств, систем мониторинга и т.д.

2. Преобразование данных: данные преобразуются в формат, удобный для обработки системой. Например, данные могут быть преобразованы в бинарный формат или в формат JSON.

3. Анализ данных: полученные данные анализируются для обнаружения аномалий и вторжений. Для этого используются различные методы и алгоритмы, такие как статистический анализ, машинное обучение, кластеризация и т.д.

4. Классификация: на основе анализа данных система определяет, является ли обнаруженная аномалия или вторжение легальным или нет. Если аномалия является легальной, то система не предпринимает никаких действий. Если же аномалия или вторжение являются незаконными, то система оповещает администратора и принимает меры для предотвращения дальнейших вторжений.

5. Уведомление: если система обнаруживает вторжение, она отправляет уведомление администратору или другим заинтересованным лицам. Уведомление может содержать информацию о времени, месте и типе вторжения.

6. Реагирование: на основе полученной информации система принимает меры для противодействия вторжению. Это может включать в себя блокировку доступа к ресурсам, отправку уведомления об инциденте в правоохранительные органы и т.д.

В целом архитектура системы, дополняется компонентами обработки данных, полученных от СОВ, компонентом сбора информации, компонентом моделирования атак, и генерацией входных данных [6]. Компонент оценки защищенности включает набор функций, реализующих вычисления показателей защищенности уровня, соответствующего получаемым моделям [10]. В агент добавлен не ряд обфускаторов [11], а так называемые полиморфные генераторы для замусоривания данных, на тот случай если нарушитель поведет себя «иначе». Имеется в виду то, что, если следовать далее по концепции «технологической сингулярности», то агент адаптивно должен усложнить свой процесс за счет простых инструкций.

Основы работы предлагаемого агента чаще всего заметны в использовании простых инструкций кода. При реализации функций, нужно знать точное расположение байтов, которые мы собираемся изменять. Техника создания мультиагентных систем широко известна специалистам [6-12]. Считается, что рассвет эпохи самомодификации уже закончился [10]. Агенты не препятствуют трассировке, и для отладчика она полностью прозрачна. Зная об основных способах построения агента [9-11], предлагается перейти к их синхронизации и получения на выходе скрытого мониторинга в средах применения технологии Больших данных. Для начала следует разобрать примерную структуру агента.

Предварительно обработанные на агенте данные в виде пакетов поступают на центральный узел мониторинга [6]. Особенностью центрального узла является возможность не только совместной обработки информации, одновременно поступающей со множества программных агентов с различных узлов сети, но и обработка внутрисетевого трафика [12]. Возможности для такого рода анализа дают современные технологии параллельной обработки и потокового анализа больших данных.

Заключение

Результаты исследований в рамках гранта № 05/22-д использовались при проведении НИР и ОКР в АО «Навигатор». В рамках указанной НИР результаты исследования применялись как часть ассимиляционной модели обработки больших данных с использованием искусственного интеллекта для построения эффективной структуры бортовых баз геоинформационных данных. В рамках ОКР научные результаты проекта использовались для повышения эффективности работы ПО на основе принципа устойчивости архитектуры системы ИИ, обеспечивающего переключение на децентрализацию самоорганизующейся карты НС. Использование результатов проекта в указанных НИР и ОКР, выполненных в АО «Навигатор», позволило:

1. повысить устойчивость архитектуры ПО бортового оборудования авиационных изделий, содержащего ПНП, и работающего в условиях возможного обнаружении непредсказуемых воздействий;

2. увеличить надежность ПО для бортового оборудования на основе переключения на децентрализацию самоорганизующейся НС;

3. обеспечить переобучение пакетов ПНП, в том числе с использованием принципов автоматической пересборки и саморепликации.

Использование результатов диссертационной работы, выполненных также на специализированном ПО, позволяет:

1. эффективно реагировать на изменяющуюся внешнюю и внутреннюю среду проекта ПО, предвидя возможные развития ситуаций, связанных с созданием ИУС за счет предложенной архитектуры интеллектуальной СОВ;

2. уменьшить количество ложных срабатываний, что повысило надежность ИУС за счет переобучения ПНП в 2 раза и, следовательно возложить 95% задач защиты информации на системы искусственного интеллекта;

3. выявить успешный результат сокращения на 35% времени анализа и принятия решений по управлению ИУС.

Данное исследование выполнено при финансовой поддержке Минцифры России (грант ИБ) в рамках научного проекта, доп. соглашение №. 40469-05/2022-д/1 от 22.05.2023 г.

СПИСОК ЛИТЕРАТУРЫ

1. Петренко С.А., Киберустойчивость Индустрии 4.0: научная монография / Петренко С.А. – СПб: «Издательский Дом «Афина», 2020. – 256 с.
2. Петренко С.А., Ступин Д.Д., Национальная система раннего предупреждения о компьютерном нападении: научная монография / Петренко С.А., Ступин Д.Д. / под редакцией С.Ф. Боева. – 2-е изд. – Университет Иннополис. – Иннополис: «Издательский Дом «Афина», 2018. -448 с.
3. Что мы думаем о машинах, которые думают: Ведущие мировые ученые об искусственном интеллекте / Джон Брокман; Пер. с. англ. – М.: Альпина нон-фикшн, 2017. – 549 с.
4. Брюс, П., Практическая статистика для специалистов Data Science: Пер. с англ. / П. Брюс, Э. Брюс. — СПб.: БХВ-Петербург, 2018. — 304 с.: ил.
5. Макконнелл С. Совершенный код. Мастер-класс / Пер. с англ. – М.: Издательство «Русская редакция», 2017. – 896 стр.:
6. Штеренберг С.И., Обнаружение вторжений в распределенных информационных системах на основе методов скрытого мониторинга и анализа больших данных: диссертация на соискание ученой степени кандидата технических наук: 05.13.19 / Штеренберг Станислав Игоревич; [Место защиты: Петерб. гос. ун-т путей сообщ.]. - Санкт-Петербург, 2018. - 182 с.: ил
7. Котенко И. В., Паращук И. Б. Информационные и телекоммуникационные ресурсы критически важных инфраструктур: особенности интервального анализа защищенности // Вестник Астраханского государственного технического университета. Серия: Управление, вычислительная техника и информатика. 2022. № 2. С. 33–40.
8. Плас Дж. Вандер, Python для сложных задач: наука о данных и машинное обучение. – СПб.: Питер, 2018. – 576 с. ил. – (Серия «Бестселлеры O’Reilly»)
9. Сикорски М., Хониг Э., Вскрытие покажет! Практический анализ вредоносного ПО – СПб.: Питер, 2018. – 768 с.: ил. – (Серия «Для профессионалов»).

10. Данилин Г.В., Соколов С.С., Ныркова А.П., Кныш Т.П. Мультисервисные сети: методы повышения защищенности данных в условиях сетевых атак // XXI век: итоги прошлого и проблемы настоящего плюс. 2020. Т. 9. № 2 (50). С. 158-163
11. Гифт Ной, Прагматичный ИИ. Машинное обучение и облачные технологии. - СПб.: Питер, 2019. – 304 с.: ил. – (Серия «Для Профессионалов»).
12. Полтавцева М.А. Агрегация и нормализация гетерогенных данных в системах мониторинга информационной безопасности и обнаружения вторжений крупномасштабных промышленных КФС. // Труды ИСП РАН, том 32, вып. 5, 2020 г., стр. 131-142

Абрамов Е.С.
ЮФУ, зав. кафедрой БИТ, к.т.н.,доцент,
abramoves@sfedu.ru

РАЗРАБОТКА МЕТОДОЛОГИИ И ПРИНЦИПОВ ПОСТРОЕНИЯ ОНТОЛОГИЧЕСКОЙ МОДЕЛИ РАССЛЕДОВАНИЯ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ

Аннотация: В статье представлены результаты разработки информационной модели компьютерного преступления с использованием онтологического подхода на базе существующих моделей сценариев компьютерных атак, учитывающая все элементы преступления, криминалистически-значимые характеристики элементов, систему связей и зависимостей между элементами. Модель также может применяться для моделирования и исследования преступлений путём обобщения сведений о характеристиках элементов, что необходимо для изучения новых типов преступлений, выработки методик их расследования, определения тенденций развития киберпреступности.

Ключевые слова: модель компьютерного преступления, онтология, компьютерная криминалистика.

1 Модель компьютерного преступления

В данной статье представлены результаты разработки информационной (цифровой) криминалистической модели преступления, на основе анализа криминалистической характеристики преступлений, существующих подходов к построению моделей компьютерных преступлений (КП), и онтологического подхода к построению моделей кибератак. Также рассмотрены основные требования к такой модели. В дальнейшем термины «цифровая криминалистическая модель компьютерного преступления» и «информационная модель компьютерного преступления» будут использоваться как синонимы.

1.1 Структурные способы совершения компьютерных преступлений

Способы компьютерных преступлений являются полноструктурными [3], поэтому могут быть выбраны различные способы подготовки, совершения и сокрытия, слабо коррелирующие с видом преступления.

Полноструктурный способ (структура способа состоит из подготовки, совершения и сокрытия преступления).

Усеченный способ:

– Подготовка, совершение (сокрытие возможно в комплексе действий по подготовке и совершению преступлений).

– Только действия по совершению преступления (преступления с внезапно возникшим умыслом, в состоянии алкогольного/наркотического опьянения, в состоянии аффекта).

– Совершение и сокрытие преступления (преступления с внезапно возникшим умыслом).

– Сокрытие преступления – совершается, как правило, заинтересованными лицами и без ведома исполнителя.

1.2 Требования к разработке криминалистической модели компьютерного преступления

В теории криминалистики криминалистическая характеристика преступлений - это научная абстракция, в которой находит отражение в обобщенном виде совокупность взаимосвязанных, криминалистически значимых данных о преступлениях определенного вида/разновидности, знание которых позволяет методически правильно организовать расследование и в частности определить типовые следственные версии. Является одним из элементов частной криминалистической методики, представляющий собой систему сведений о типичных криминалистически значимых признаках преступлений и связях между ними, знание которых помогает в выдвижении версии о совершенном преступлении.

Для расследования компьютерных преступлений принципиально важно иметь их цифровые модели, которые будут максимально адаптированы к использованию в цифровой среде и с инструментарием, предназначенным для работы с компьютерной информацией .

Важно заметить, что такая модель именно цифровая, поскольку в своем содержании имеет выражение свойств преступлений в виде математических/формальных символов и должна быть представлена в машиночитаемой кодировке. Здесь на первый план вы ходит машинное моделирование, под которым понимается реализуемый на вычислительной машине метод исследования, предполагающий замену реального процесса его математической моделью [1].

Ключевая особенность такой модели: в достижении цели противодействия киберпреступности она должна позволять анализировать различные специфические объекты цифровой среды, нестандартную сетевую активность, паттерны поведения в Интернет-пространстве и т.п . Модель должна являться инструментом установления криминального события того или иного вида по его цифровым следам. Для компьютерных преступлений следует учитывать, что одним и тем же способом могут совершаться различные виды преступлений.

Сформулируем требования общего характера к таким моделям:

1) отсутствие избыточности в ее математическом описании;

2) адекватность, состоящая в наиболее точном воспроизводстве конкретного вида преступлений как объекта-оригинала;

3) обеспечение прозрачности получаемого результата для человека и машины, заключающейся в «его понятности пользователю не математику и в то же время пригодности для дальнейшей обработки в качестве компьютерной информации» [2];

4) релевантность элементов, т.е . воспроизводство тех признаков и закономерностей, которые необходимы именно для выявления, расследования и предупреждения преступных деяний;

5) использование определений признаков из соответствующей предметной области, выражающихся системой понятий, присущих объектам-оригиналам.

2 Анализ источников и подходов к разработке информационной модели компьютерного преступления

Согласно [4], основным принципом формирования информационно-компьютерных моделей должна является возможность ранжировать их по сложности способов реализации

противоправных действий, включая используемые IT-технологии и корреляции с этими способами уровня компетенции преступников, состава преступной группы или сообщества. Корреляционные связи существуют также между способом компьютерного преступления и компьютерной грамотностью потерпевшего, которая также может иметь разные уровни компетентности. Информационно-компьютерные модели компьютерных преступлений при обобщении больших массивов информации могут служить одним из основных элементов частных криминалистических методик расследования. Учитывая эти принципы, а так же требования 1-5 и предыдущего раздела, проанализируем существующие подходы к разработке цифровой криминалистической модели компьютерного преступления.

Несмотря на давно появившуюся потребность в подобных моделях, лишь относительно недавно начали появился исследования, ставящие целью разработку модели КП как системы криминалистически значимых взаимовлияемых элементов и связей между ними. Данный подход является онтологическим [5], в отличие от ранее предлагавшихся подходов на основе таксономий.

Таксономия учитывает один тип отношений, тогда как онтология учитывает множество различных сложных отношений между концепциями.

Онтология, является более сложной формой категоризации. Можно сказать, что это сложный вариант таксономии. Он включает в себя форму таксономии иерархической структуры для категоризации, но также включает в себя произвольные сложные отношения для классификации понятий. Эти произвольные сложные отношения показывают различные отношения между концепциями, отличными от простых родительско-дочерних отношений. Здесь одна категория может быть связана с несколькими другими категориями.

Далее представлено краткое изложение существующих подходов к построению моделей и классификации компьютерных преступлений.

Общепринятый подход, используемый для классификации киберпреступлений в целом и используемый в некоторых из цитируемых исследований, заключается в том, чтобы сосредоточиться на роли технологий в совершении преступления .

В этом общепринятом подходе киберпреступления классифицируются как одна из двух дихотомий высшего уровня: *«преступления с использованием компьютеров»* или *«преступления, нацеленные на компьютеры»*. Согласно [6], «преступления с использованием компьютера» - это преступления, которые предшествовали Интернету, но получили новую жизнь в киберпространстве, т.е. мошенничество, воровство, отмывание денег, сексуальные домогательства, разжигание ненависти и порнография, а «преступления нацеленные на компьютеры» - это те преступления, которые возникли одновременно с созданием Интернета и не могли существовать отдельно от него, т.е. взлом, вирусные атаки и порча веб-сайтов. Очевидно, такой бинарный подход не может служить основой для систематизации быстро меняющихся КП .

В работе [7] предложена таксономия и онтологическая структура классификации компьютерных сетевых атак, которая позволяет классифицировать сетевые атаки по классам: сценарий атаки, субъект, местоположение субъекта, агрессор, цель атаки, мотивация, область действия, уязвимость, актив, эффект, фаза, механизм атаки и уровень автоматизации. Внутри каждого класса предоставляется дополнительная информация для классификации сетевых атак. Хотя эта онтологическая структура ориентирована исключительно на атаки на компьютерные сети, ее стиль и структура основываются на общепринятой в сфере информационной безопасности терминологии и типовых подходах к классификации

атакующих действий. При этом с точки зрения модели КП классификация определяют дополнительные классы/характеристики, которые можно использовать для классификации КП . К недостаткам предложенного онтологического подхода можно отнести то, что он ориентирован исключительно на атаки на компьютерные сети и не может обрабатывать целый ряд КП , в частности совершенных против отдельных лиц, а также не может представлять смешанные типы атак.

В работе [8] предложена онтология для классификации киберпреступлений. Основными понятиями, представленными в онтологии, являются: действие, агент, контакт, внешний наблюдатель, воздействие, местоположение, мотивация, акт социальной инженерии, цель, технологическая роль и точка зрения. Представленная онтология является информативной, поскольку она предлагает несколько характеристик для классификации киберпреступлений, пытаясь дать комплексное представление о КП . К недостаткам онтологии относятся то, что она изначально разрабатывалась для оценки влияния КП на общество, на «внешнего наблюдателя». Кроме того, не используются такие элементы КП , как уязвимость, эксплуатационное и информационное воздействие.

Ни одна из рассмотренных работ не предлагает достаточно целостной модели для описания КП , т.к. они не могут учитывать целый ряд постоянно меняющихся типов КП и неспособны учитывать сложные взаимодействия между преступником (атакующим), жертвами, воздействиями, местоположениями, мотивами и собственно событием преступления.

Таким образом, существующие модели на основе таксономического подхода недостаточны, узки по своему охвату, поскольку каждая из них фокусируется на отдельных точках зрения (например, роль компьютера, атака, точка зрения злоумышленника или защитника) или используют разные терминологии для обозначения одного и того же объекта. Кроме того, они не могут эффективно представлять диапазон постоянно обновляющихся типов компьютерных преступлений. Онтологический подход важен для предметной области, поскольку одно и то же КП может классифицироваться следователями по-разному, что приводит к неточному выявлению тенденций и моделей преступления. Разрабатываемая модель должна избежать этих ограничений путем использования более полной онтологии классификации КП , которая включает несколько точек зрения (например, событие преступления, злоумышленника, воздействие, мотив, жертва, цель, заявитель, уязвимость, средства совершения преступления, местонахождение (источник воздействия) и само правонарушение), расширяя таким образом количество знаний в модели.

Разрабатываемая информационная модель КП должна отвечать следующим требованиям:

1. Использование общепринятой в сфере информационной безопасности терминологии и подходов к онтологическому описанию КП .
2. Включать разные точки зрения для анализа КП и систему взаимосвязей между элементами, предоставляющими эти точки зрения.
3. Иметь гибкую расширяемую структуру элементов, представленную в виде формальной онтологической модели взаимодействия элементов.

Такая модель позволит не только более полно описывать совершаемые КП , но и иметь возможность расширяться под новые элементы и типы КП . Использование формального описания должно упростить обмен знаниями в экспертном сообществе и между программным обеспечением.

3 Разработка базовой онтологической модели компьютерного преступления

3.1 Базовая онтологическая модель компьютерного преступления

Основываясь на результатах проведённого анализа и на сформулированных требованиях, перейдём к разработке модели.

Для реализации модели КП в по схеме «сущность-связь» решено было использовать ER-диаграммы.

Схема «сущность-связь» (также ERD или ER-диаграмма) - это разновидность блок-схемы, где показано, как разные «сущности» (люди, объекты, концепции и так далее) связаны между собой внутри системы. ER-диаграммы чаще всего применяются для проектирования и отладки реляционных баз данных в сфере образования, исследования и разработки программного обеспечения и информационных систем для бизнеса. ER-диаграммы (или ER-модели) полагаются на стандартный набор символов, включая прямоугольники, ромбы, овалы и соединительные линии, для отображения сущностей, их атрибутов и связей. Эти диаграммы устроены по тому же принципу, что и грамматические структуры: сущности выполняют роль существительных, а связи – глаголов.

Таким образом, модель КП , разработанная на основе ER-диаграммы, может представлять компьютерное преступление как систему (под структурой системы понимают состав ее элементов и постоянные связи между ними), и учитывать основные элементы КП , их характеристики (атрибуты) и связи между ними.

Разработанная концептуальная онтологическая модель компьютерного преступления представлена на рис. 1. Эта модель определяет основные элементы КП , характеристики элементов в виде атрибутов, и отношения между ними. Характеристики элементов концептуальной модели обсуждаются ниже. Модель разработана с возможностью расширения, и при необходимости в неё могут быть добавлены дополнительные элементы, характеристики и отношения.

3.2 Характеристики модели

Событие преступления **Attack_Event** – это КП в реальном мире, связанное с использованием компьютеров, или преступление, совершенное злоумышленником полностью в цифровом пространстве. Важными характеристиками являются, в т.ч., даты начала и окончания **Attack_Event** –если они известны, либо надо предпринимать действия по их установлению (***+StartTime, +EndTime***).

Уязвимость **Vulnerability** – это недостаток или слабое место в системе, которое используется Преступником (**Attacker**) в **Attack_Event**. Таким образом, *уязвимость* применима только к событию преступления, совершенному против информационно-коммуникационной техники. Существует большое множество классификаций уязвимостей автоматизированных систем (NVD/CVE, ФСТЭК и др.), рассмотрение которых выходит за рамки этой статьи. В настоящем исследовании уязвимости классифицируются следующим образом: уязвимость реализации (***+ImplementationVulnerability***), уязвимость проектирования (***+DesignVulnerability***), уязвимость конфигурации (***+ConfigurationVulnerability***) и уязвимость политики безопасности (+***SecurityPolicyVulnerabilit***).

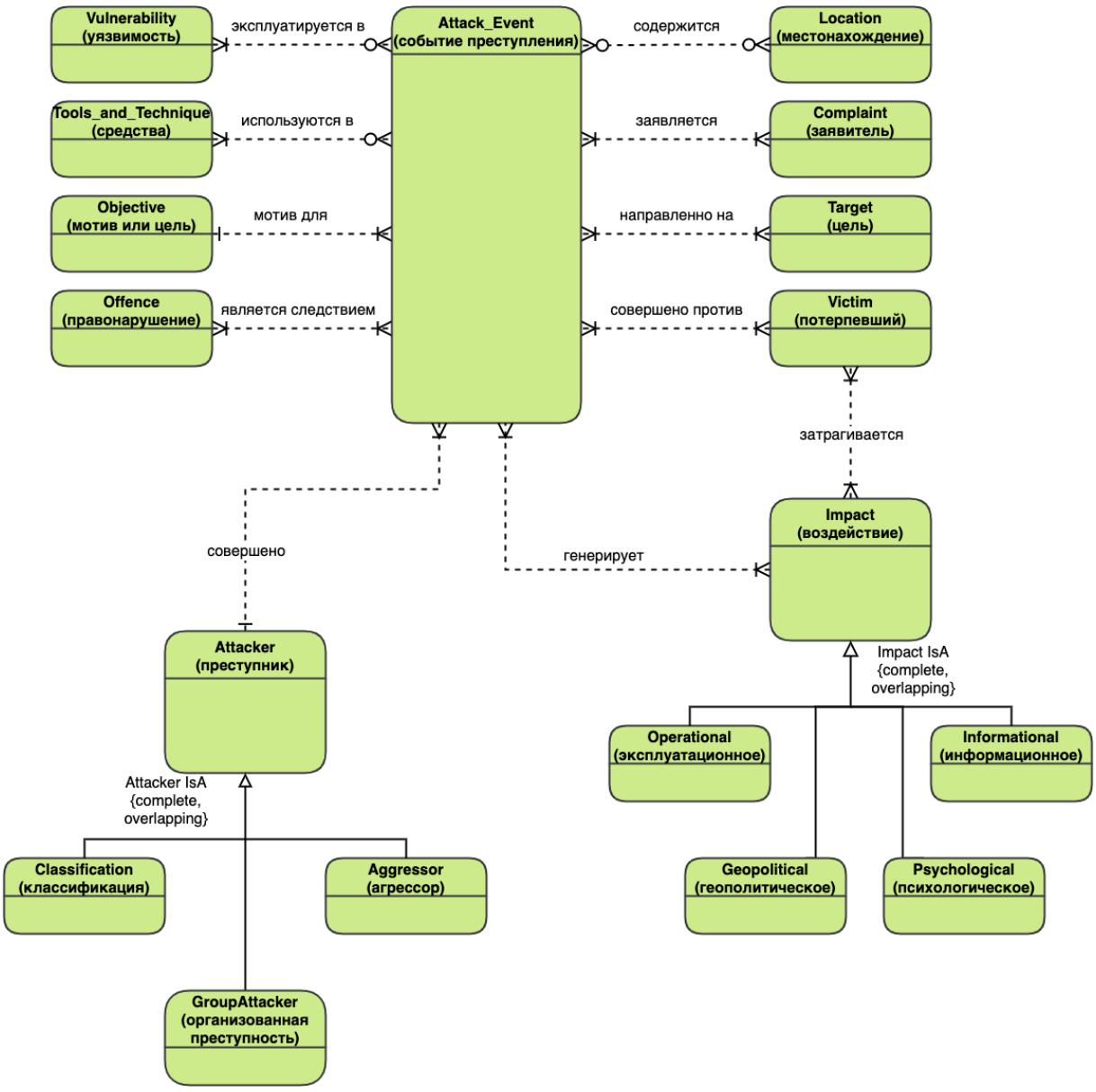


Рис. 1 Базовая онтологическая модель компьютерного преступления

Средства **Tool_and_Technique** можно рассматривать как инструментальные средства и методы (т. е. инструменты и/или техники), используемые Преступником (**Attacker**) для выполнения **Attack_Event**. В модели используются следующие характеристики **Tool_and_Technique**: средства (***+Tool***), социальная инженерия (***+SocialEngineering***), тайный сговор (***+IllicitCollusion***) и вектор атаки (***+AttackVector***).

Мотив **Objective**. Мотив можно рассматривать как главную цель, мотив или конечную задачу преступника (**Attacker**) совершающего **Attack_Event**. Некоторые характеристики: месть ***(+revenge)***, обогащение (***+enrichment***), ненависть (***+hatred***), хулиганство (***+bullying***), самосохранение (***+SelfPreservation***) и мораль (***+moral***).

Правонарушение **Offence**. Правонарушение может является отсылкой к определениям незаконных действий в отношении компьютерной информации, используемым в статьях УК РФ (272-274 статьи). Примером может служить «неправомерный доступ к компьютерной информации» [9].

Расположение **Location**. Расположение затрагивает пять других элементов: Преступник, событие преступления, жертва, заявитель и цель (соответственно ***+Attacker,***

+Attack_Event, +Victim, +Complainant, +Target). Местонахождение относится к стране (как правило) и/или конкретному адресу преступника/преступной группы, жертвы и/или цели, с которой происходит событие **Attack_Event**, заявителя, который сообщает о событии преступления **Attack_Event**, и откуда запускается событие преступления. Событие преступления **Attack_Event** может быть запущено из нескольких источников.

Заявитель **Complainant**. Заявитель – это тот, кто сообщает о событии преступления, информируя власти о незаконной деятельности. Заявитель может частным лицом или организацией ***(+private, +group*** и ***+organization***). Кроме того, заявитель может быть или не быть жертвой. Например, если домашний компьютер причастен к КП , его владелец может быть одновременно и потерпевшим, и заявителем. Но взломанный ПК в организации означает, что потерпевшей стороной становится организация, а сотрудник, работавший на ПК – заявителем, хотя воздействие (**Impact**) будет направлено на него.

Потерпевший **Victim**. Потерпевший (или жертва преступления) – это объект, на который каким-то образом влияет событие преступления **Attack_Event**. Характеристики **Victim**: ***+IndividualVictim, +GroupVictim, +OrganizationVictim, +GovernmentVictim***. *Потерпевший* может быть или не быть конкретной целью преступления. Если *Потерпевший* был конкретной целью, то значения **Victim** и **Target**(цель) совпадают. С другой стороны, если, например, *Преступник* массово распространяет вирус, *Потерпевший* не обязательно является конкретной *Целью*, но становится жертвой преступления в зависимости от наличия *Уязвимости* в конкретной автоматизированной системе.

Цель **Target**. Цель – это объект, на который конкретно направлено событие преступления **Attack_Event**. Для идентификации цели используются следующие характеристики: ***+TargetInfrastructure, +TargetPersonalDevice, +TargetNetworkDevice, +TargetOrganization, +TargetIndividual, +TargetGovernment, +TargetGroup, +TargetSoftware, +TargetSite, +TargetSkills***. Необходимо отметить, что **Attack_Event** может включать одну или несколько целей.

Влияние **Impact**. Воздействие может быть определено как прямое воздействие события преступления на жертву. В данном исследовании в качестве характеристик воздействия используются эксплуатационный (включающий операционный и экономический эффект), информационный, психологический и геополитический эффект.

Преступник **Attacker**. Преступник может быть определен как объект, который пытается совершить или совершает преступление **Attack_Event** способом, определённым в перечне *Правонарушений*. Классификация выделена в отдельный элемент, так как она:

- важна,
- изменчива,
- может применяться несколько классификаций одновременно.

Преступник может быть как одиночкой, так и группой. В статье используются четыре типа **GroupAttacker**: ***+OrganizedCriminalGroup, +StateGroup, +SexualGratificationGroup, +IdeoliticalGroup*** [10].

Преступник может быть *Агрессором*. Согласно [7] *Агрессор* характеризует причину вовлечённости *Преступника* в *Преступление*, а не тип *Преступника*. То есть *Преступник* может быть нанят для совершения КП , либо это может входить в его должностные обязанности и он получил санкцию на совершение **Attack_Event**. Характеристики *Агрессора*: ***+State, +Commercial, +Individual, +SelfIncited, +Unknown***. Следует отметить, что когда

атакующий и агрессор совпадают, применяется SelfInstigator (Самостоятельный исследователь) [7].

Кроме того, обязательной характеристикой *Преступника* является уровень владения компьютерными технологиями ***+TargetSkills***.

4 Возможности применения онтологическая модели компьютерного преступления

Разработанная модель предоставляет возможность и необходимость моделирования компьютерных преступлений путем обобщения на основе изучения больших массивов уголовных дел сведений о криминалистически значимых характеристиках вида преступления и их закономерных связях между собой [4].

На основании выделения общности способов для различных видов преступлений, совершаемых с использование компьютерных средств и систем, возможно формирование информационно-компьютерных моделей преступлений, которые будут отличаться предметами посягательства и потерпевшей стороной, а так же учитывать информацию об уровень владения компьютерными технологиями преступника и потерпевшей стороны [11].

Другим примером является изучение компьютерных атак на локальные корпоративные сети. Эти атаки могут быть как внешними, так и производиться изнутри организации с участием её сотрудников. Заметим, что преступник-инсайдер может использовать вредоносные программы, как и внешний нарушитель. Причем его участие может быть опосредованным путем предоставления соучастникам сведений, необходимых для несанкционированного доступа к корпоративной компьютерной сети, в том числе об уязвимых местах в программном обеспечении либо ошибках в настройках сетевого оборудования. Подобные факты и закономерности также позволяет учитывать разработанная модель компьютерного преступления.

При проведении форензик-экспертиз эксперт сталкивается с задачей синтеза обоснования соответствия артефактов исследования характеристикам, криминализирующим исследованное деяние в соответствии с определениям уголовного кодекса.

Рассмотрим возможность применения модели КП при разработке синтезирующей части экспертного заключения на примере [12].

Для синтеза заключения о наличии незаконных функций в рассматриваемом ПО (тех, которые приводят к уничтожению, блокированию, модификации, копированию компьютерной информации и нейтрализации средств защиты компьютерной информации) экспертам необходимо описать схемы вредоносных программных воздействий на компьютерную информацию (КИ), циркулирующую в ИС. С точки зрения разработанной модели необходимо установить характеристики элемента **Offence** по известным характеристикам **Tool_and_Technique** и **Victim/Target**, уже установленным ранее в ходе форензик-экспертизы.

Необходимо отметить, что сейчас данное решение не имеет чётко установленных параметров для отнесения их к уголовно наказуемым деяниям, и целиком должно являться результатом профессионализма экспертов. Для решения задачи эксперты использовали модель описания вредоносного программного воздействия (рис. 2) в виде набора элементов *{субъект воздействия, (тип воздействия$_i$, тип воздействия$_{i+1}$, …, тип воздействия$_N$), объект воздействия}* [12].

Рис. 2 Модель описания вредоносного программного воздействия

Уже на данном этапе видно, что предложенная экспертами модель воздействия укладывается в разработанную модель КП с использованием элементов:

- Tool_and_Technique,
- Target,
- Impact,
- Victim.

Под *субъектом воздействия* понималось конкретное вредоносное программное обеспечение (ВПО), реализующее заведомо вредоносные функции, специально разработанное для осуществления преступления. В терминах модели это Tool_and_Technique.

Под *объектом воздействия* понималась конкретная компьютерная информация, подвергнувшаяся воздействию ВПО (Victim/Target). В данном случае Victim и Target совпадают.

Под *типом воздействия i* понимались один или несколько из перечисленных методов вредоносного программного воздействия:

- модификация КИ,
- уничтожение КИ,
- блокирование КИ,
- копирование КИ,
- нейтрализация (обход) средств защиты КИ.

В терминах модели это Offence.

Далее рассмотрим подробно схемы вредоносных программных воздействий отталкиваясь от субъектов воздействия.

Одна из схема вредоносного программного воздействия представляется в виде следующего набора элементов:

{неоригинальное ПО, блокирование исполнения оригинального ПО, оригинальное ПО}

Таким образом устанавливается, что использование неоригинального ПО приводит к несанкционированному блокированию приложения оригинального ПО, то есть к невозможности осуществлять требуемые операции с компьютерной информацией ИС. С точки зрения модели КП устанавливается одна из характеристик элемента Offence – «блокирование КИ».

Другая схема вредоносного программного воздействия представлялась в виде следующего набора элементов:

{троянское программное обеспечение, (нейтрализация средств защиты, модификация загрузчика), оригинальное ПО}

Исходя из этого формулируется, что использование неоригинального ПО приводит к нейтрализации средств защиты и несанкционированной модификации компьютерной информации оригинального ПО информационной системы, путем изменения алгоритма его работы. С точки зрения модели КП устанавливаются ещё две характеристики элемента Offence – «модификация КИ», «нейтрализация (обход) средств защиты КИ».

Аналогичным образом можно представить с использованием модели все синтезирующие схемы из заключения.

Необходимо обратить внимание, что КТЭ не устанавливает вину подозреваемых – и как видно из вышеприведённого анализа, данные действия проводятся без привлечения характеристик элемента **Attacker**, исключительно с анализом программно-технических средств воздействия **Tool_and_Technique**.

5 Расширенная онтологическая модель компьютерного преступления

Базовая информационная модель компьютерного преступления включает в себя основные криминалистические характеристики преступления и взаимосвязи между ними. Опираясь на богатую практику расследования инцидентов информационной безопасности, мы можем расширить модель, добавив в неё методы выявления значений указанных характеристик. Для этого воспользуемся методами, которые предоставляет cyber threat intelligence model [13] и MITRE ATT&CK object model relationships [14]:

- Существующие технические подходы расследования инцидентов информационной безопасности опираются на методы кибербразведки (Cyber Threat Intelligence, TI) и модель описания связей между объектами атаки MITRE ATT&CK.
- Threat Intelligence сконцентрирована на получении любых знаний об индикаторах кибератак, необходимых для их обнаружения, оценке и всяческом обогащении таких знаний.
- MITRE ATT&CK модель представляет собой публичную базу знаний, содержащую онтологический набор тактик и техник поведения злоумышленников во внутренней сети организации и может быть направлена на выявление техник использования конкретных уязвимостей и определения конкретных результатов атаки.

Высокоуровневую модель расследования компьютерного преступления можно представить в виде триады (рис. 3)

Рис.3 Триада расследования компьютерного преступления.

Модель использования данных кибербразведки предполагает установление неочевидных взаимосвязей между элементами компьютерного преступления. Это достигается при помощи сбора и анализа данных из различных источников для обеспечения высокого качества анализа собранных данных требуется онтология. Модель, представленная на рисунке 4, служит этой цели и представляет собой семантическое представление анализа и расследования реализации киберугроз. Также модель может дать основу для получения конкретных количественных значений характеристик компьютерного преступления.

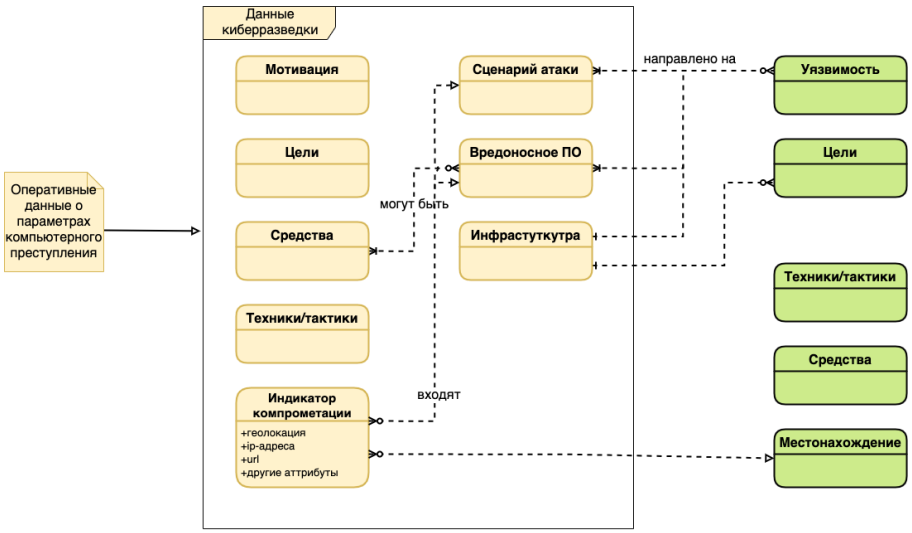


Рис. 4. Модель использования данных киберразведки.

Модель использует разнообразные разработанные таксономии, например, CWE (Common Weakness Enumeration), CAPEC (Common Attack Pattern Enumeration and Characteristics), STIX (Structured Threat Information Expression), MITRE ATT&CK, включающие информацию обо всём жизненном цикле атаки и для обмена структурированной информацией об угрозах [15].

Взаимосвязь объектной модели MITRE ATT&CK и базовой онтологической модели компьютерного преступления показана на рис. 5. Объектная модель включает акторов, техники/подтехники, программное обеспечение, тактика, а так же показывает связь с характеристиками преступления. Рисунок 6 показывает основные отношения объектов и конкретный пример их использования.

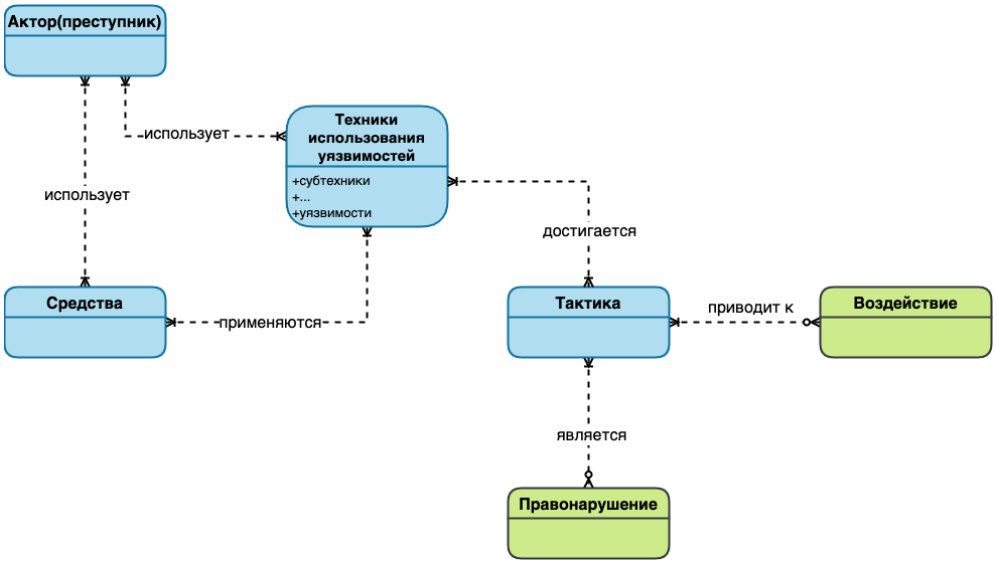


Рис. 5. Модель MITRE ATT&CK

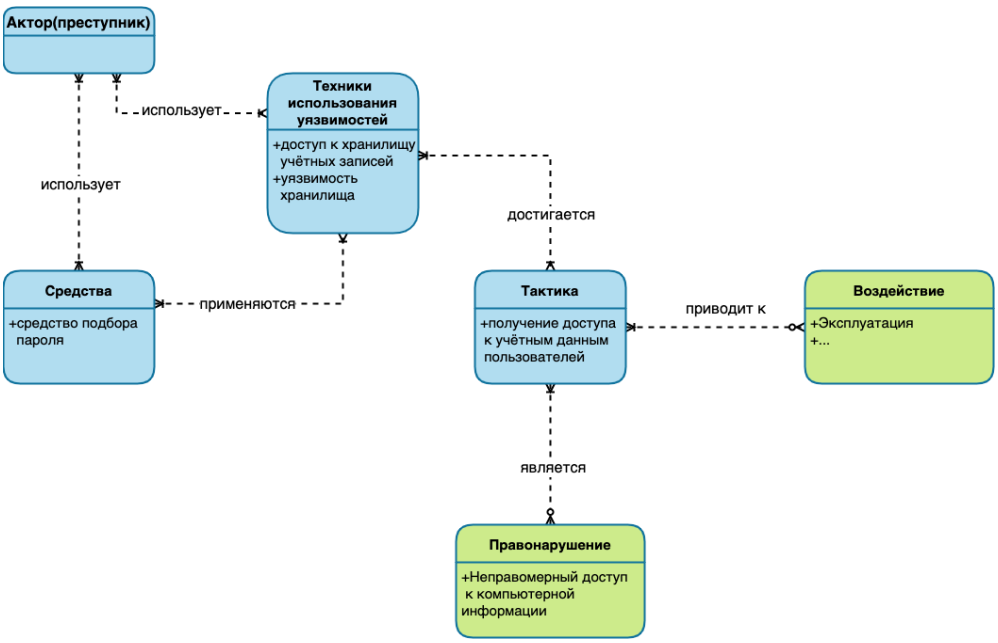


Рис. 6. Модель MITRE ATT&CK – пример использования.

Объектная модель ATT&CK реализует абстрактный уровень модели кибербразведки, которая показана на рис. 4. TTP были переданы напрямую, сущность актора MITRE ATT&CK соответствует преступнику в онтологической модели компьютерного преступления на рис. 1. Данные в MITRE ATT&CK постоянно обновляются на основе общедоступных аналитических отчетов по новым атакам.

Таким образом, для более эффективного использования онтологической модели (см. рис. 1) для расследования киберпреступления можно расширить эту модель, применив модель использования данных кибербразведки и объектную модель MITRE ATT&CK для получения конкретных количественных значений характеристик преступления, как показано на рисунке 4 и рисунке 6.

Результат совместного использования этих моделей представлен в виде расширенной онтологической модели компьютерного преступления (рис. 7).

6 Заключение

В статье проведён анализ требований к разработке криминалистической модели компьютерного преступления, сформулирован собственный набор требований. Проведён анализ подходов к разработке информационной модели компьютерного преступления, выбран онтологический подход на основе схемы «сущность-связь» с использованием ER-диаграмм. Разработана базовая онтологическая модель компьютерного преступления. Проведено исследование возможности применения разработанной информационной модели компьютерного преступления при проведении forensic-экспертиз на основе реального заключения экспертов.

В результате разработана информационная модель компьютерного преступления с использованием онтологического подхода на базе существующих моделей сценариев компьютерных атак, учитывающая все элементы преступления, криминалистически-значимые характеристики элементов, систему связей и зависимостей между элементами.

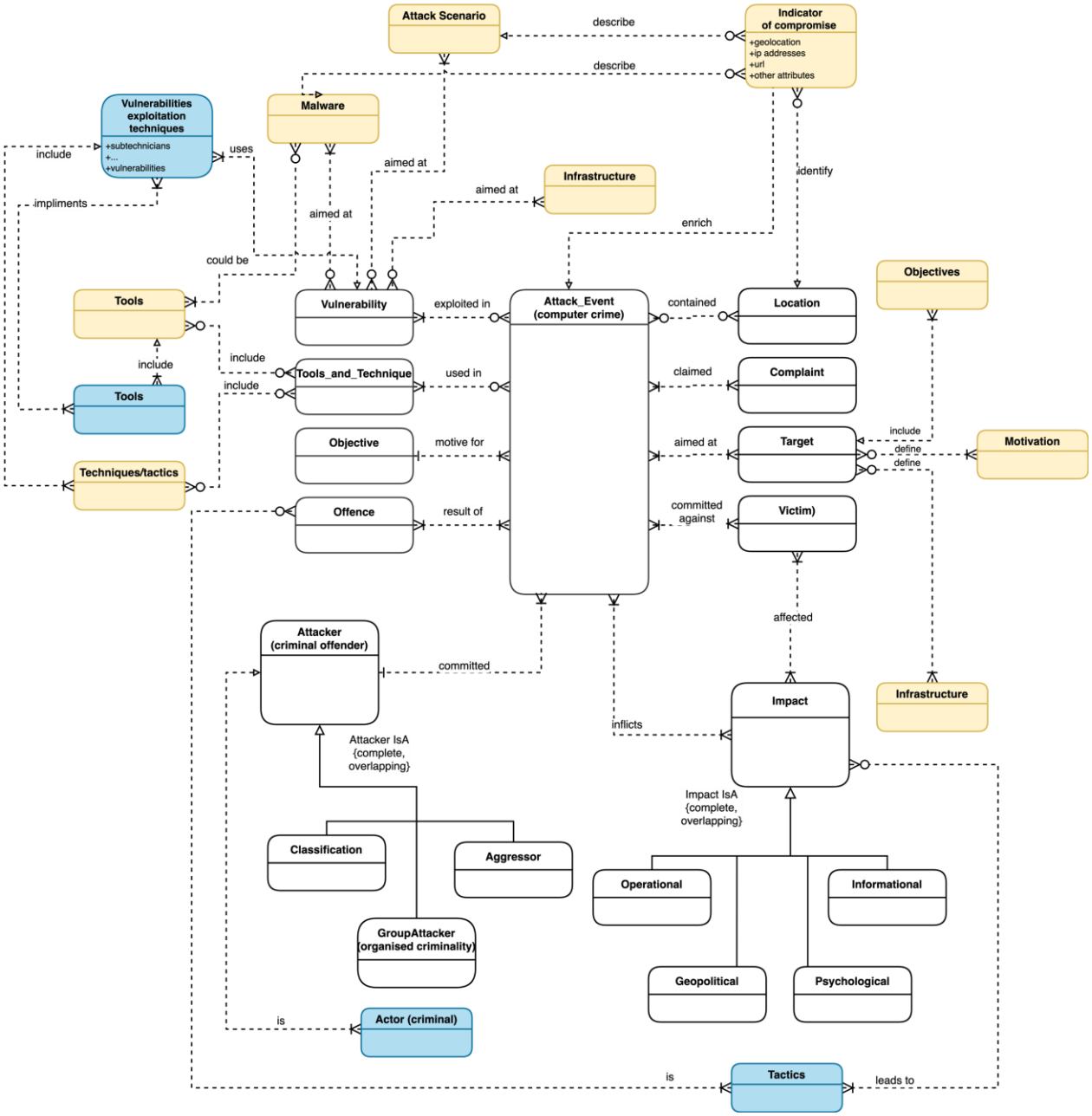


Рис. 7. Расширенная онтологическая модель компьютерного преступления

Для более эффективного использования базовой модели для расследования киберпреступления можно расширить эту модель, применив модель использования данных кибермразведки и объектную модель MITRE ATT&CK для получения конкретных количественных значений характеристик преступления

Модель может применяться для моделирования и исследования преступлений путём обобщения сведений о характеристиках элементов, что необходимо для изучения новых типов преступлений, выработки методик их расследования, определения тенденций развития киберпреступности.

Последующие исследования будут направлены на

- Наполнение теоретической модели практическими данными о расследуемых или раскрытых КП

- Разработка системы поддержки принятия решений при проведении расследования КП , в частности при формулировании вопросов следствия в рамках назначения компьютерно-технической экспертизы
- Вопросы должны позволять максимально полно идентифицировать все элементы и характеристики КП

СПИСОК ЛИТЕРАТУРЫ

1. Бессонов А.А., Монография «Искусственный интеллект и математическая статистика в криминалистическом изучении преступлений» // Издательство: Проспект. ISBN: 978-5-392-34143-6, 816 стр. 2021 г.
2. Бессонов А. А., Цифровая криминалистическая модель преступления как основа противодействия киберпреступности // Академическая мысль. - No 4 (13). – 2020. – С. 58–61.
3. Бессонов А.А., Способ преступления как элемент его криминалистической характеристики // Пробелы в российском законодательстве. 2014. №4. URL: https://cyberleninka.ru/article/n/sposob-prestupleniya-kak-element-ego-kriminalisticheskoy-harakteristiki (дата обращения: 01.09.2022).
4. Россинская Е.Р., Информационно-компьютерные криминалистические модели компьютерных преступлений как элементы криминалистических методик (на примере "кибершантажа")/ Е.Р. Россинская, А.И. Семикаленова // Вестн. Том. гос. ун-та. Право. 2021. №42. URL: https://cyberleninka.ru/article/n/informatsionno-kompyuternye-kriminalisticheskie-modeli-kompyuternyh-prestupleniy-kak-elementy-kriminalisticheskih-metodik-na (дата обращения: 01.09.2022).
5. Donalds C., Toward a cybercrime classification ontology: A knowledge-based approach / Donalds C., Osei-Bryson K. M. //Computers in Human Behavior. – 2019. – Т. 92. – С. 403-418.
6. Furnell S. Cybercrime: Vandalizing the information society. – London : Addison-Wesley, 2002. – С. 3-540.
7. Van Heerden R. P. et al. A computer network attack taxonomy and ontology //International Journal of Cyber Warfare and Terrorism (IJCWT). – 2012. – Т. 2. – №. 3. – С. 12-25.
8. Barn, R., (2016, June12-15). An ontological representation of A taxonomy for cybercrime./ Barn, R., Barn, B. // Paper presented at the 24th european conference on information systems (ECIS), Istanbul,Turkey.
9. Уголовный кодекс РФ (УК РФ 2015) (с изменениями на 30 декабря 2015 года) [Электронный ресурс]. – http://docs.cntd.ru/document/ugolovnyj-kodeks-rf-uk-rf, (дата обращения: 25.08.2023).
10. Donalds, C., A cybercrime taxonomy: Case of the jamaican jurisdiction. / Donalds, C., Osei-Bryson, K.-M. //Paper presented at the CONFirm 2014 proceedings.
11. Россинская Е.Р., Концепция учения об информационно-компьютерных криминалистических моделях как основе методик расследования компьютерных преступлений // Вестник Восточно-Сибирского института МВД России. 2021. №2. URL: https://cyberleninka.ru/article/n/kontseptsiya-ucheniya-ob-informatsionno-kompyuternyh-kriminalisticheskih-modelyah-kak-osnove-metodik-rassledovaniya-kompyuternyh (дата обращения: 22.08.2022).

12. «Заключение комиссии экспертов от 03 июня 2021 года (первичная комплексная комиссионная компьютерно-техническая судебная экспертиза по уголовному делу №11707070001100041)».
13. Mavroeidis, V., Cyber Threat Intelligence Model: An Evaluation of Taxonomies, Sharing Standards, and Ontologies within Cyber Threat Intelligence (2021). / Mavroeidis, V., Bromander, S. // https://www.duo.uio.no/bitstream/handle/10852/58492/CTI Mavroeidis. pdf?sequence=4.
14. MITRE. MITRE ATT&CK Framework (2023). https://attack.mitre.org/.
15. Mundt, M., (2022). Towards Mitigation of Data Exfiltration Techniques Using the MITRE ATT&CK Framework. In: Gladyshev, P., Goel, S., James, J., Markowsky, G., Johnson, D. (eds) Digital Forensics and Cyber Crime. ICDF2C 2021. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol 441. Springer, Cham. https://doi.org/10.1007/978-3-031-06365-7_9

Жукова М.Н.
ФГБОУ ВО «Сибирский государственный университет науки и технологий имени М.Ф. Решетнева», доцент, кандидат технических наук, доцент,
zhukova@sibsau.ru

МОДЕЛИ И АЛГОРИТМЫ МОНИТОРИНГА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СРЕДСТВ И СИСТЕМ ИНФОРМАТИЗАЦИИ, НАХОДЯЩИХСЯ ПОД ВОЗДЕЙСТВИЕМ РЕАЛИЗАЦИЙ УГРОЗ БЕЗОПАСНОСТИ

Аннотация: Работа посвящена разработке методологических основ, комплекса моделей и алгоритмов агрегации данных и их последующей обработки с поиском инсайдерской активности для формирования управляющих воздействий в рамках сценариев реагирования в условиях выполнения требований мониторинга информационной безопасности средств и систем информатизации, находящихся под воздействием реализаций угроз безопасности. Полученные результаты позволят применять модели и алгоритмы интеллектуального анализа данных, осуществляющих мониторинг событий информационной безопасности для синтеза управляющих воздействий с целью автоматизированного формирования сценариев реагирования. Расширить класс выявляемых угроз нарушения безопасности систем информатизации в условиях временных и ресурсных ограничений с использованием методов глубокого обучения. Создать алгоритмическое обеспечение для программных средств, позволяющих эффективно анализировать большие гетерогенные данные с целью выявления событий безопасности, происходящих под воздействием реализаций угроз безопасности.

Ключевые слова: мониторинг информационной безопасности, управление уязвимостями, обнаружение и анализ угроз, управление событиями, машинное обучение.

Общей целью исследования является разработка методологических основ, комплекса моделей и алгоритмов агрегации данных и их последующей обработки с поиском инсайдерской активности для формирования управляющих воздействий в рамках сценариев реагирования в условиях выполнения требований мониторинга информационной безопасности средств и систем информатизации, находящихся под воздействием реализаций угроз безопасности.

Цель исследования полностью соответствует текущей цели диссертационного исследования и направлению проводимых исследований, собираемых данных и проектируемых моделей и алгоритмов мониторинга информационной безопасности средств и систем информатизации.

В соответствии с поставленной целью сформулированы следующие задачи:

1. Системный анализ проблемы определения источников сбора данных, зависимостях сервисов и формирования подхода, позволяющего отслеживать события возникших векторов атак с применением методов искусственного интеллекта.
2. Исследование и расширение класса выявляемых угроз нарушения безопасности систем информатизации в условиях временных и ресурсных ограничений с использованием методов глубокого обучения.
3. Разработка методов интеллектуального анализа данных, позволяющих осуществлять скрытый мониторинг событий информационной безопасности при защите от

инсайдерской активности для формирования управляющих воздействий с целью автоматизированного формирования сценариев реагирования.

4. Формальное описание процессов и процедур, необходимых для синтезирования ресурсно-сервисной модели: детализации данных по инфраструктуре на уровне, достаточном для задач мониторинга информационной безопасности.

5. Аналитико-имитационное моделирование условий реализации системно-технических и архитектурных решений программных средств, позволяющих эффективно анализировать большие гетерогенные данные с целью выявления событий безопасности, происходящих под воздействием реализаций угроз безопасности .

6. Проверка работоспособности и реализуемости разработанного специального модельно-алгоритмического обеспечения и апробация разработанных решений.

Вопросам разработки методов обнаружения вторжений, анализа атак и выбора защитных мер посвящено большое количество научных работ. Задачи управления и обеспечения безопасности информационных систем на основе систем обнаружения вторжений с защищенными процессами обработки и хранения больших объемов информации исследовались в работах Зегжды П.Д., Буйневича М.В., Котенко И.В., Куо Б. и др… [1-3]. А также зарубежных исследователей: К. Нейгеля, Э. Таненбаума, К. Щипёрского, Н.В. Лихачева (Крис Касперски), М. Клеппмана, Ч. Хоара, Ф. Чезарини, Л. Авраамова, Дж. Паттерсона [4-7].

Рассмотрев существующие решения класса EDR, SOAR становится понятным, что требуется настроить большое количество различных показателей и методик вычисления различных метрик. Не существует единого подхода к выбору, определению и вычислению показателей защищенности, учитывающих различные данные на разных этапах функционирования систем защиты информации. Современные СОВ направлены в большей степени на выявление внешнего нарушителя, они не скрывают своего существования от внутреннего нарушителя и потому уязвимы для его вмешательства в процессе мониторинга. Не известно подхода к обобщенному анализу уязвимостей к атакам как со стороны внутренних, так и внешних нарушителей в ИС, при условии сбора и обработки накапливающихся с различных источников, больших данных, что определяет необходимость разработки новых моделей, методов и методик на основе применения существующих решений в интеграции с методами искусственного интеллекта для обеспечения решения задачи мониторинга информационной безопасности в условиях реализации угроз безопасности [8,9].

Логично рассматривать и применять комплексные решения, своего рода «тяжеловесы», которые позволят в рамках единого подхода решать сразу множество задач: настройка сборщиков событий безопасности, автоматизированное формирование метрик (в результате интеллектуального анализа инцидентов ИБ), агрегация данных из различных источников, их последующая обработка с желательным выявлением инсайдерской активности (по возможности «отравления данных»), дальнейшее формирования сценариев реагирования с последующей оркестрацией систем. А также неизменные требования по интеграции с SIEM, NGFW, IDS/IPS, сканерами уязвимостей, антивирусным ПО, DLP, сервисами TI, системами ITSM, Service Desk, базами данных и т. д. Кроме этого, современный объем обрабатываемой информации требует также настройки дашбордов по различным разрезам аналитики [10], с возможностью автоматического уведомления и рассылки оповещений, формирования частичного воздействия и регистрации инцидента для дальнейшей работы с ним.

Существует ряд решений, который позволяет в том или ином виде решить часть перечисленных задач (EDR BI.ZONE, SOAR Security Vision, SIEM системы различных

производителей). Однако, современное состояние развития информационных систем, с постоянным изменением ландшафта угроз, внедрением новых цифровых сервисов не позволяет использовать единый подход. Требуется внедрение синтезируемых технологий, на основе анализа данных, скрытого мониторинга событий безопасности, прецедентного подхода.

При анализе поставленных задач возникает представление о характеристиках получаемых данных, это при условии четкой постановки задачи с точки зрения определения метрик для формирования системы мониторинга информационной безопасности (например, в соответствии с ГОСТ Р 59547-2021 «Защита информации. Мониторинг информационной безопасности. Общие положения»). Даже в этом случае большинство получаемых (собираемых) данных являются гетерогенными, нечеткими, требующими серьезной предварительной обработки и агрегирования. Кроме этого, объемы собираемых данных легко соотносятся с такими понятиями как «озеро данных» или Big Data. Таким образом, требуется применение специализированных алгоритмов, в большинстве случаев относящихся к алгоритмам машинного обучения, для решения поставленных задач.

Анализ нормативно-методических документов, а также лучших зарубежных практик показывает, что, как правило, анализу подлежит определенный набор данных, заранее определяемых при настройке сборщиков данных для дальнейшего анализа в соответствующих системах, класса SIEM и тд. Однако, выявление расхождений, в большинстве случае, возможно только при наличии разнородных данных как по своей природе, так и по наличию даже малейших отклонений. Выбор того или иного источника данных, сбор и последующий анализ полученной информации должен производиться на основе возможных подозрений о реализации инсайдерской активности для формирования управляющих воздействий с целью автоматизированного формирования сценариев реагирования. Таким образом, предполагается постоянный динамический анализ защищенности информационной системы.

Данное решение невозможно реализовать в рамках единого подхода, требуется синтез различных внутренних моделей и алгоритмов, в зависимости от показателей мониторинга информационной безопасности средств и систем информатизации. Решение видится в виде ресурсно-сервисной модели, позволяющей осуществлять детализацию данных по инфраструктуре на уровне, достаточном для задач мониторинга информационной безопасности.

Большие надежды возлагаются на методы профилирования пользователей, применяемые в совокупности с механизмами мониторинга информационной безопасности различных объектов. Рост подобных решений показывает неплохую перспективность данного подхода. Однако, практика применения (а опыт еще не достаточно большой, чтобы можно было говорить о полноценной статистической информации) показывает возникновения еще больших проблем, связанных уже не только с настройкой метрик и данных для мониторинга, но и написание и подключение «коннекторов», собираемых информацию по поведению пользователей автоматизированных систем. Статистических метрик среднего и стандартного отклонения часто не достаточно. Возникают вопросы, связанные с тем, какие поведенческие индикаторы следует вводить и как оценивать и объединять их определенным образом. В распоряжении организаций обычно нет таких возможностей. С другой стороны, для приобретения знаний и накопления статистики в области мониторинга ИБ в сетях на основе больших данных требуются годы исследований.

В статье Г. Одина «Большие данные: средство, а не ответ» описываются факторы, которые ставят сложные задачи перед каждым, кто занимается обработкой больших данных и генерацией полезных, своевременных результатов их анализа:

1) количество - объем данных, производимых большим разнообразием сетевых источников, постоянно увеличивается, при этом данные поступают как в структурированной, так и в неструктурированной форме в зависимости от поставщиков ресурсов.

2) скорость доставки скорость доставки данных не должна препятствовать их быстрой обработке. Изменения трафика и конфигурации ресурсов внутри вычислительной сети может происходить за миллисекунды. Если не выполнить своевременный анализ этих данных, то их значимость может существенно снизиться. Тогда эти данные не могут быть использованы для обработки и прогнозирования ситуаций в режиме реального времени;

3) видоизменяемость - создание данных происходит не по заранее известному графику. Большие данные могут появиться как в результате непредсказуемых событий, так и в результате регулярных событий;

4) множество форматов - все данные различаются по своему формату. Разработчики решений добавляют к данным специальные расширения, обеспечивая больший объем собираемой информации и делая свои продукты наиболее привлекательными. Разнообразие форматов и расширений данных, существенно усложняет проведение анализа данных;

5) множество источников - сбор, сравнение и преобразование больших данных, полученных от различных источников, является весьма сложной задачей.

При всех проблемах, описанных выше, не стоит забывать еще и о том, что часть рассматриваемых подходов и решений, хорошо применяемых для инфраструктур автоматизированных систем, совершенно не рассматривают технологии виртуализации. Применение таких технологий, на сегодняшний день, зачастую является единственно возможным решением, по размещению вычислительных мощностей организации и выполнению бизнес-задач, поддержке системы защиты информации, обеспечение нормального функционирования штатных средств защиты информации.

Таким образом, рассмотрение единого базиса, позволяющего решать задачи мониторинга, анализа собираемых данных, разметки и применения для задач прогнозирования, не зависимо от технологии, используемой на инфраструктуре объекта — данная задача является значимой и актуальной для рассмотрения в рамках диссертационного исследования.

Экспериментальные исследования предлагается провести с помощью моделирования процессов идентификации событий безопасности, возникающих при реализации угроз на тестовых стендах, в том числе имитирующих характеристики производительности вычислительной инфраструктуры организаций различного типа.

Научная новизна заявленного исследования будет состоять в следующем:

1. Модель обработки данных, формализующая принципы агрегации и параллельной обработки потоков данных для эффективного процесса мониторинга информационной безопасности средств и систем информатизации, находящихся под воздействием реализаций угроз безопасности.
2. Формализованный подход к определению источников сбора данных, основанному на использовании входных данных об ИС и ее уязвимостях, зависимостях сервисов.
3. Методика расширения класса обнаруживаемых угроз безопасности на основе обоснованного выбора гибридной архитектуры источников сбора, агрегации и оркестрации

систем, позволяющей повысить точность обнаружения угроз безопасности и обеспечить работу с входными данными переменной структуры.

4. Методика и алгоритмы анализа, в ограниченное время, большого потока данных, релевантных цели поиска признаков реализаций угроз безопасности.

5. Модели и алгоритмы интеллектуального анализа данных, позволяющих осуществлять мониторинг событий информационной безопасности для синтеза управляющих воздействий с целью автоматизированного формирования сценариев реагирования.

6. Расширение класса выявляемых угроз нарушения безопасности систем информатизации в условиях временных и ресурсных ограничений с использованием методов глубокого обучения.

7. Разработка программных средств, позволяющих эффективно анализировать большие гетерогенные данные с целью выявления событий безопасности, происходящих под воздействием реализаций угроз безопасности.

Использование технологии больших данных при мониторинге ИБ в сетях ставит множество важных вопросов, требующих эффективных методов обработки информации. Они необходимы для углубленного понимания и оперативного принятия обоснованных решений по изменению стратегии обеспечения ИБ для ИС в соответствии с результатами анализа собранных данных. Кроме того, учитывая, что анализу подвергаются сетевые данные, становятся очевидными причины замедления интеграции мониторинга ИБ в сетях и технологии больших данных. Собираемые данные имеют различную структуру, что усложняет процесс их идентификации и эффективного анализа. Для повышения эффективности процесса мониторинга ИБ, необходим целостный подход к анализу больших данных, собранных в результате мониторинга, объединение различных методов обработки полученных данных, а также расширение возможностей средств анализа и визуализации информации.

СПИСОК ЛИТЕРАТУРЫ

1. Смирнов Д. В. Система сбора и анализа информации из различных источников в условиях Big Data / Смирнов Д. В., Грушо А.А., Забежайло М.И., Тимонина Е. Е. // International Journal of Open Information Technologies, 2021. V. 9. № 4. Pp. 64- 74
2. Штеренберг С.И. Распределенная система обнаружения вторжений с защитой от внутреннего нарушителя / С.И. Штеренберг, М.А. Полтавцева // Проблемы информационной безопасности. Компьютерные системы. 2018. № 2. С. 59-68
3. Демидов, Р. А. Анализ угроз кибербезопасности в динамических сетях передачи данных с применением гибридной нейросетевой модели / Р.А. Демидов, П. Д. 13 Зегжда, М. О. Калинин // Проблемы информационной безопасности. Компьютерные системы. – 2018. – № 2. – С. 27-33.
4. Ha D. Insider threat assessment: Model, analysis and tool / Ha D., Iyer A., Ngo H.Q., Upadhyaya S. // In Network Security. – Boston: Springer, 2010. – P. 143-174.
5. Garfinkel R. Privacy protection of binary confidential data against deterministic, stochastic, and insider threat / Garfinkel R., Gopal R., Goes P. // Management Science – 2002. – Vol. 48(6). – P. 749-764.
6. Sinclair S. Preventative directions for insider threat mitigation via access control / Sinclair S., Smith S.W., // In Insider Attack and Cyber Security. – Springer, 2008. – P. 165-194.

7. Khan M.I. Detecting anomalous behavior in DBMS logs. / Khan M.I., Foley S.N. // Risks and Security of Internet and Systems - 11th International Conference, CRiSIS 2016, Rosco, 137 France, September 5-7, 2016. – Revised Selected Papers. – Lecture Notes in Computer Science, – Springer, 2016. – Vol. 10158. – P.147-152.
8. Hussain S. R. Detecting anomalous database transactions by insiders / Hussain S. R., Sallam A. M., Detanom E. B.// In Proceedings of the 5th ACM Conference on Data and Application Security and Privacy. – CODASPY ’15, New York, NY, USA, 2015. ACM. – P.25-35.
9. Sallam A. Data and syntax centric anomaly detection for relational databases / Sallam A., Fadolalkarim D., Bertino E., Xiao Q. // Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, – 2016. – Vol.6(6). – P. 231-239.
10. Милославская Н.Г. Визуализация информации при управлении информационной безопасностью информационной инфраструктуры организации / Милославская Н.Г., Толстой А.И., Бирюков А.Л.// Научная визуализация. 2014. Том 6, №2. Стр. 74 - 91.

Магомедов Ш. Г.
РТУ МИРЭА, заведующий кафедры КБ-4 «Интеллектуальные системы информационной безопасности», к.т.н, доцент,
magomedov_sh@mirea.ru

АТРИБУТИВНАЯ МОДЕЛЬ УПРАВЛЕНИЯ ДОСТУПОМ В ОРГАНИЗАЦИЯХ ВЫСШЕГО ОБРАЗОВАНИЯ НА ОСНОВЕ АНАЛИЗА СОБЫТИЙ БЕЗОПАСНОСТИ

Аннотация: Статья посвящена разработке агентной системы управления риском в информационных технологиях высшего образования. Автор предлагают инновационный метод агрегации риска, основанный на инкрементальной безопасности и нечеткой логике. Система включает два агента, отслеживающих аспекты безопасности: неудачные попытки входа, взаимодействие пользователей с ресурсами. Предложенные агенты используют анализ данных в реальном времени и оценку контекста для выдачи оценки риска в зависимости от действий пользователей и характеристик среды. Результаты агентов агрегируются в общий уровень риска с помощью нечетких правил. Разработанная модель позволяет эффективно управлять безопасностью и принимать управленческие решения, направленные на минимизацию рисков.

The article focuses on the development of an agent-based risk management system in higher education information technology. The authors propose an innovative risk aggregation method based on incremental security and fuzzy logic. The system comprises two agents monitoring security aspects: failed login attempts, user-resource interactions. The proposed agents use real-time data analysis and context assessment to provide risk assessment based on user actions and environmental characteristics. The agents' results are aggregated into an overall risk level using fuzzy rules. The developed model enables efficient security management and decision-making to minimize risks.

Ключевые слова: управление доступом, информационные технологии, риск безопасности, агентная система, инкрементальная безопасность, нечеткая логика, высшее образование.

access control, information technology, security risk, agent-based system, incremental security, fuzzy logic, higher education.

Введение

Изменение политической обстановки в последние годы обусловило необходимость пересмотра как текущих аспектов защиты информации, так и основополагающих принципов в области информационной безопасности в организациях высшего образования. Одним из ключевых принципов обеспечения информационной безопасности является применение политик безопасности, которые позволяют применять технические, организационные и правовые меры для обеспечения защиты как критической информационной инфраструктуры и государственных информационных систем, так и обрабатываемой информации. Существующие подходы к управлению безопасностью базируются на использовании статических или частных политик безопасности (средств защиты) для объектов критической информационной инфраструктуры, информационных систем и других объектов информатизации[1].

Использование статических подходов безопасности позволяет обеспечить необходимый уровень защиты от известных и существующих угроз безопасности. Однако этот

подход требует внесения изменений в конфигурацию средств защиты при модификации или реконфигурировании технических средств объектов информатизации при существенном изменении внешних условий.

Традиционные модели управления доступом основаны на логике доступа к ресурсам на основе правил управления доступом[2]. Этот метод решает большинство проблем при разграничении доступа к объектам, но имеет существенный недостаток. Он заключается в применении статичных, предопределенных политик безопасности, которые не гарантируют безопасность объектов доступа в изменяющихся условиях окружающей обстановки. В различных ситуациях традиционные модели формируют одно и то же решение по управлению доступом. Подобное поведение не позволяет использовать их в качестве адаптивных методов в изменяющихся условиях.

В последние годы в мире часто фиксируют инциденты, связанные с утечкой конфиденциальной информации из-за внутренних нарушителей как в частных, так и в государственных учреждениях. Из-за недетерминированного поведения пользователей иногда достаточно сложно отличить легитимные запросы на предоставление полномочий на основе традиционных статичных моделей управления доступом.

Развитие атрибутивной модели управления доступом в организациях высшего образования с фокусом на анализ событий безопасности является актуальным. Для оценки риска предлагается использование агентов. Традиционные методы управления доступом, хотя эффективны в некоторых случаях, связаны с определенными ограничениями. Они устанавливают связь между логикой управления доступом и запрашиваемым ресурсом. Реализация этих моделей позволяет управлять доступом в различных сценариях, включая непредвиденные ситуации из-за неудачно спроектированных политик доступа, а также возможное злоупотребление доступом со стороны злоумышленников, получивших доступ к существующим учетным записям. Тем не менее, традиционные модели неспособны эффективно управлять непредвиденными сценариями и ситуациями, так как они основаны на статических и заранее определенных политиках.

Управление доступом на основе атрибутов (Attribute-Based Access Control, ABAC) представляет собой перспективную парадигму, при которой авторизация субъекта для выполнения определенных операций зависит от атрибутов, связанных с субъектом, объектом и запрашиваемыми операциями, а также контекстуальных атрибутов окружающей среды. Этот метод легко адаптируется и настраивается с использованием различных атрибутов, что делает его подходящим для распределенных и быстро меняющихся сред. ABAC способен выражать сложные наборы правил, учитывая множество различных атрибутов субъекта и объекта, что устраняет необходимость в явных авторизациях отдельных субъектов. ABAC считается моделью авторизации «следующего поколения» из-за своей способности обеспечивать динамическое, контекстно-зависимое и интеллектуальное управление доступом, а также предлагать гибкость в реализации, используя существующую инфраструктуру.

Существующие модели контроля доступа страдают от отсутствия динамичности и точности оценки риска. Однако современные исследования предпринимают попытки заполнить этот пробел, разрабатывая модели, которые используют функции реального времени для принятия динамических решений о доступе приложений. Одной из перспективных моделей является модель управления доступом на основе риска, которая анализирует риски для каждого запроса на доступ и динамически разрешает или запрещает доступ на основе предполагаемого значения риска. Однако основной проблемой является

недостаток надежной методики оценки рисков, особенно в отсутствие достаточных данных для описания вероятности и воздействия риска. В данной статье предложена модель нейро-нечеткой системы (NFS) для оценки значения риска безопасности, связанного с каждым запросом доступа. Результаты исследования показали, что алгоритм Левенберга-Марквардта (LM) является оптимальным для реализации этой модели. Эта модель обеспечивает эффективное время обработки и может применяться для принятия динамических и контекстно-зависимых решений о доступе на основе функций реального времени. Ее эффективность была проверена на примере сценариев контроля доступа в детской больнице, что продемонстрировало ее потенциал в принятии решений о доступе для различных приложений.

Основной текст

Атрибутивная модель управления доступом не ограничивает сложность процессов. Из-за более простой реализации в рамках применения этого подхода стоимость поддержки при реализации более сложных правил не увеличивается. Кроме того, появляется возможность обеспечения контроля доступа и к действиям, и к данным. Данная модель является набором условий, в которых атрибуты должны соответствовать требованиям, предъявляемым к ним[4]. Можно явно выделить несколько категорий атрибутов:

- атрибуты ресурса (тип, создатель, стоимость, название и т. д.);
- атрибуты субъекта (имя, отдел, должность, лимит утверждений и т. д.);
- атрибуты действия (название);
- атрибуты среды (IP-адрес, время, устройство).

Для того чтобы выполнить авторизацию, сравнивают значения всех атрибутов в момент проверки прав и ожидаемые значения. Доступ к ресурсу обеспечивается при выполнении всех условий.

Спроектируем ИТ-инфраструктуру образовательного учреждения с применением атрибутивной модели управления доступом.

Инфраструктура образовательного учреждения включает в себя значительное число связанных между собой элементов, безопасность которых необходимо обеспечить:

- сервисы управления образовательным процессом;
- сервисы управления научными проектами;
- сервисы управления персоналом;
- сервисы контроля и управления доступом;
- сервисы бухгалтерского учета;
- сервисы управления инфраструктурой и т. д.

Среди угроз ИТ-инфраструктуре организации, работающей в сфере образования, можно назвать рассылку сообщений с вредоносными вложениями, попытки несанкционированного доступа к данным организации и многие другие. Злоумышленники разрабатывают все более совершенные механизмы атаки на информационные системы организаций, в т.ч. образовательных учреждений. Тогда в качестве атрибутов доступа ИТ-сервисов высшего образования можно выделить следующие атрибуты:

- роль: студент, преподаватель, административный персонал, внешние сущности, руководители подразделений;
- тип устройства доступа: рабочий ПЭВМ, ноутбук, мобильное устройство;

- тип сервиса: сервисы управления образовательным процессом, сервисы управления научными проектами, сервисы управления персоналом, сервисы контроля и управления доступом, сервисы бухгалтерского учета, сервисы управления инфраструктурой;
- местоположение: кампус 1, кампус 2, …, кампус N, филиал;
- тип подключения: VPN, внутренняя сеть, сеть Интернет;
- действие: запись, чтение, создание, удаление.

Необходимым требованием к ИТ-инфраструктуре организации является обеспечение защиты информационной образовательной среды организации и постоянного мониторинга и верификации пользователей. При этом пользователь должен иметь возможность оставаться в сеансе доступа к информационному ресурсу в течение времени, необходимого для работы. Работы в области адаптивной безопасности [5] показали, как применять этот вид проверок на основе различных техник.

Одна из них это – «Контекстно-зависимая безопасность».

Этот подход опирается на контекстно-зависимую информацию, такую как геолокация, время доступа, репутация определенного IP-адреса или домена, тип используемого устройства и т.д., для принятия решений по предоставлению доступа[6]. Вся эта информация, собранная и обработанная динамически, может обеспечить бóльшую защищенность и гранулярность относительно статических методов в различных областях применения. Эта концепция появляется в большинстве случаев в сценариях аутентификации и авторизации в распределенных системах, решение о предоставлении доступа может быть основано на различных процедурах или атрибутах в зависимости от контекста конкретного запроса[7].

Дополнительной техникой является инкрементная (интеллектуальная) безопасность[2].

Этот подход обычно сочетает в себе различные методы и инструменты, такие как большие данные, аналитика или управление информацией и событиями безопасности, для обнаружения аномалий, выбросов или отклонений от стандартного поведения и принятия соответствующих мер. Инкрементальная/интеллектуальная безопасность основана на сборе, стандартизации и анализе данных, генерируемых сетями, приложениями, базами данных, журналами и другой инфраструктурой в режиме реального времени. Эта информация оценивается и обрабатывается (с помощью машинного обучения, распознавания образов и т.д.) для перевода данных в удобочитаемый формат, который поддерживает принятие обоснованных решений.

Значения для реальных данных

Иллюстрация работы системы оценки риска на основе агентов мониторинга логов

Для иллюстрации работы алгоритмов нечеткого логического вывода при агрегации показаний агентов было создано 2 простых агента с настраиваемыми параметрами.

Агент наблюдения за пользователями (Агент А)

Этот агент следит за количеством неудавшихся попыток входа, выдает уровень риска (от 0 до 10) если таких попыток много за период времени. Пороговые значения для определения уровня риска настраиваются. Выдает уровень риска в зависимости от количества неудачных аутентификаций за 10 минут.

На рисунке 2 показан пример возвращаемого уровня риска агентом В.

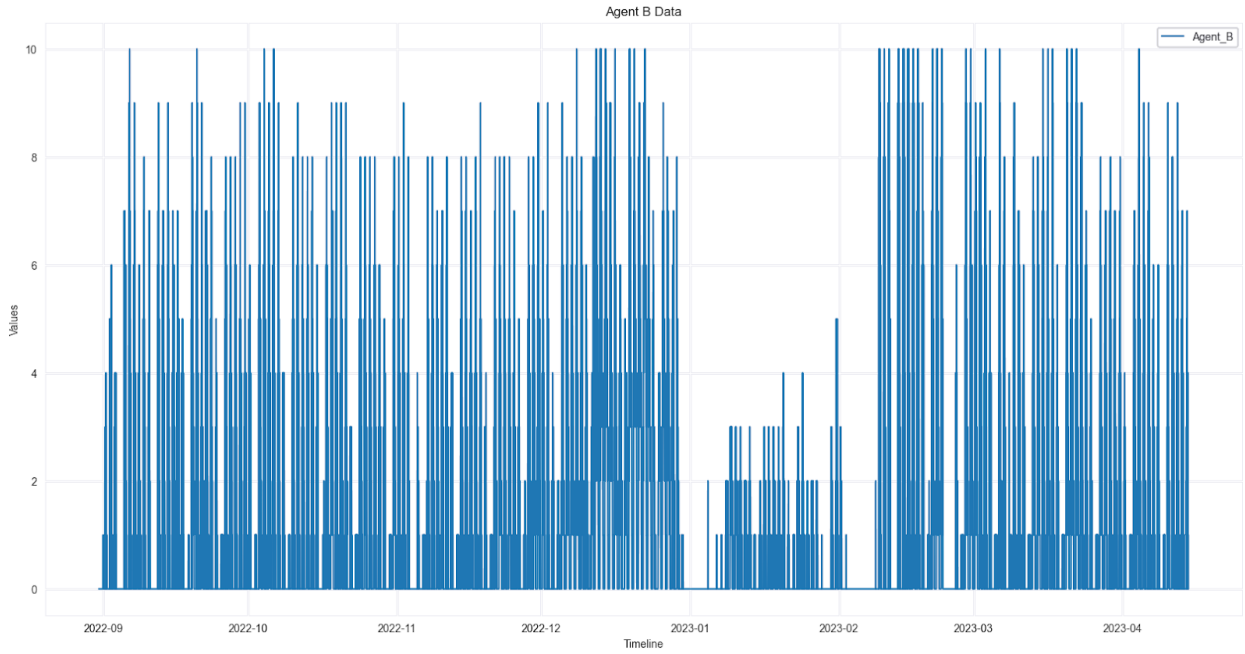


Рис. 1. Пример возвращаемого уровня риска агентом B

Агент наблюдения за взаимодействием пользователей и ресурсов (Агент B)

Этот агент следит за количеством пользователей одновременно (в пределах заданного интервала времени) обращающихся к ресурсу, возвращает повышенный риск при превышении частоты обращения заданного порога.

В агенте задан словарь, в котором хранятся ключ- имя сервиса, значение- среднее количество обращений и максимальное количество обращений за 10 минут.

Уровень риска формируется по принципу близости к порогу. Нижний порог — это среднее количество обращений, верхний порог, максимально зафиксированный за 10 минут. Если у одного из сервисов количество обращений равно или больше максимального, то риск равен 10. Иначе риск считается как процент от максимума для самого загруженного сервиса.

На рисунке 3 показан пример возвращаемого уровня риска агентом C.

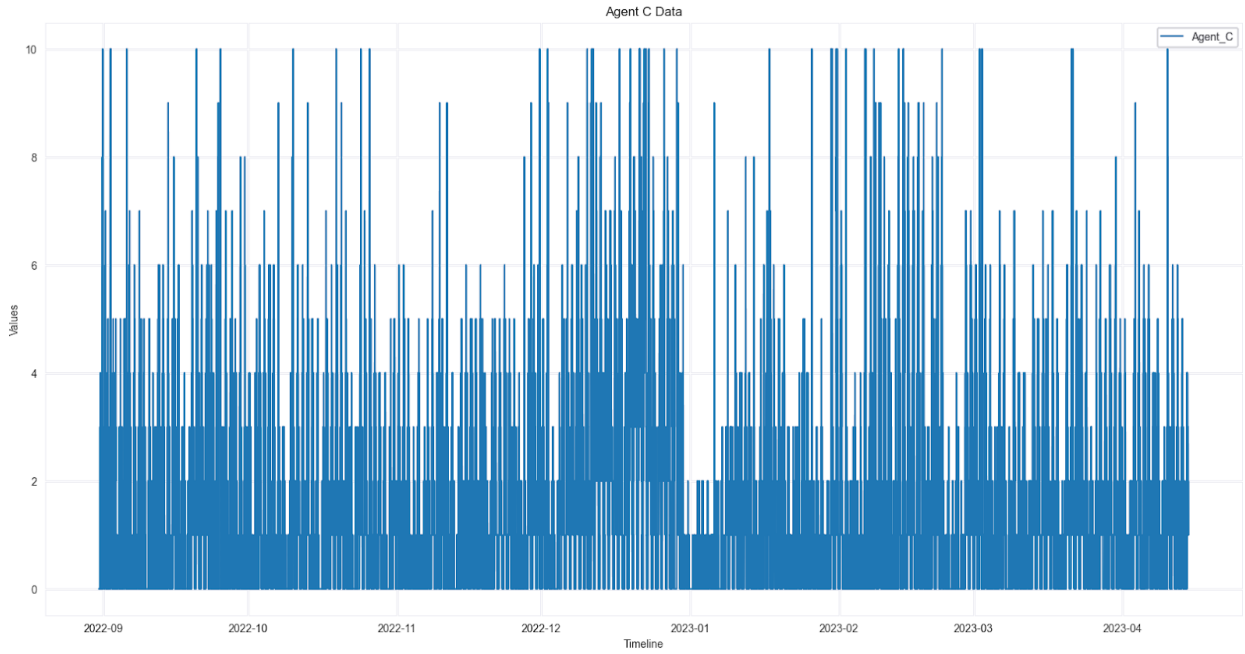


Рис. 2. Пример возвращаемого уровня риска агентом C

Согласно методике[4], показания агентов A-D из шкалы 1..10 переводятся в нечеткий вид со значениями риска «низкий», «средний», «высокий».

Данный риск ориентированный подход позволяет внедрить риск ориентированную модель управления доступом в системах высшего образования.

СПИСОК ЛИТЕРАТУРЫ

1. Ma K., Yang G., Xiang Y. RCBAC: A risk-aware content-based access control model for large-scale text data // Journal of Network and Computer Applications. 2020, Vol. 167. DOI: 10.1016/j.jnca.2020.102733

2. Fan, X., Li, C., Dong, X. A real-time network security visualization system based on incremental learning. // J. Visualization 22 (1), 2019, 215–229.

3. Chen A., Lu G., Xing H., Xie Y., Yuan S. Dynamic and semantic-aware access-control model for privacy preservation in multiple data center environments // International Journal of Distributed Sensor Networks. 2020, Vol. 16. Iss. 5. DOI: 10.1177/1550147720921778

4. Магомедов Ш.Г., Козачок А.В., Тарланов А.Т. Риск-ориентированная атрибутивная модель управления доступом для организаций высшего образования. // Правовая информатика. 2023. № 1. С. 72-82.

5. Calvo M., Beltrán M. A model for risk-based adaptive security controls // *Computers & Security*. 2022, Vol. 115, Article ID 102612. DOI: 10.1016/j.cose.2022.102612

6. Козачок А.В. Спецификация модели управления доступом к разнокатегорийным ресурсам компьютерных систем // Вопросы кибербезопасности. 2018. № 4 (28). С. 2-8. DOI: 10.21681/2311-3456-2018-4-2-8

7. Магомедов Ш.Г. Архитектура вычислительного комплекса с многоуровневым контролем доступа к веб-сервисам по общедоступным сетям // International Journal of Open Information Technologies. 2021. Т. 9. № 3. С. 36-43.

Павленко Е.Ю.
ФГАОУ ВО Санкт-Петербургский
политехнический университет Петра Великого
(ФГАОУ ВО СПбПУ),
доцент, к.т.н., доцент,
pavlenko@ibks.spbstu.ru

ИНТЕЛЛЕКТУАЛЬНЫЙ СИНТЕЗ САМООРГАНИЗУЮЩИХСЯ СИСТЕМ, УСТОЙЧИВЫХ К КОМПЬЮТЕРНЫМ АТАКАМ

Аннотация: работа посвящена вопросу автоматического синтеза структуры самоорганизующихся систем, в основе которых лежат ad hoc сети. Необходимым условием синтеза является создание такой структуры, которая обладала бы устойчивостью к различного рода кибератакам. Первостепенными шагами к достижению поставленной цели, отраженными в работе, является систематизация ad hoc сетей, определение классов угроз информационной безопасности для них и разработка математической модели, описывающей функционирование ad hoc сети. На базе разработанной с использованием теории графов модели сформулированы критерии устойчивости и выделены параметрические и структурные метрики для оценки состояния сети. Представлены результаты экспериментальных исследований, подтверждающие целесообразность использования этих метрик. Отдельно выделена метрика, связанная с числом сетевых мотивов, способных характеризовать реализацию угроз на систему и одновременно с этим являться основой для синтеза устойчивых структур системы.

Ключевые слова: самоорганизующиеся сети, киберустойчивость, синтез, искусственный интеллект, теория графов, сетевые мотивы.

Современные цифровые системы, реализующие процессы всех сфер деятельности человека, имеют сложную структуру и в значительной степени отличаются друг от друга – как за счет выполняемого функционала, так и за счет внутреннего технического устройства. Как правило, для повышения гибкости функционирования и обеспечения масштабируемости таких систем, используется динамическая сетевая инфраструктура, обладающая способностью к самоорганизации и наделяющая этим же свойством всю систему в целом.

Целью научного проекта в рамках реализации гранта является обеспечение информационной безопасности самоорганизующихся систем путем использования интеллектуального синтеза вариантов их перестроения с учетом ограничений, накладываемых в зависимости от вида сети, лежащей в их основе.

Данный доклад посвящен решению следующих задач, поставленных в рамках научного проекта:

1. Систематизации видов динамических сетей в соответствии с назначением самоорганизующихся систем, функционирующих на их основе и определяющих специфику динамики сети.
2. Определению классов угроз информационной безопасности, характерных для каждого вида сети в соответствии с назначением функционирующих на их базе самоорганизующихся систем.

3. Разработке математической модели, базирующейся на теории графов и сопоставляющей каждому виду сети ограничительную функцию для перестроения, в зависимости от назначения построенной на ее основе самоорганизующейся системы.

4. Разработке методов оценки параметрических и структурных показателей состояния каждого вида сети, основанных на теории графов.

Прежде чем перейти к систематизации, сформулируем особенности самоорганизующихся сетей (ad hoc сетей), отличающие их от классических клиент-серверных сетей [1]:

1. Отсутствие единой точки отказа за счет децентрализованной структуры сети. Данная особенность значима с точки зрения обеспечения кибербезопасности, поскольку в системе отсутствует «узкое» место, при отказе которого происходит отказ всей системы.

2. Отсутствие единого центра управления, что следует из предыдущего пункта. Значительная часть современных кибератак на сложные системы заключается не столько в ее выводе из строя, сколько в перехвате управления системой. Распределенная сетевая структура существенно усложнит реализацию подобного вектора атаки.

3. Невысокая стоимость развертывания относительно базовых сетей, поскольку для создания ad hoc сетей практически не требуется использовать дорогостоящее оборудование. Распространенный тип ad hoc сетей – сенсорные сети – состоят из миниатюрных датчиков, которые при низкой стоимости обеспечивают эффективное решение проблем зондирования и сбора данных.

4. Способность к самостоятельному установлению сетевых соединений между узлами и адаптации к изменяющимся условиям (например, к изменениям сетевой топологии).

5. Отсутствие во многих случаях четких границ сетевого периметра. В совокупности с расширением функциональных возможностей, эта особенность существенно затрудняет оценку устойчивости сети (и всей системы) к кибератакам.

Типов ad hoc сетей достаточно много, ключевыми в рамках сделанной систематизации являются [2]: MANET (mobile ad hoc network) – беспроводные децентрализованные самоорганизующиеся сети мобильных устройств, VANET (vehicular ad hoc network) – автомобильные самоорганизующиеся сети, SPAN (smartphone ad hoc network) – сети ad hoc, узлами которых являются смартфоны, mesh-сети – беспроводные ячеистые сети, WSN (wireless sensor network) – сенсорные сети, и т.д.

Все эти сети могут лечь в основу проектируемой сложной системы, и тем самым, наделить ее всеми характерными для них преимуществами и недостатками. В связи с этим, задача синтеза самоорганизующихся сетей в первую очередь определяется типом сети, лежащем в ее основе. Выделим значимые критерии функционирования самоорганизующейся сети:

1. Мобильность узла в пространстве. В случае с сетью, узлы которой способны перемещаться в пространстве, задача синтеза структуры системы, устойчивой к кибератакам, включает контроль перемещений узлов друг относительно друга.

2. Способности узла по обмену данными. В случае с одноранговой ad hoc сетью, все узлы имеют одинаковый тип и могут соединяться только друг с другом, выступая одновременно приемником и передатчиком данных. В случае с ad hoc сетью более сложного типа, у каждого узла есть набор типов узлов, с которыми он может обмениваться данными (как на отправку, так и на прием информации).

3. Функциональные возможности узла. В случае с простейшими датчиками (сенсорами), их функции ограничиваются приемом и передачей данных, в то время как узлы более сложного типа способны выполнять и другие операции над данными: агрегирование, шифрование, вычисление ряда статистик и т.п.

Все эти критерии определяют нюансы и ограничения, которые должны быть учтены при синтезе структуры самоорганизующейся системы. Рассмотрим классы угроз, характерные для самоорганизующихся систем и лежащих в их основе ad hoc сетей.

Классы угроз информационной безопасности

Угрозы информационной безопасности (киберугрозы) для ad hoc сетей разделяются на 2 больших класса:

1. Киберугрозы физической (аппаратной) среде системы, функционирующей на базе ad hoc сети. Они направлены на получение физического доступа к отдельным узлам системы и получение возможности прямого воздействия на них. К этому классу также можно отнести киберугрозы, связанные с подделкой и нарушением работоспособности устройств, входящих в состав системы.

2. Кибернетические киберугрозы. При их реализации выполняется информационное воздействие, затрагивающее инфраструктуру самой системы. Такие киберугрозы способны нарушить корректное функционирование системы и привести к ее отказу. Они реализуются путем внедрения вредоносного программного обеспечения на устройства или за счет получения несанкционированного доступа к сети передачи данных и характеризуются, как правило, фальсификацией информационных потоков.

Математическая модель функционирования ad hoc сети

Формальным способом описания процесса работы некоторой самоорганизующейся сети является математическая модель, позволяющая учесть специфику каждого типа сети и при этом закладывающая основу для построения с использованием ее терминологии различных методов обнаружения угроз безопасности и методов синтеза устойчивых структур.

Сформулируем требования к модели:

1. Модель должна позволять учитывать различные типы узлов в составе системы.

2. Модель должна обеспечивать возможность описания сетевых соединений и их характеристик (частота инициирования, время соединения и т.п.).

3. Модель должна учитывать киберфизическую природу большинства современных самоорганизующихся систем. Это означает, что значимое влияние на функционирование системы оказывают как физические параметры устройств, так и информационные характеристики, важные для обмена данными.

Сформулированным требованиям соответствует математический аппарат теории графов, при этом предлагается использовать динамические графы [3]. В силу возможности их рассмотрения как «временного ряда статических графов», имеем широкий спектр возможностей для изучения состояний системы и определения наиболее устойчивых подграфов и значимых характеристик узлов, которые должны быть учтены при синтезе.

Разработанная математическая модель кратко выглядит следующим образом. Ad hoc сеть представляется в виде ориентированного графа $G=(V,E)$, где $V=\{v_1,v_2,...,v_n\}$ – множество узлов сети, $E=\{e_1,e_2,...,e_n\}$ – множество дуг, $E\subseteq(V\times V)$. Начальное состояние сети обозначается G^0, а некоторое состояние сети в момент времени $p-$ G^p. Будем

рассматривать «снимки» графа, каждый «снимок» S^i есть совокупность предыдущего состояния графа, множества выполненных преобразований Op^i и времени t_n. Таким образом, $S^i = (G^{t_{n-1}}, Op^i, t_n)$.

Op есть множество унарных операций, выполненных при переходе от предыдущего «снимка» к текущему, $Op = (action, v_k, E_{ij})$, где $action$ – тип операции, v_k – вершины, над которыми операции совершались, E_{ij} – дуги, к которым были применены операции. $action = (VA, VD, EA, ED)$, операция добавления вершины, удаления вершины, добавления дуги и удаления дуги, соответственно. Результатом применения каждой из операций к вершине или паре вершин является 0 или 1, в зависимости от того, было выполнено преобразование или нет.

Состояние графа G^i описывается как общими структурными характеристиками графа Str, так и характеристиками отдельных вершин $Vrtx$ и дуг Ed.

Структурные характеристики Str включают связность Cn, диаметр D, число вершин $|V|$ и дуг $|E|$ в графе. К значимым характеристикам вершин графа относятся значения центральности $Cent$, заряд батареи устройства Pow, мощность сигнала Sg. Для дуг графа значимыми характеристиками являются непосредственно передаваемые данные в виде временных рядов TS, качество соединения W и статистики над данными $Stat$.

Поскольку модель учитывает различные типы ad hoc сетей, на ее базе должна быть реализована ограничительная функция перестроения, специфичная для каждого типа сети. Первым шагом к реализации такого подхода является выделение критериев устойчивости сетей к атакам.

Критерии устойчивости сети к атакам

Сформулируем критерии устойчивости к кибератакам, варьирующиеся в зависимости от типа ad hoc сети, в частности, от того, способны ли ее узлы перемещаться в пространстве или нет.

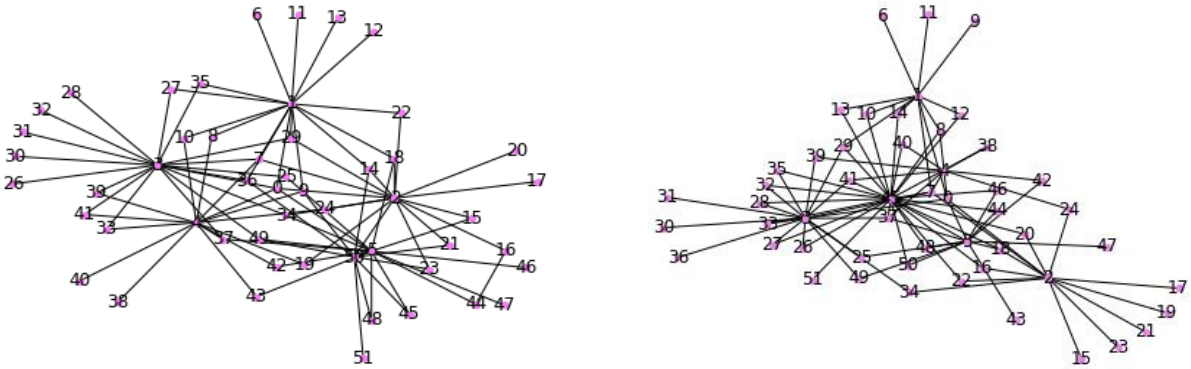
1. Для сети с узлами, способными перемещаться в пространстве, критерием устойчивости является сохранение связности сети при перемещении узлов друг относительно друга. Математически зададим этот критерий через вероятность связности группы узлов $P_c(v_0, (v_1, ..., v_n))$.

2. Для сети с узлами, положение которых в пространстве статично, можно выделить несколько метрик, как структурных – относительно всего графа, так и метрик, связанными с отдельными узлами. Среди них: метрика центральности критических вершин графа по степени, уровень заряда батареи узла сети, число компонент связности, диаметр графа.

Следует отметить, что предложенные критерии обладают научной новизной. Анализ современного состояния исследований в данной области показал, что ряд публикаций, посвященных понятию «киберустойчивость», не содержит предложений по получению ее численного показателя [4-7]. Часть публикаций сосредоточена исключительно на структурных либо параметрических показателях сети или на сетях определенного типа [8], часть предполагает привлечение экспертов

Методы оценки параметрических и структурных показателей состояния ad hoc сетей

Разработан комплекс методов, оценивающий параметрические и структурные показатели состояния сети, проведены их экспериментальные исследования. Рассмотрим пример графов, моделирующих ad hoc сеть до атаки «воронка» и при реализации данной атаки (Рис. 1).



а) б)

Рис. 1. Изменения в ad hoc сети в ходе реализации атаки «воронка»

Анализ динамики центральности вершин по степени позволил выявить резкое увеличение степени узла №2 (с 6 до 28), даже визуально видно, что на Рис. 1 б) он является центром графа. Это связано с тем, что в ходе атаки все передаваемые данных поступали на него.

Характерная для ad hoc сетей атака «испытание бессонницей» также была смоделирована для одного из узлов сети, в результате чего было значительное изменение в динамике заряда батареи: уровень заряда снизился, а попытки восстановить его нейтрализовывались атакой, чем объясняются скачки на графике (Рис. 2).

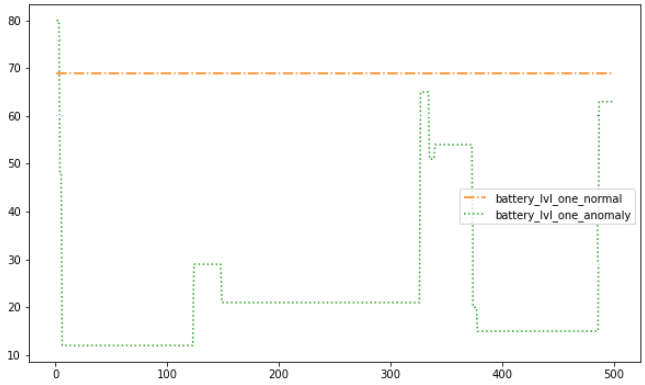
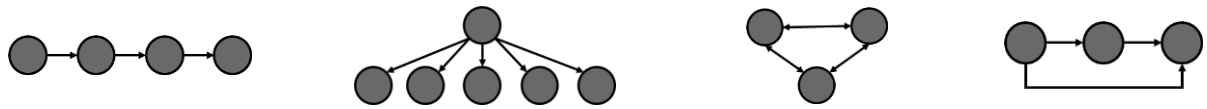


Рис. 2. Динамика значения параметра «уровень заряда батареи»

Однако в случае с крупномасштабными сетями, анализ данных от большого числа устройств представляет собой трудоемкую вычислительную задачу, а кроме того, не предоставляет информации о сети в целом.

В контексте устойчивости системы к кибератакам следует говорить о способности системы выполнять свои функции даже в условиях целенаправленных деструктивных информационных воздействий. Это говорит о необходимости задания на графовой модели некоторой целевой функции, сохранение которой обеспечит устойчивость системы.

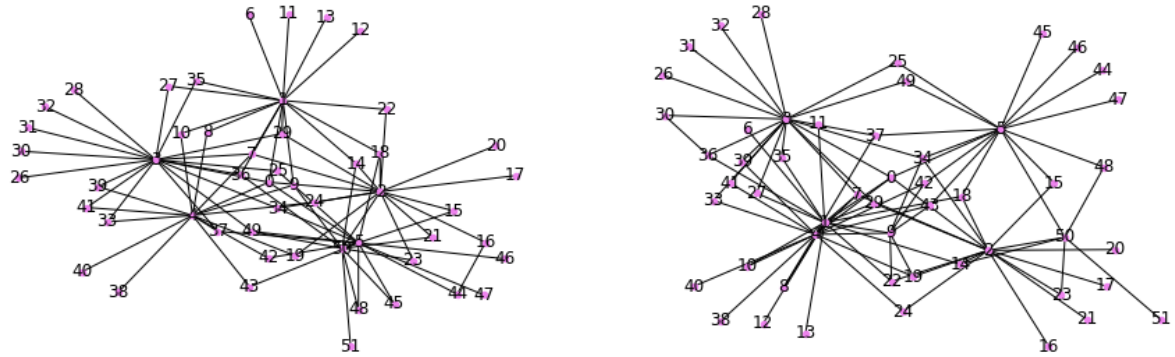
В связи с этим в качестве основного метода оценки состояния сети с узлами, положение которых в пространстве статично, предлагается использовать анализ числа сетевых мотивов, представляющих собой типовые связные подграфы на заданном числе вершин, наиболее часто встречающиеся в графе большей размерности [9]. Частота встречаемости разных сетевых мотивов представляет собой важную многомерную числовую характеристику структуры большой сети, будь то компьютерная сеть или сеть социальных взаимодействий или биологическая сеть. По результатам анализа основных типов сетевых мотивов, представленных в источнике [10], выделены типы мотивов, встречающихся в сенсорных сетях (Рис. 3). При этом, выделяются как случаи с одноранговыми сенсорными сетями, так и случаи с сетями, в которых структура имеет хотя бы некоторую иерархию.



а) б) в) г)

Рис. 3. Типы сетевых мотивов, характерные для самоорганизующихся сенсорных сетей

Для атаки Сивиллы, реализованной в рамках экспериментальных исследований, различие в графах не такое явное, как в случаях с другими атаками (Рис. 4). Однако в графе на рисунке 4 б) появились циклы, описываемые последовательностью вершин: 3-30-36-3, 2-50-23-2, что свидетельствует о нарушениях в процессе маршрутизации.



а) б)

Рис. 4. Типы сетевых мотивов, характерные для самоорганизующихся сенсорных сетей

Изначальное число сетевых мотивов, аналогичных Рис. 3 в), составляло 28, но с началом реализации атаки выросло до 52, что говорит о значимых статистических изменениях в исходном графе, моделирующем сеть.

Однако значимость сетевых мотивов не только в их возможности характеризовать различные кибератаки на сеть, но и в том, что реализуемая системой целевая функция, выраженная в терминах модели как совокупность путей на графе, является сетевым мотивом.

Подходы к синтезу устойчивых структур самоорганизующихся систем

Совокупность описанных выше исследований является основой для формирования подходов к синтезу устойчивых структур.

1. Синтез сети должен строиться на основе сетевых мотивов, характеризующих целевую функцию системы.

2. Связность графа является одной из важнейших характеристик синтезируемой системы. Число компонент связности при синтезе не должно увеличиваться, а появление изолированных вершин либо исчезновение точек сочленения графа должно устраняться за счет способности сети к самоорганизации.

3. Синтез структуры должен выполняться с учетом ограничений на информационные и физические характеристики узлов сети. Должны соблюдаться ограничения по допустимой степени вершин, уровню заряда батареи и т.п.

К направлениям дальнейших исследований относится синтез структур с учетом заданных ограничений с использованием искусственных нейронных сетей. Их использование позволит ускорить процесс генерации устойчивых структур и автоматически подбирать оптимальные варианты их построения для заданного типа ad hoc сети.

Все эти вопросы найдут свое отражение в подготавливаемой диссертации, полученные результаты будут обладать научной новизной, поскольку на данный момент нет известных научно-технических решений, обеспечивающих синтез самоорганизующихся структур с использованием нейронных сетей, с четом их типов, а также киберфизической природы порождаемых систем. Кроме того, стоит отметить решаемую в данном контексте задачу создания вариативных показателей устойчивости системы к атакам, что является мало освещенной в научной литературе темой. Предполагается получение следующих результатов по завершению проекта:

1. Комплекс методов оценки устойчивости самоорганизующейся системы к компьютерным атакам, где каждый метод адаптирован к конкретному виду сети и его специфике.

2. Новый метод синтеза самоорганизующихся систем, устойчивых к компьютерным атакам.

3. Модульная архитектура системы автоматического интеллектуального синтеза самоорганизующихся систем, устойчивых к компьютерным атакам.

СПИСОК ЛИТЕРАТУРЫ

1. Mathur, S. ParkNet: drive-by sensing of road-side parking statistics / S. Mathur, T. Jin, N. Kasturirangan, J. Chandrashekharan, W. Xue, M. Gruteser, W. Trappe // Int’l Conf. on Mobile Systems, Applications, and Services. — 2010. — Pp. 123–136.

2. Student, V.R.P. A study of ad-hoc network: A review / V.R.P. Student, R. Dhir // Int. J. — 2013. — No. 3(3) . — Pp.135-138.

3. Harary, F. Dynamic graph models / F. Harary, G. Gupta // Mathematical and Computer Modelling. — 997. — No. 25(7). — Pp.79-87.

4. Marquis, V. Toward attack-resilient state estimation and control of autonomous cyber-physical systems / R. Ho, W. Rainey, M. Kimpel, J. Ghiorzi, W. Cricchi, N. Bezzo // 2018 Systems and Information Engineering Design Symposium (SIEDS)2018. — 2018. Pp. 70-75.

5. Jeon, H. Resilient state estimation for control systems using multiple observers and median operation / H. Jeon, S. Aum, H. Shim, Y. Eun // Mathematical Problems in Engineering. — 2016.

6. Qurashi, M. An architecture for resilient intrusion detection in ad-hoc networks / M. Qurashi, C.M. Angelopoulos, V. Katos // Journal of Information Security and Applications. — 2020. — No.53. —Pp.102530.

7. Zhang, D. Measuring the resilience of mobile ad hoc networks with human walk patterns / D. Zhang, J.P. Sterbenz // 2015 7th International Workshop on Reliable Networks Design and Modeling (RNDM). — 2015. — Pp. 161-168.

8. Buinevich, M. Forecasting issues of wireless communication networks' cyber resilience for an intelligent transportation system: An overview of cyber attacks / M. Buinevich, A. Vladyko // Information. — No. 10(1). — P.27.

9. Юдин Е.Б. Расчет числа сетевых мотивов методом случайной выборки каркасов / Е.Б. Юдин, В.Н. Задорожный // ОНВ. — 2015. — №2 (140).

10. Tran, N. Current innovations and future challenges of network motif detection / N. Tran, S. Mohan, Z. Xu, C. Huang // Briefings in bioinformatics. — 2014.

Ушаков И.А.
СПбГУТ, доцент кафедры защищенных систем связи, к.т.н.
ushakov.ia@sut.ru

РАЗРАБОТКА МЕТОДОВ, МОДЕЛЕЙ И АЛГОРИТМОВ, ОСНОВАННЫХ НА МЕТОДАХ МАШИННОГО ОБУЧЕНИЯ И ОБРАБОТКИ БОЛЬШИХ ДАННЫХ, ДЛЯ ОБНАРУЖЕНИЯ ИНСАЙДЕРОВ В КОМПЬЮТЕРНЫХ СЕТЯХ

Аннотация: в докладе рассмотрены цели и задачи научного проекта в рамках реализации гранта, включая взаимосвязь исследования с диссертационной работой, приведен анализ современного состояния исследований в области обнаружения инсайдеров, а также предлагаемые методы и подходы к решению поставленных задач, представлены новизна исследования и ожидаемые по окончании проекта научные результаты.

Ключевые слова: информационная безопасность, большие данные, машинное обучение, инсайдеры.

Постановка задачи, степень разработанности темы

Проблема обеспечения защиты информации, циркулирующей в компьютерной сети, становится исключительно важной, требующей решения ряда специальных задач. В частности, с февраля 2022 года Россия столкнулась с беспрецедентными по своему масштабу кибератаками. Большое количество из этих атак были осуществлены внутренними сотрудниками (инсайдерами), которые находились на предприятиях, в том числе относящихся к объектам критической информационной инфраструктуры [1].

Сложность обнаружения инсайдеров в компьютерных сетях (КС) напрямую следует из развития информационных технологий, связанных с постоянным увеличением параметров сетевого трафика: его количества; скорости; многообразия обрабатываемых данных (голос, видео, пользовательские данные); количества сессий, не связанных со своими целями и задачами. Компании и организации постоянно генерируют огромные массивы данных, которые требуют эффективного управления. Все это приводит к существенному усложнению анализаторов трафика, при этом существующие системы как правило не способны справляться с такими большими объемами данных и сложностью, в то время как инсайдеры скрывают свои действия в общем потоке действий легитимных пользователей. Кроме того, современные инсайдерские атаки являются комплексными и используют множество механизмов реализации и множество векторов атак для получения несанкционированного доступа и компрометации информационных объектов во внутренней КС [2, 3, 4, 5].

Проблеме существования инсайдеров в КС было посвящено большое количество работ как отечественных ученых (П.Д. Зегжды, И.В. Котенко, А.В. Лукацкого, А.А. Молдовяна, В.Ю. Осипова, И.Б. Саенко и др.), также и зарубежных (Khan, A.Y., C. Cheh, M. Collins, Mohammed Nasser Al-Mhiqani, Y. Shuang-Hua, L. Liu и др.). Однако, несмотря на сделанный учеными существенный задел, проблема обнаружения инсайдеров в КС не может считаться разрешенной и требует проведения новых исследований, что и будет осуществлено в исследовательской работе.

В настоящее время большое количество исследований посвящено вопросам обнаружения аномалий с помощью методов машинного обучения и обработки больших данных [6, 7, 8, 9].

Целью разрабатываемого проекта является разработка и исследование методов, моделей и алгоритмов, основанных на методах машинного обучения и обработки больших данных, для обнаружения инсайдеров в компьютерных сетях.

Задачи исследования:

1. Провести анализ предметной области.
2. Разработать метод обнаружения инсайдеров в компьютерных сетях, в том числе используя методы сетевой стеганографии.
3. Разработать алгоритм обнаружения инсайдеров в компьютерных сетях, основанный на методах машинного обучения и обработки больших данных.
4. Разработать модель инсайдера.
5. Разработать модель представления больших данных об инсайдерских атаках.
6. Разработать архитектуру и реализовать программный комплекс системы обнаружения инсайдеров в КС.
7. Провести эксперименты в рамках исследования.

При решении поставленных задач используются методы системного анализа, теории множеств, методов машинного обучения, больших данных, управления рисками, информационной безопасности, современные методы программирования.

Модель представления больших об инсайдерских атаках

В настоящее время атаки инсайдеров сложные, они состоят из множества этапов и векторов атак для получения нелегитимного доступа, а также компрометации объектов во внутренней КС. Любой пользователь КС может быть инсайдером, а значит в системах защиты от атак необходимо, чтобы выполнялись процедуры по анализу и контролю всех действий пользователей (профилирование поведения пользователей).

В исследованиях, существующих на данный момент, такие процедуры получили название поведенческий анализ пользователей – User Behavior Analytics (UBA), а также поведенческий анализ пользователей и сущностей – User and Entity Behavior Analytics (UEBA) [10, 11].

UBA и UEBA формально являются одним и тем же классом систем. Но UBA-системы применяют информацию, в которой содержатся только данные об активности пользователей, а значит, они основываются на пользователях и их ролях (правах доступа), в то время как UEBA-системы, кроме информации об активности пользователей, еще используют информацию об их системном окружении (трафике, базах данных, хостах и программном обеспечении). Благодаря этому системы UEBA профилируют не только пользователей, но и состояние программного и аппаратного обеспечения в целом.

Для возможности реализовать UBA и UEBA необходимо наличие системы управления базами данных (СУБД), которая сможет легко масштабироваться и будет обладать высокой скоростью обработки запросов. В настоящее время для этой цели используется СУБД NoSQL. Решения на основе NoSQL дают масштабируемый и гибкий способ решения задач, которые ранее управлялись реляционными базами данных [12, 13, 14].

В рамках диссертационного исследования предполагается использовать СУБД NoSQL OrintDB. Она предлагает объединенные возможности документо-ориентированной и графо-ориентированной баз данных. Гибридный формат позволяет пользоваться полными

графическими возможностями в сочетании с функциями, которые обычно присущи только базам данных документов.

Чтобы построить модель представления больших об инсайдерских атаках в формате NoSQL надо собрать максимальное количество данных из системы. Благодаря этим данным формируются профили поведения пользователей, а потом по совокупности этих профилей становится возможным определить, поведение каких пользователей будет отличаться от нормального поведения. Также в дальнейшем на основе этой информации будет возможно выявить возможных инсайдеров и какие несанкционированные действия они могут предпринять. Данная модель будет учитывать поведение пользователей для дальнейшей возможности использования модели при обнаружении внутренних нарушителей информационной безопасности.

Для построения модели представления больших данных об инсайдерских атаках в целях обнаружения инсайдеров в компьютерной сети необходимо рассмотреть источники собираемых данных. Источниками данных являются все клиентские устройства в компьютерной сети, их конфигурации, данные об аутентификации пользователей (успешной или не успешной), сведения об операционных системах и приложениях, которые используют пользователи, сведения о потоках данных в сети, сведения о соответствии хостов и конечных точек, метрики о событиях информационной безопасности (получаемые от SIEM-систем).

Источники сбора данных, описывающих поведение пользователя в компьютерной сети представлены на рисунке 1.

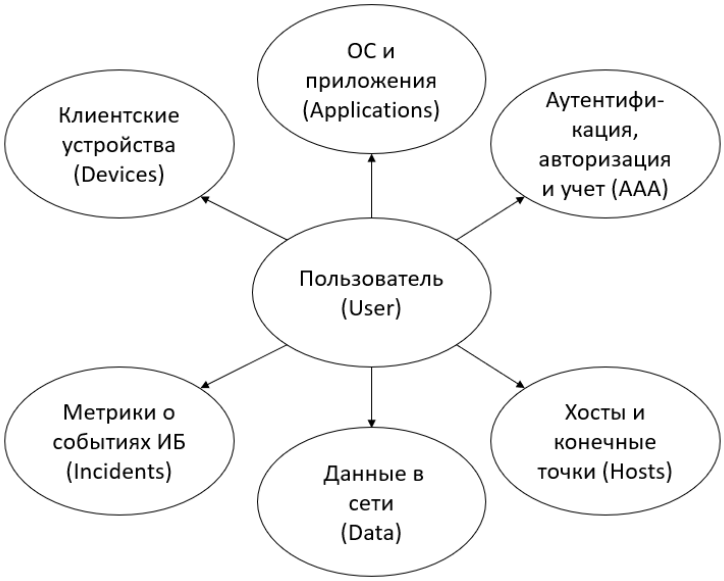


Рис. 1. Источники сбора данных

Формальный вид модели имеет следующий вид:

$$M = \langle E, I \rangle \tag{1.1}$$

где E - элементы, которые представляют атрибуты поведения пользователя, а I - модель инсайдера и критерии, позволяющие отнести пользователя к категории инсайдера.

Примеры критериев, позволяющих отнести пользователя к категории инсайдера:

1. Созданное за малое время большое количество обращений к компьютерам.
2. Создание в минуту большого количества нетиповых запросов (более тысячи запросов в минуту).

3. Аномальное завершение сессии.
4. Наличие узлов, которые не являются членами домена.
5. Отсутствие доменного имени.
6. Посещение запрещенных или опасных сайтов.
7. Подмена DNS-сервера
8. Появление нестандартных подключений.
9. Загрузка данных в нерабочее время.
10. Попытки подобрать пароль.

Зачастую по одному критерию невозможно сделать однозначный вывод о принадлежности пользователя к категории инсайдеров. В этом случае используются комбинации критериев.

Архитектура и программный комплекс системы обнаружения инсайдеров в КС

Разрабатываемая архитектура системы обнаружения инсайдеров включает в себя три уровня обработки информации: (1) уровень сети и обработки данных (метрики информационной безопасности, в том числе полученные от SIEM-систем); (2) уровень обработки информации, включая хранилище данных; (3) уровень аналитической обработки информации и событий безопасности (включая компонент визуализации).

Научная новизна

Модель представления больших данных об инсайдерских атаках отличается от существующих возможностью обеспечения хранения и анализа признаков пользователей, приложений, устройств и сервисов, а также возможностью учета динамики изменения этих признаков.

Алгоритм обнаружения инсайдеров в компьютерных сетях, основанный на методах машинного обучения и обработки больших данных, отличается от существующих использованием системного подхода к обнаружению инсайдеров.

Метод обнаружения инсайдеров в компьютерных сетях отличается от существующих использованием предложенной модели представления больших данных об инсайдерских атаках и алгоритме обнаружения инсайдеров в компьютерных сетях.

Заключение

В диссертационном исследовании предлагается разработать и исследовать методы, модели и алгоритмы, основанные на методах машинного обучения и обработки больших данных для обнаружения инсайдеров в компьютерных сетях. Результаты исследования предлагается использовать в учебном процессе на кафедре защищенных систем связи СПбГУТ при реализации направлений подготовки 10.03.01 «Информационная безопасность», дисциплина «Методы оценки безопасности компьютерных систем»; 10.04.01 «Информационная безопасность», дисциплины: «Цифровая криминалистика», «Защита облачных вычислений и телекоммуникаций», «Тестирование на проникновение и этичный хакинг». А также при реализации специальностей: 10.05.02 «Информационная безопасность телекоммуникационных систем», дисциплины: «Цифровая криминалистика», «Межсетевое экранирование и системы предотвращения вторжений», «Тестирование на проникновение и этичный хакинг»; 10.05.07 «Противодействие техническим разведкам», дисциплины «Цифровая криминалистика», «Межсетевое экранирование и системы предотвращения вторжений», «Тестирование на проникновение и этичный хакинг».

Результаты исследования будут опубликованы в журналах из Перечня ВАК Минобрнауки России.

В ходе реализации проекта будут зарегистрированы программы для ЭВМ, получены акты внедрения представленных в диссертации результатов.

Данное исследование выполнено при финансовой поддержке Минцифры России (грант ИБ) в рамках научного проекта, соглашение №. № 40469-05/23-Д.

СПИСОК ЛИТЕРАТУРЫ

1. Быстров, И. С. анализ методик обнаружения киберинсайдеров, апробированных на наборе данных CERT / И. С. Быстров, И. В. Котенко // Информатизация и связь. – 2022. – № 1. – С. 7-12. – DOI 10.34219/2078-8320-2022-13-1-7-12.
2. Khan, A.Y. Malicious Insider Attack Detection in IoTs Using Data Analytics. / Khan, A.Y.; Latif, R.; Latif, S.; Tahir, S.; Batool, G.; Saba, T. // IEEE Access 2020, 8, 11743–11753. doi:10.1109/ACCESS.2019.2959047.
3. Liu, L. Insider Threat Identification Using the Simultaneous Neural Learning of Multi-Source Logs. / Liu, L., Chen, C.; Zhang, J.; De Vel, O.; Xiang, Y. // IEEE Access 2019, 7, 183162–183176. doi:10.1109/ACCESS.2019.2957055.
4. Mohammed Nasser Al-Mhiqani. A new intelligent multilayer framework for insider threat detection / Mohammed Nasser Al-Mhiqani, Rabiah Ahmad, Z. Zainal Abidin, Karrar Hameed Abdulkareem, Mazin Abed Mohammed, Deepak Gupta, K. Shankar // Computers & Electrical Engineering, Volume 97, 2022, 107597, ISSN 0045-7906, https://doi.org/10.1016/j.compeleceng.2021.107597.
5. Ушаков, И.А. Обнаружение инсайдеров в компьютерных сетях на основе комбинирования экспертных правил, методов машинного обучения и обработки больших данных : специальность 05.13.19 "Методы и системы защиты информации, информационная безопасность" : диссертация на соискание ученой степени кандидата технических наук / Ушаков Игорь Александрович. – Санкт-Петербург, 2020. – 215 с.
6. Котенко, И.В. Методика обнаружения аномалий и кибератак на основе интеграции методов фрактального анализа и машинного обучения / И. В. Котенко, И. Б. Саенко, О. С. Лаута, А. М. Крибель // Информатика и автоматизация. – 2022. – Т. 21, № 6. – С. 1328-1358. – DOI 10.15622/ia.21.6.9.
7. Beena, A.L. Information Security Insider Threats in Organizations and Mitigation Techniques. / A.L. Beena, S. Kabir Humayoon // In proceedings of the 2019 International Conference on Recent Advances in Energy-efficient Computing and Communication (ICRAECC). Nagercoil, India. – 2019. pp. 1-4.
8. Tanzila Saba, Amjad Rehman, Tariq Sadad, Hoshang Kolivand, Saeed Ali Bahaj, Anomaly-based intrusion detection system for IoT networks through deep learning model, Computers and Electrical Engineering, Volume 99, 2022, 107810, ISSN 0045-7906, https://doi.org/10.1016/j.compeleceng.2022.107810.
9. Лаута, О. С. Подход к работе системы защиты сети передачи данных от компьютерных атак на основе гибридной нейронной сети / О. С. Лаута, В. Х. Федоров, Е. Г. Баленко, Д.Ю. Васюков, Д.А. Иванов // Инженерный вестник Дона. – 2023. – № 1(97). – С. 237-250.
10. Kotenko, I. An approach for stego-insider detection based on a hybrid NoSQL database / I. Kotenko, K. Izrailov, A. Krasov, I. Ushakov // Journal of Sensor and Actuator Networks. – 2021. – Vol. 10, No. 2.

11. Котенко, И.В. Выявление инсайдеров в корпоративной сети: подход на базе UBA и UEBA / И. А. Ушаков, Д. В. Пелевин, А.И. Преображенский, А.Ю. Овраменко // Защита информации. Инсайд. – 2019. – № 5(89). – С. 26-35.
12. Котенко, И.В. Методы интеллектуального анализа системных событий для обнаружения многошаговых кибератак: использование баз знаний / И. В. Котенко, Д. А. Левшун // Искусственный интеллект и принятие решений. – 2023. – № 2. – С. 3-14. – DOI 10.14357/20718594230201.
13. Лаута, О.С. Модель воздействия компьютерных атак на информационно-телекоммуникационную сеть / О. С. Лаута, Д. А. Иванов, Э. В. Аведян // I-methods. – 2022. – Т. 14, № 3.
14. Ададуров, С. Е. Подход к обеспечению устойчивости и оперативности системы хранения больших данных / С. Е. Ададуров, И. В. Котенко, И. Б. Саенко // Автоматика, связь, информатика. – 2022. – № 12. – С. 19-21. – DOI 10.3464

РАЗДЕЛ 3. НАУЧНЫЕ ДОКЛАДЫ ГРАНТОПОЛУЧАТЕЛЕЙ 2022 ГОДА – СОИСКАТЕЛЕЙ УЧЁНОЙ СТЕПЕНИ КАНДИДАТА НАУК

Аверьянов В.С.
СибГУ им.ак. М.Ф. Решетнева, м.н.с.,
averyanov124@mail.ru

ФИЗИЧЕСКИЕ СОСТОЯНИЯ СВЕТОВЫХ ЧАСТИЦ В ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ С КВАНТОВЫМ РАСПРЕДЕЛЕНИЕМ КЛЮЧЕЙ БЕЗОПАСНОСТИ

Аннотация: В статье рассмотрен ряд вопросов возникающих при создании квантовых волоконно-оптических систем связи с КРК (квантовое распределение ключей). Проведено исследование процессов приготовления собственных – «чистых» состояний фотонов в квантово-оптических системах для экспериментов по генерации информационных кубит для четырех трансформируемых состояний света: фоковского, глауберово, естественно-теплового и сжатого. Особое внимание уделено вакуумным приближенным к классическому состоянию электромагнитного поля, так и фотонным состояниям. Отмечены такие понятия, как: амплитуда, фаза и число частиц, используемых экспериментаторами для описания состояний квантованного поля в системах с КРК.

Ключевые слова: амплитуда, безопасность, вектор, реликтовые частицы, системы КРК, фотон.

Известные на сегодня протоколы квантовой передачи данных [1] содержат в своих алгоритмах процедуру проведения измерений со стороны легитимных пользователей и сторонних наблюдателей. Под измерениями принято считать вычисления произвольного математического оператора гамильтониана $\widehat{H}$, где сам факт поиска трансформирует состояния системы, присваивая ей статус «наблюдаемой».

$$\widehat{H}_{|}\psi\rangle = |\psi\rangle\langle\psi| \quad (1)$$

$$E = mc^2mc^2 = (mc2)^2 = E^2 - (cp)^2 \quad (2)$$

Прежде всего, эрмитов оператор согласно выражению (1) линейно зависим от вектора состояния частицы $|\psi\rangle$ в её гильбертово-проективном пространстве, а также от масса-энергетических показателей согласно (2) [2, 3]. Показатели точности измерений при этом выражены через неопределенность фаз поляризации частиц $\Delta\varphi$ по отношению к общему числу измерений частиц Δx. Тогда, поиск $\widehat{H}$ и начальное состояние частицы $|\psi\rangle$ отличаются энергетическим импульсом от трансформируемого состояния $|\psi_n\rangle$ вперед по временной оси. Такое состояние является невырожденным и может быть записано как:

$$\widehat{H}_{\varphi} = \frac{|\psi\rangle\Delta\varphi}{\Delta x} \quad (3)$$

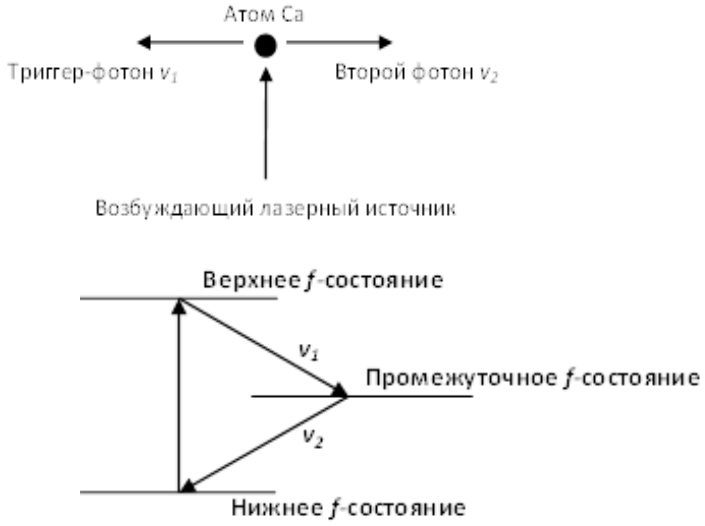
Исходя из (3) сторонний наблюдатель, а также участники информационного обмена в процессе измерений $\widehat{H}_{\varphi}$ получат лишь одно значение 0 или 1, если результат равен 1, то система перейдет в свое первоначальное состояние $|\psi\rangle$, в случае нулевого значения $|\psi_n\rangle$. В таких случаях наблюдатель проводит процесс отбора интересующих частиц для последующих измерений в произвольном состоянии системы, иначе говоря приготавливает требуемые состояния.

На практике, в экспериментальных установках применяют различные методы приготовления вектора состояний частицы $|\psi\rangle$. Одним из ключевых, оказывающих влияние на статистические свойства является неопределенность фаз поляризации по отношению к общему числу частиц [4]. Так, например, состояния Фока - это точно определенное число фотонов и фазы поляризации, когерентные состояния – случайно распределенные реликтовые частицы с неопределенностями фаз и числа излученных фотонов.

Под состояниями Фока $|n\rangle$ принято считать собственные состояния числа фотонов $\hat{n}$:

$$\hat{n}|n\rangle = n|n\rangle, n = 0, 1, 2\ ,3, \ldots \quad (4)$$

При этом в квантовомеханической теории принято, что каждая наблюдаемая величина соответствует линейном оператору гамильтониану $\widehat{H}$, а волновые функции согласно корпускулярно-волнового дуализма являются собственными состояниями этого оператора. Тогда, вектор состояния частицы $|\psi\rangle$ находящийся в состояниях Фока $|n\rangle$ сопоставим с общим числом излученных фотонов, а флуктуация квантовых частиц в световом потоке отсутствует, т.к. $\Delta x=0$, при этом статистический параметр Манделя ξ=-1 [5, 6]. В экспериментах, по молекулярно-лучевой технологии одной из приоритетных задач является создание сфокусированного потока атомов с помощью двухфотонного лазерного источника излучения, а также их перевод в произвольное возбужденное состояние. При излучении частицы светового потока смешиваются с фоновым освещением и фотонами лазера, задача исследователя заключается в том, чтобы определить собственное однофотонное состояние излучения. Первый успешный эксперимент по антисовпадению [2,3], где источник одиночных фотонов облучал атом калия с переводом его в некоторое *f*-состояние представлен на рисунке 1 (а, б) и 2.



(а) **(б)**

Рис. 1. Возбуждение атома Ca и переход в f-состояние (а). Переход на новый уровень и поведение при релаксации (б).

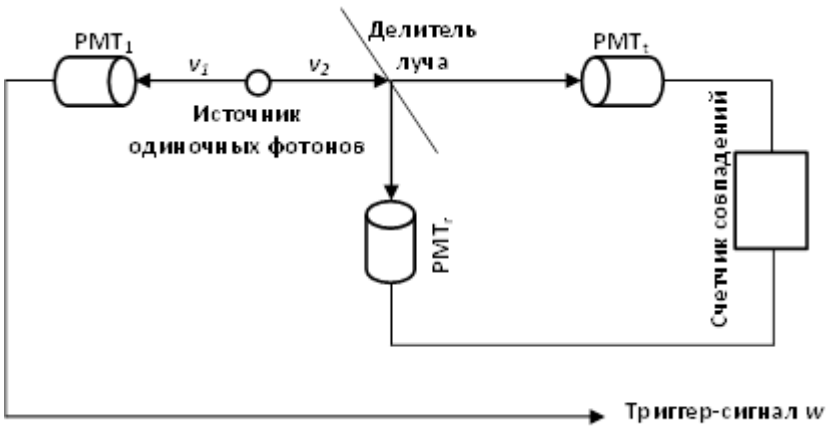


Рис. 2. Схема установки по антисовпадению Аспе с коллегами. Эксперимент по приготовлению однофотонного фоковского состояния частицы [4]

Способ приготовления состояний Фока представленный на рисунке 2 является довольно сложным в технической реализации, но предоставляет прекрасную возможность понять, что такое фотоны, раскрыть их основные свойства как реликтовых частиц, которые как нельзя кстати подходят под требования квантовых протоколов передачи данных на базе КРК.

Глауберовы или когерентные состояния $|\psi\rangle$ названы в честь американского физика R. J. Glaubera. Они представляют собой классические состояния светового поля, в котором волновой пакет начального состояния системы смещен от высококачественного лазерного источника, а излученные волны не расплываются в процессе трансформации системы. При этом статистический параметр Манделя $\xi \geq 0$ [6]. Когерентные состояния рассматриваются как собственные состояния оператора уничтожения $\hat{n}$:

$$\hat{n}|n\rangle = n|n\rangle \tag{5}$$

Идеально когерентные состояния обладают определенными амплитудами $|n|$ и фазами *arg n* по отношению к собственным состояниям $|n\rangle$. При этом волновые пакеты для световых полей в статистических смесях когерентных состояний являются классическими, а невозможность их представления в виде ансамбля фотонов в когерентных состояниях [5, 7] является их неклассическим представлением. Эксперименты по генерации неклассических световых полей являются важным достижением в современной квантовой оптике.

К свойствам когерентных состояний следует отнести, что состояния вакуума есть собственные состояния $|n\rangle$, если $|n| = 0$. При этом поиск средней энергии вакуума сводится к поиску не эрмитова оператора $\hat{H}$, где его собственные значения комплексны и соответствуют амплитуде $|n|$ волны в её классическом оптическом представлении:

$$\langle \hat{H} \rangle = \langle n \left| \hat{n}n^{+} + \frac{1}{2} \right| n \rangle = |n|^2 + \frac{1}{2} \tag{6}$$

Из выражения (6) следует, что при волноподобных состояниях смещение фазы на угол φ сдвигает фазу *arg n* амплитуды когерентного состояния. В том числе, глауберово состояние возможно разложить по амплитуде $|n\rangle$ собственного состояния в фоковском базисе:

$$|n\rangle = \sum_{a=0}^{\infty} exp(-\frac{1}{2}|n|^2) \frac{n^a}{\sqrt{a!}} |a\rangle \tag{7}$$

Уравнение (7) указывает, что когерентное состояние волнового пакета имеет пуассоновскую статистику для $0 \leq a \leq \infty$, а вероятность нахождения *n* фотонов в их когерентном состоянии напрямую зависит от амплитуды вероятности вектора $|n\rangle$. Тогда:

$$P_{|n\rangle} = \exp(-|a|^2)\frac{\langle a\rangle^{2n}}{n!} \quad (8)$$

Вероятность нахождения фотонов в их когерентном состоянии согласно (8) позволяет сделать вывод о том, что дисперсия при когерентном излучении и среднеквадратичном разбросе $|n|$ волны не зависит от её начального среднего значения как в (6).

К тепловому излучению относятся природно-естественные проявления солнечного света или света от люминесцентных ламп и ламп накаливания. Соответственно, тепловое излучение света – это произвольное состояние электромагнитного поля [8], в котором происходит трансформация энергии теплового движения реликтовых частиц в электромагнитное излучение. При этом свет не взаимодействует сам с собой, а его тепловой характер вызван энергетическим возбуждением элементарных частиц, как результат при контакте с окружающими объектами излучение термолизуется и происходит обмен фотонами, а излученная тепловая энергия флуктуирует по отношению к последним. Термолизованный свет может быть выражен через фоковские состояния частиц с произвольным числом фотонов n и оператором плотности p:

$$\hat{p} = \sum_{n=0}^{\infty}(1 - exp^{-\beta})\big|n\rangle\langle n|exp^{-n\beta} \quad (9)$$

$$\beta = \frac{\hbar\omega}{k_B T} \quad (10)$$

Выражение (10) представляет собой отношение энергии к температуре, где kB – постоянная Больцмана [7], тогда при ранее известной T среднее число фотонов в одной световой моде равно:

$$\langle n\rangle = \frac{1}{exp^{\beta}-1} \quad (11)$$

Согласно (9, 10, 11) путем трансформации теплового оператора плотности через гауссово распределение глауберовых состояний, можно найти необходимое физическое обоснование любого из тепловых свойств квантовых элементарных частиц. Трансформируемые тепловые состояния фотонов активно применяются в системах КРК с ионными ловушками.

В фоковских или вакуумных состояниях фотонов в электромагнитном поле частицы обладают квадратурными амплитудами, а также квантовмеханическими эффектами [9], распределение вероятности таких макрообъектов согласно принципов квантовой механики находится в прямой зависимости от числа излученных и хаотично взаимодействующих частиц в пространстве. Глауберовы состояния отличаются тем, что обладают статистической неопределенностью своих квадратур. Здесь возникает вопрос, а что есть состояния с минимальной неопределенностью? Знаменитое доказательство В. Паули опубликованное в его статье в «Handbuch der Physik» и формула минимальной неопределенности:

$$\Delta x \Delta p_x \geq h \quad (12)$$

$$\Delta q \Delta p \geq \frac{1}{2} \quad (13)$$

Выражение (12) является соотношением неопределеннойстей Гейзенберга, где координата Δx соответствует пространственной проекции импульса Δp_x, результат такого произведения не может быть меньше величины порядка h, где $h \geq \frac{1}{2}$. В. Паули предложил свою - локальную версию (13) принципа Гейзенберга [10, 11], в которой пространственное смещение состояния частицы с минимальной неопределённостью, как и для когерентных состояний может быть задано гауссовыми волновыми функциями, при которых дисперсии Δq и Δp не обязаны быть равными (12), а статистическая неопределенность квадратурной

амплитуды q может быть сжата как большую, так и в меньшую сторону. При этом произведение дисперсии всегда больше или равно $\frac{1}{2}$, что соответствует фоковскому состоянию частицы.

Для детального изучения сжатого состояния света, необходимо ввести параметр Манделя ξ представленного в виде некоторого действительного числа [12] и характеризующего отклонение Δq и Δp от априорных значений вакуумных состояний, параметр ξ в данном случае является критерием сжатия света в вакууме:

$$\Delta^2(qp) = \frac{1}{2}\left(exp^{-2\xi} + exp^{+2\xi}\right) \quad (14)$$

$$\Delta^2 q = \frac{1}{2}exp^{-2\xi}, \Delta^2 p = \frac{1}{2}exp^{+2\xi} \quad (15)$$

Исходя из выражений (14, 15) при $\xi=0$ получим несжатое состояние света, а произведение дисперсий Δq и Δp будет соответствовать минимальному значению неопределенности [13] как и в (13). Координатная волновая функция $\psi(q)$ квадратурной амплитуды q, а также импульсная $\psi(p)$ для сжатого состояния в соответствии с фоковским состоянием равна:

$$\varphi(q) = \frac{1}{2}\psi(exp^{\xi}q) \quad (16)$$

$$\hat{\varphi}(p) = -\frac{1}{2}\hat{\psi}(exp^{-\xi}p) \quad (17)$$

Выражение (16, 17) отражает факт того, что волновые функции $\varphi(q), \hat{\varphi}(p)$ обладают свойствами пространственного растяжения и сжатия, а также обратимы друг относительно друга. Согласно доказательства В. Паули, состояния с минимальной неопределённостью [14] для волновых функций выражены смещенными гауссовыми состояниями вакуума:

$$\psi(\Delta q \Delta p) = \pi^{-1/4}exp^{\xi/2}\left[-exp^{2\xi}\frac{(q-q_0)}{2} + exp^{2\xi}\frac{(p-p_0)}{2} + ipq - \frac{iq_0p_0}{2}\right] \quad (18)$$

Согласно (18) возможно получить не только математическое представление сжатого состояния света в его пространственном представлении, но и физический процесс для экспериментальных установок по генерации сжатых состояний реликтовых частиц.

Заключение. Вопросы, изложенные в данном материале, безусловно не исчерпывают всего многообразия задач, решаемых в квантовой теории информации, оптике и системах связи [15, 16]. Однако, приведенный материал служит иллюстрацией к вводной части по созданию экспериментальных установок генерации ключевой последовательности и новых сверхзащищенных волоконно-оптических линий связи наземного базирования.

СПИСОК ЛИТЕРАТУРЫ

1. Аверьянов В.С., Карцан И.Н. Гибридный квантово-классический подход для защиты наземных линий связи // Южно-Сибирский научный вестник. 2019. Т. 4 (28). С. 264-269.
2. Koczyk P., Wiewior P., Radzewicz C. «Фотон определяет статистику – эксперимент для студентов». Amer. J. Phys., vol. 64, pp. 240-245 (1996).
3. Galvez E.J., Holbrow C.H., Pysher M.J., Martin J.W., Coutremanche N., Heilig L. и Spencer J. «Интерференция коррелированных фотонов: пять экспериментов для студентов демонстрирующих квантовые принципы». Amer. J. Phys., vol. 73 pp. 127-140 (2005).
4. Дж. Гринштейн, А. Зайонц. Квантовый вызов. – М: Интеллект. 2008 г. – 400 с.
5. Ландсберг Г.С. Оптика / Г.С. Ландсберг. – 6-е издани.-М: Физматлит, 2003. – 848

6. Ландау Л. Д., Лифшиц Е. М. Квантовая механика. Нерелятивистская теория. Изд. 2-е. М.: Физматлит. 1963. - 702 с.

7. Новосадов Б. К. Аналитическая механика атома. М.: Нобель Пресс. 2014. - 322 с.

8. D. V. Strekalov and G. Leuchs, in Quantum Photonics: Pioneering Advances and Emerging Applications, ed. by R. Boyd, S. Lukishova, and V. Zadkov, Springer Series in Optical Sciences, Vol. 217, p. 51 (2019).

9. Zurek W. H. et al. Quantum Decoherence. Poincar e Seminar 2005 / Eds.: B. Duplantier, J.-M. Raimond, V. Rivasseau. Basel: Birkhéauser Verlag, 2007. X, 192 p.

10. Giacomo A. D. et al. Field Correlators in QCD. Theory and Applications // Phys. Rep. 2002. V. 372, No. 4. P. 319Ä368.

11. Haake F. Quantum Signatures of Chaos. Berlin: Springer-Verlag, 1991. 242 p.

12. Орлов А. И. Непараметрические критерии согласия Колмогорова, Смирнова, омега-квадрат и ошибки при их применении //Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета. – 2014. – №. 97. – С. 31-45.

13. Старунов В. С., Фабелинский И. Л. Вынужденное рассеяние Мандельштама—Бриллюэна и вынужденное энтропийное (температурное) рассеяние света //Успехи физических наук. – 1969. – Т. 98. – №. 7. – С. 441-491.

14. Каплан И. Г. Принцип запрета Паули и проблемы его теоретического обоснования //Известия высших учебных заведений. Физика. – 2020. – Т. 63. – №. 8. – С. 9-23.

15. Аверьянов В. С. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ. – Сибирский государственный университет телекоммуникаций и информатики КОНФЕРЕНЦИЯ: ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ Новосибирск, 14–18 ноября 2022 года Организаторы: Сибирский государственный университет телекоммуникаций и информатики.

16. Разгуляев К. А. и др. Об одном способе хранения и управления ключами в системах квантовых коммуникаций //Вестник современных цифровых технологий. – 2020. – №. 2. – С. 14-20.

Банокин П.И.
Томский государственный университет систем управления и радиоэлектроники, кафедра КИБЭВС, преподаватель
pavel805@gmail.com

ИДЕНТИФИКАЦИЯ ВНУТРЕННИХ УТЕЧЕК ДАННЫХ НА ОСНОВЕ АНАЛИЗА ПОВЕДЕНИЯ ПОЛЬЗОВАТЕЛЕЙ

Аннотация: Рассмотрены алгоритмы поиска посторонних значений в массиве поведенческих данных. Предложен алгоритм идентификации утечек данных на основе анализа текстовых документов и графа переходов между состояниями клиента корпоративной информационной системы. Выполнена реализация алгоритма и проведена серия экспериментов.

Ключевые слова: утечки данных, поведение пользователей.

В 2023 году отмечается значительное увеличение количества случаев утечек данных по сравнению с прошлым годом [1]. Данные корпоративных информационных систем (КИС), в том числе систем управления взаимоотношениями с клиентами (CRM), являются одной из главных целей злоумышленников. Среди случаев утечек данных можно выделить выгрузки выборок данных согласно требованиям преступника-заказчика [2] [3]. В роли исполнителя преступления может выступать недобросовестный сотрудник организации, который в силу своих служебный обязанностей имеет доступ к данным КИС. Идентификация поведения пользователя в процессе поиска данных и их выгрузки для последующей передачи заказчику, включая переписывание данных или фотографирование экрана, позволит предотвратить утечку данных и обеспечить устойчивую работу предприятия. Невозможность сформировать исчерпывающий набор сценариев внутренних утечек и высокая интенсивность потока данных КИС делают необходимым применение специального программного обеспечения для контроля действий сотрудников.

Один из способов ранней идентификации – анализ профессионального поведения пользователя – основан на предположении, что поведение пользователя меняется в момент совершения утечки данных. Изменения могут быть выражены в виде обращения к ранее не используемым категориям данных или элементам корпоративной информационной системы или нетипичными действиями при выполнении бизнес-процессов.

Объектом исследования является поведение пользователей в корпоративных информационных системах. **Предметом исследования** являются закономерности профессионального поведения пользователей корпоративных информационных систем.

Целью диссертационной работы является выявление и изучение закономерностей профессионального поведения пользователей на основе анализа данных КИС, разработка алгоритмов идентификации утечек данных с учетом установленных закономерностей и применение созданного на этой основе программного комплекса для контроля действий пользователей. Для выполнения цели диссертационной работы необходимо решение следующих задач:

1. Изучение и сравнение существующих методов анализа поведения пользователей программного обеспечения и идентификации утечек данных.

2. Анализ функциональности, архитектуры и способов реализации программных средств для контроля действий пользователей, формирование требований к программной реализации алгоритмов идентификации утечек данных.
3. Поиск способов определения закономерностей поведения пользователей корпоративного программного обеспечения. Создание модели поведения пользователя. Разработка алгоритма идентификации аномального поведения пользователей.
4. Реализация разработанных алгоритмов идентификации аномального поведения пользователей в виде программного комплекса.
5. Внедрение и апробация программного комплекса для контроля действий пользователей, оценка эффективности реализованных алгоритмов.

Методы исследования.

В диссертации использованы методы объектно-ориентированного подхода к созданию программного обеспечения, методы машинного обучения, проектирования баз данных. Средства языка моделирования UML использованы для проектирования программного обеспечения. В качестве языков реализации программного обеспечения использовались языки Python, C#.

Научная новизна диссертационной работы состоит в следующем:

1. Разработан алгоритм идентификации утечек данных, особенностью которого является возможность определять поведенческие аномалии двух типов: аномалии в поведенческом графе или аномалии в загруженных пользователем текстовых данных КИС.
2. Разработан алгоритм определения уровня значимости поведенческой аномалии, использующий модели поведения нескольких пользователей.
3. Создана модель поведения пользователя корпоративной информационной системы, особенностью которой является использование графа де Брюина второго порядка для учета контекста предыдущего состояния и получения связанных с изменением состояния текстовых данных.

Защищаемые положения

1. Разработанный алгоритм идентификации утечек данных позволяет определять поведенческие аномалии двух типов: аномалии в поведенческом графе или аномалии в загруженных пользователем текстовых данных КИС.
   Соответствует пункту 6 паспорта специальности: Методы, модели и средства мониторинга, предупреждения, обнаружения и противодействия нарушениям и компьютерным атакам в компьютерных сетях.
2. Использование моделей поведения нескольких пользователей позволяет определить степень значимости обнаруженной поведенческой аномалии. точность
   Соответствует пункту 8 паспорта специальности: Анализ рисков нарушения информационной безопасности и уязвимости процессов обработки, хранения и передачи информации в информационных системах любого вида и области применения.
3. Модель поведения пользователя на основе графа де Брюина второго порядка и ассоциированных со сменой состояния текстовыми данными позволяет установить признаки, характеризующие обнаруженную аномалию.
   Соответствует пункту 6 паспорта специальности: Методы, модели и средства мониторинга, предупреждения, обнаружения и противодействия нарушениям и компьютерным атакам в компьютерных сетях.

Для процесса анализа поведения пользователя распространенным источником входных данных являются лог-записи [4] [5] [6] – структурированные элементы данных, содержащие информацию о событиях в работе программного обеспечения. Исследование коллекции лог-записей позволяют определить сбои в работе аппаратного и программного обеспечения, а также выявить закономерности поведения пользователей. Лог-запись содержит как минимум два атрибута: название события и время его возникновения. Поиск посторонних элементов осложняется несбалансированностью тренировочных наборов данных, которые содержат преимущественно нормальные элементы, а все типы аномальных объектов не могут быть известны заранее [4]. Также тренировочный набор данных является неразмеченным. Для обработки лог-записей и выявления посторонних элементов широко применяются методы обработки естественного языка, включая метрики обратной частоты документа (inversed document frequency, IDF) [6] [7], векторные представления текстовых данных [8] и методы теории графов [9] [10]. В работе [6] выявляются необычные частоты событий и необычное время их возникновения для обнаружения аномалий. В процессе выявления аномалий используется фиксированный перечень ранжированных по важности событий с применением метрики обратной частоты документа (IDF), в роли текстового документа выступает рабочий день сотрудника предприятия, содержащий список событий. В исследовании [5] анализ текстовых данных лог-записей ограничен описанием события и базой синонимов и антонимов событий. В упомянутых выше работах при анализе поведения пользователя не принимаются во внимание текстовые данные КИС.

Процесс контроля действий пользователя может быть реализован централизованным (сбор данных и анализ на сервере КИС) или распределенным (сбор данных на клиентских устройствах и анализ на сервере) способами. Первый способ привлекателен упрощенной архитектурой и развертыванием, но его реализация осложнена закрытым исходным кодом КИС и системы управления БД. Второй способ предполагает установку программы-агента для отслеживания действий на каждое клиентское устройство, а получаемые от агентов данные содержат более подробные сведения о действиях пользователей. Текстовые атрибуты включают отображаемые в клиенте КИС данные. Графовая модель данных включает последовательности перехода клиента КИС от одного состояния к другому. При наблюдении на сервере графовая модель может быть представлена последовательностью вызова методов сервера КИС или последовательностью обращения к таблицам БД.

Входными данными для процесса идентификации утечек данных являются лог-записи, представленные вектором *x=(src, user, posted, event, elementPath, elText, text),* где *src* – идентификатор программы-агента, user – имя пользователя, posted – время возникновения события (смены состояния клиента КИС), *elementPath* – идентификатор элемента управления пользовательского интерфейса, elText – текстовые данные элемента управления, *text* – текстовые данные клиента КИС в виде коллекции параграфов текста. Лог-запись преобразуется в вектор признаков. Вектор $x = \{s_1, s_1, ..., s_m, b_1, b_2, ..., b_n\}$ признаки графовой модели данных (компоненты s_i) и текстовые признаки (компоненты b_j).

Первым этапом анализа поведения пользователей (рис. 1) является построение иерархии элементов интерфейса пользователя, которыми пользуется сотрудник. Затем выполняется обрезка дерева – редко используемые узлы (листья) включаются в родительский узел.

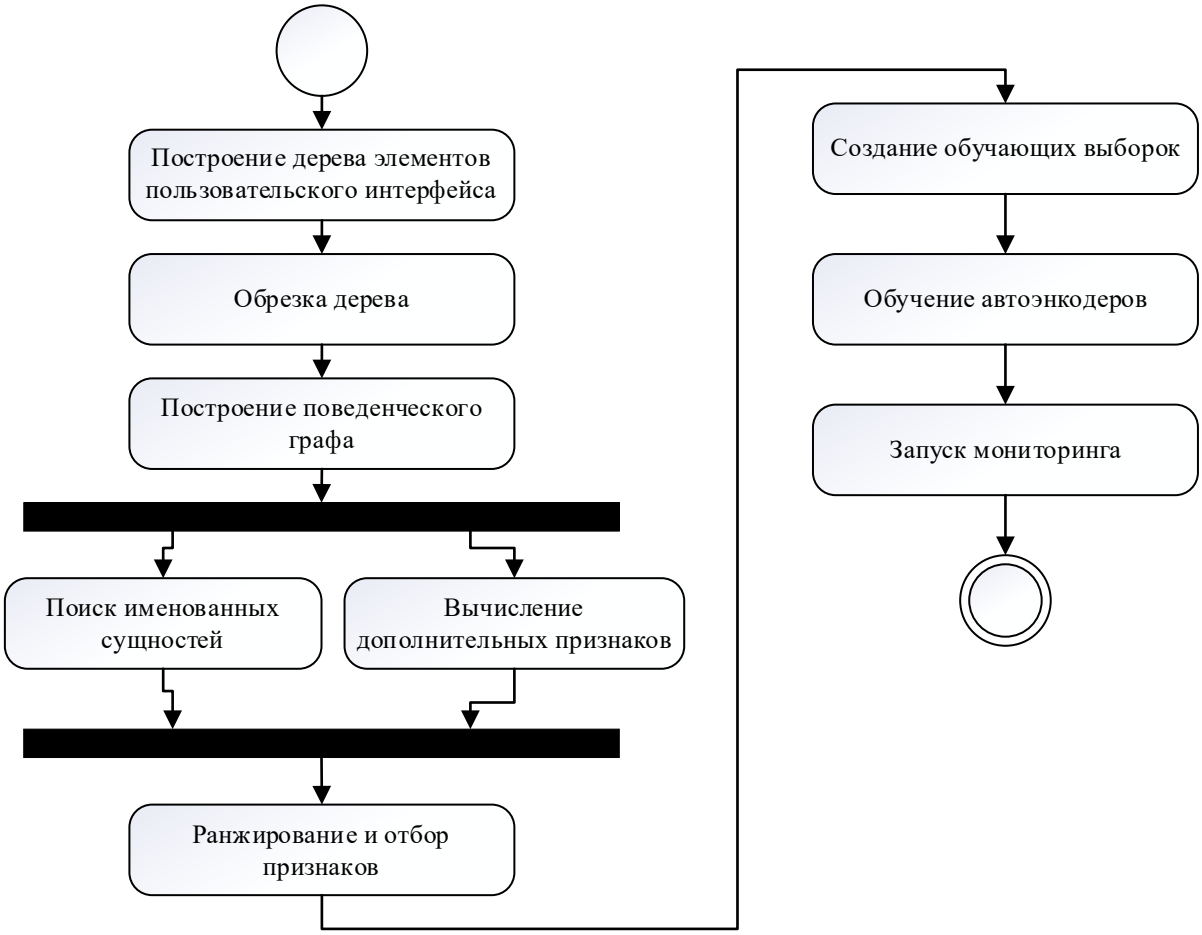


Рис. 1– Процесс идентификации утечек данных

Полученное дерево применяется для получения идентификаторов элементов интерфейса. Состоянию программы сопоставляется идентификатор узла дерева. В каждом состоянии клиента КИС – текстовые данные являются множеством параграфов. Для проведения анализа ценность представляют только новые параграфы текста, полученные из корпоративной БД при совершении пользователем действия. Новые текстовые данные представлены множеством $S_i^{<PageText>} = P_{k+1} / P_k = \varnothing$, где P_k – множество параграфов текста в состоянии программы в момент k, P_{k+1} – множество параграфов текста в состоянии программы в момент $k+1$. При представлении перехода программы из состояния S_k в состояние S_{k+1} в виде объединенного узла $S_k S_{k+1}$ происходит построение графа де Брюина [6] второго порядка (рис. 2). Вершина графа второго порядка хранит в виде атрибута параграфы текста и предыдущее состояние – контекст.

Рис. 2. Преобразование последовательности лог-записей в граф де Брюина второго порядка

Для определения поведенческой аномалии используется функция оценки *f=y(model, winow),* возвращающая числовую оценку соответствия последовательности действий пользователя *window* на основе ранее наблюдаемой модели поведения $model$. Модель поведения представлена обученной нейронной сетью-автоэнкодером на коллекции лог-записей, представляющих собой переходы по вершинам поведенческого графа де Брюйна. Оценка безопасности поведения принадлежит диапазону [0; 1] и определяется на основе превышения ошибки репликации автоэнкодера ранее наблюдаемых значений. Значение оценки «0» свидетельствует о полном соответствии модели поведения, а значение «1» – о максимальном несоответствии модели поведения.

Текстовые данные профиля поведения пользователя преобразуются в набор категориальных признаков поведения. В множество категориальных признаков включаются обнаруженные именованные сущности, географические признаки, установленные по телефонным кодам, адресам и ИНН, товарные категории и др. Соответствие текстовых данных модели поведения производится с помощью ансамбля автоэнкодеров, каждый из которых используется для разных групп категориальных признаков.

Коллекция $window = (x_t, x_{t+1}, ..., x_{t+l})$ является окном (подпоследовательностью) длины l, где каждый элемент x_i является преобразованной лог-записью, содержащей идентификатор вершины графа второго порядка и признаки текстовых данных. Каждое временное окно $window$ преобразуется в вектор (рис. 2), компоненты которого равны сумме компонент векторов-лог-записей $window\_vector = \sum_{i=0}^{l} x_i$. Нормирование значений признаков временного окна происходит отдельно для графовых и текстовых признаков. От длины временного окна зависит характер обнаруживаемых поведенческих аномалий: от просмотра отдельных записей от массовой выгрузки данных. Использование временных окон вместо изолированных лог-записей позволяет снизить разреженность данных за объединения значений признаков из нескольких узлов графа и соответствующих этим узлам текстовых признаков.

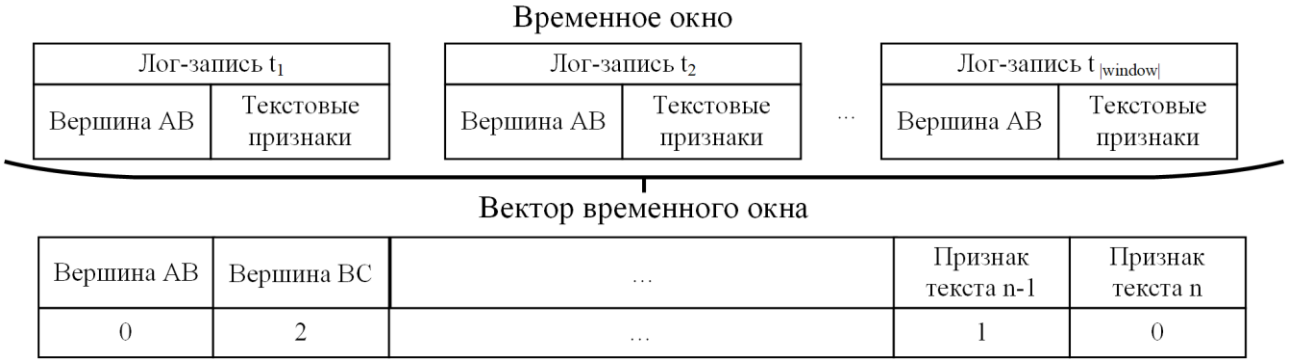


Рис. 3. Преобразование коллекции лог-записей в окно

При обнаружении поведенческой аномалии происходит оценка ее значимости. Коллекция лог-записей *window* с обнаруженной аномалией проверяется на соответствие моделям поведения других пользователей КИС. Приоритет аномалии устанавливается согласно следующей формуле:

$$R = 1 + \sum_{i=0}^{|U|} f(model_{u_i}, window), \quad (1)$$

где U – множество пользователей со схожими служебными обязанностями, $model_{u_i}$ – *модель пользователя* $u_i \in U$.

Реализация алгоритма

Алгоритм идентификации поведенческих аномалий реализован в виде программной системы, включающей агент для получения лог-записей, монитор процессов клиента, обработчик лог-записей и накопитель данных.

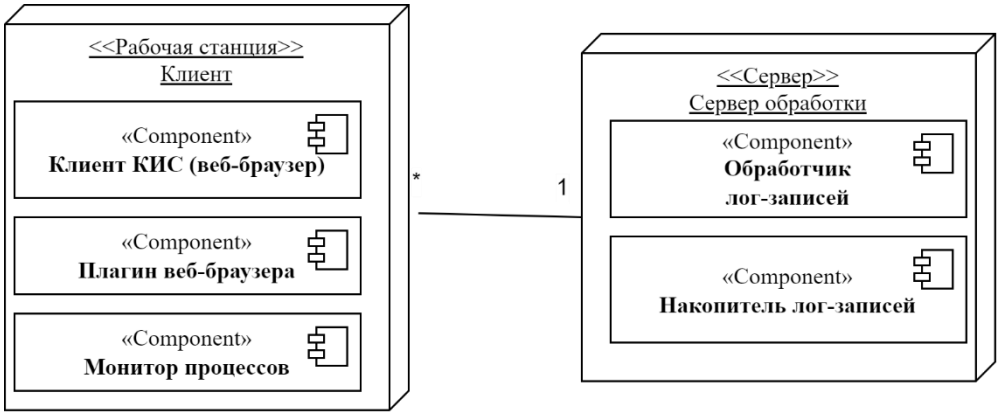


Рис. 4. Компонентная архитектура

Проведенный экспериментальный анализ подтвердил преимущество использования графа второго порядка для определения поведенческих аномалий.

Таблица 1

Результаты эксперимента

Сценарий	**Алгоритм**	**Тип данных**	**Количество информативных признаков**	**Размер временного окна, лог-записей**	**Площадь под ROC-кривой, %**
Единичные случаи	Автоэнкодер	Граф первого порядка	16	24	80,1
		Граф второго порядка	39	24	92,2
		Граф второго порядка	39	12	83,5
Выгрузка записей несвойственной тематики	Автоэнкодер	Текстовый	47	24	87,4
	Ансамбль автоэнкодеров	Текстовый	47	24	91,9
Последовательная выгрузка данных	Автоэнкодер	Граф второго порядка	40	24	87,0
	Автоэнкодер	Текстовый	47	24	83,2
	Ансамбль автоэнкодеров	Текстовый	47	24	86,8

Заключение

Представленный алгоритм идентификации утечек данных позволяет определять аномалии поведения пользователей с возможностью объяснения их причины, устанавливаемой по подмножеству признаков временного окна. Дальнейшем развитием работы является расширение множества сценариев утечек данных и последующая оценка и адаптация алгоритма по результатам проведенной оценки.

СПИСОК ЛИТЕРАТУРЫ

1. Количество утечек данных в крупных компаниях выросло в 1,5 раза // Ведомости. - 2023. - 12.05. - Ст. 19.
2. Исакова Т. Особо уцененная информация // Газета «Коммерсантъ». 2022. 27, декабрь. Ст. 33.
3. Исакова Т., Королев Н. На работу как на фишинг // Газета «Коммерсантъ». - 2022. - 08.08. - Ст. 18.
4. Software execution logs using the siamese network // Automated Software Engineering. - 2022. - №29.
5. Weibin M. [et al.] LogAnomaly: Unsupervised Detection of Sequential and Quantitative Anomalies in Unstructured Logs // Proceedings of the Twenty-Eighth International Joint Conference on Artificial Intelligence. - Macao, China: IJCAI, 2019. - С. 4739-4745.
6. Hu J., Baoming T., Lin D. Anomalous User Activity Detection in Enterprise Multi-Source Logs // International Conference on Data Mining Workshops. - New Orleans, USA: IEEE, 2017. - С. pp. 797-803.
7. Mohotti W., Nayak R. Efficient outlier detection in text corpus using rare frequency and ranking // ACM Transactions on Knowledge Discovery from Data. - 2020. - №14(6).
8. Haixuan G., Shuhan Y., Xintao W. LogBERT: Log Anomaly Detection via BERT // International Joint Conference on Neural Networks (IJCNN). - Shenzhen, Chin: IEEE, 2021.
9. Ma X. at al. A Comprehensive Survey on Graph Anomaly Detection with Deep Learning // IEEE Transactions on Knowledge and Data Engineering. - 2021.
10. Boniol P., Palpanas T. Series2Graph: graph-based subsequence anomaly detection for time series // Proceedings of the VLDB Endowment. - Tokyo: VLDB Endowment, 2020. - С. 1821–1834.

Барков В.В.
МТУСИ, старший преподаватель
v.v.barkov@mtuci.ru

КЛАССИФИКАЦИЯ ПРОТИВОПРАВНЫХ И НЕЖЕЛАТЕЛЬНЫХ МОБИЛЬНЫХ ПРИЛОЖЕНИЙ МЕТОДАМИ МАШИННОГО ОБУЧЕНИЯ В ПОТОКОВОМ РЕЖИМЕ

Аннотация: Исследование направлено на повышение эффективности методов машинного обучения при классификации трафика мобильных приложений в потоковом режиме с целью выявления противоправных и нежелательных приложений. Научная новизна состоит в разработке и исследовании улучшенных алгоритмов классификации трафика мобильных приложений методами машинного обучения с применением автокодировщиков как для классификации, так и для обнаружения дрейфа концепта.

Ключевые слова: алгоритмы классификации; дрейф концепта; поток данных; атрибуты и мобильные приложения; метки класса

Актуальность темы

Задача выявления опасного контента – противоправных, нежелательных и вредоносных приложений в сетевом трафике, генерируемом в том числе мобильными устройствами, приобретает особую актуальность в связи с активным развитием в мире мобильной связи Интернета вещей.

Под противоправным контентом понимается информация, содержание которой противоречит законодательству Российской Федерации. В числе типовых нарушений, которые должны выявляться в контенте — призывы к массовым беспорядкам, оскорбление общества, государственной власти, официальных государственных символов, конституции или исполнительной власти, призывы к суицидам, информация, связанная с изготовлением и приобретением наркотиков, и др. Федеральное законодательство предусматривает порядок ограничения не только к таким ресурсам в сети Интернет, но и к программным приложениям. Ограничение доступа к приложениям предусматривается в случаях распространения с их помощью информации с нарушением авторских и/или смежных прав, а также в случае установления факта неисполнения организатором распространения информации в сети Интернет обязанностей, предусмотренных законодательством.

Для операторов мобильной связи информация об использовании тех или иных приложений пользователями необходима для получения статистики по наиболее часто используемым. Мониторинг приложений обеспечивает при необходимости ограничение доступа к сетевым ресурсам.

Для решения подобных задач классификации мобильного трафика в настоящее время широкое распространение получили методы интеллектуального анализа данных (Data Mining, DM) и машинного обучения (Machine Learning, ML). Они позволяют адаптироваться к постоянно изменяющейся структуре Интернет-ресурсов и учитывать специфику сетевого трафика. Внедрение таковых методов, как показывает опыт, позволяет производить классификацию, анализ и фильтрацию сетевого трафика вредоносных и нежелательных приложений с высокой эффективностью.

Вместе с тем известные работы, посвященные проблеме классификации трафика, слабо учитывают требование выявления неизвестного типа трафика. В одних случаях при проектировании классификаторов приложений с учителем неизвестный трафик полностью исключается в предположении наличия только известных классов. В других случаях неизвестный трафик вовсе не рассматривался в экспериментах, обучение происходило на данных из ограниченного числа классов приложений и тестировались с помощью других данных из тех же известных классов.

Известно, что отсутствие полной и достоверной информации о структуре помехового (фонового) трафика значительно снижает качество классификации интересующих приложений. Одним из способов повышения качества классификации является использование искусственных нейронных сетей (ИНС), в частности, автокодировщиков (АК).

Степень разработанности темы

Теоретическую базу диссертации в области методов ML составляют работы таких ученых, как Айвазян С.А., Айзерман М.А., Барсегян А.А., Загоруйко Н.Г., Вапник В.Н., Воронцов К.В., Mitchell T., Hastie T., Tibshirani R., Friedman J.T., Xu K., Zhang Z., Bhattacharyya S., Heckerman J.D. и др. Эти исследования были выполнены преимущественно в области экономики, и некоторые их результаты можно встроить в предмет сетевых и телекоммуникационных исследований.

Отдельные вопросы ML-исследований трафика рассматривались в трудах Большева А.К., Гетьмана А.И., Зубкова Е.В., Котенко И.В., Козьмовского Д.В., Михайлова А.Ю., Маркина Ю.В., Назарова А.О., Петровского М.И., Санарова А.С., Шелухина О.И., Щербаковой Н.Г., M. Pietrzyk, Z. Chen, B. Yang, J. Erman, K. Balachandran, J.H. Broberg, T. Bujlow, V. Carela-Español, C.C. Aggarwal, Y. Wang, G.S.o Han, J. Erman, M. Arlitt, A. Mahanti и др. Однако задаче классификации трафика мобильных приложений было уделено недостаточно внимания.

Вышесказанное обусловливает актуальность настоящего исследования, направленного на повышение эффективности классификации трафика мобильных приложений методами машинного обучения в потоковом режиме.

Целью диссертационного исследования является повышение эффективности классификации противоправного контента, нежелательных и вредоносных приложений в сетевом трафике методами машинного обучения в потоковом режиме.

Достижение поставленной цели предусматривает решение **частных задач:**

1) Сравнительный анализ известных алгоритмов классификации IP-трафика неправомерных/нежелательных мобильных приложений в условиях априорной неопределенности в режиме offline;
2) разработка нового алгоритма на основе использования ИНС в виде автокодировщика;
3) разработка алгоритма обнаружения смены концепта в наблюдаемых данных при классификации трафика мобильных приложений;
4) разработка алгоритмов классификации трафика мобильных приложений в потоковом режиме с «конечной» и «бесконечной» памятью на базе созданных репрезентативных выборок;
5) разработка программного комплекса (ПК) «Система анализа трафика» (САТ) для автоматизации процесса классификации трафика мобильных приложений.

Объект исследования: мобильный сетевой трафик.

Предмет исследования: классификация мобильных приложений в трафике методами

ML в условиях априорной неопределенности

Методы исследования: методы математического моделирования, теории вероятности и математической статистики, машинного обучения и интеллектуального анализа (обработки) данных. Методологической основой исследования является системный подход.

Основные научные положения, выносимые на защиту.

1) Способ отбора рационального числа атрибутов на основе анализа их информативности, фиксируя допустимую вероятность ложной классификации. Определены, ограничения на структуру анализируемых данных по числу потоков и пакетов в потоке, в то время как *общепринятые подходы* предполагают расчет характеристик на основе данных всего потока.
2) Модифицированный алгоритм классификации нежелательных приложений в условиях неконтролируемого фонового трафика, отличающийся от известных каскадным включением нейронной сети в виде АК, выполняющего предварительную фильтрацию и вторичного классификатора.
3) Статистическая *модель обнаружения смены концепта* классифицируемых приложений мобильного трафика, *отличающаяся от известных включением* в качестве базового детектора дрейфа концепта АК, в котором наличие дрейфа оценивается посредством оценок ошибок реконструкции анализируемых приложений и превышения пороговых значений.
4) *Новый алгоритм обнаружения смены концепта* мобильных приложений в потоковом режиме с обработкой в скользящем окне в режиме накопления с «конечной памятью», как с равномерной, так и неравномерной интенсивностью поступления данных, ***отличающийся*** *от известных* учетом «старения» данных в окне обработки и негауссовским характером изменяющихся параметров классифицируемых приложений;
5) Модифицированный алгоритм Adaptive Random Forest (MARF), осуществляющий классификацию значительно (в 2-3 раза) быстрее, чем алгоритмы RF, Hoeffding Adaptive Tree, K nearest neighbors, Oza Bagging, за счет введения «запасных деревьев», обучение которых начинается всякий раз, когда обнаруживается наличие дрейфа концепта.

Научная новизна состоит в следующем:

1) Методика отбора значимых атрибутов классификации, обеспечивающая повышение достоверности и снижение вероятности ложной классификации, обеспечивающая достоверность классификации зашифрованных приложений более 90% при размере обучающей выборки ограниченной 300 потоками с 16-58 пакетами в каждом потоке (в зависимости от приложения), в то время как *общепринятые подходы* предполагают расчет характеристик по данным всего потока. Предложенная методика позволяет отбирать атрибуты для эффективной классификации к потокам в потоковом режиме и является *инвариантной* по отношению к разным типам трафика.
2) *Алгоритм*, состоящий из последовательно включенных АК и типового классификатора обеспечивает лучшую классификации нежелательных приложений в условиях априорной неопределенности и неконтролируемого фонового трафика, *повышает достоверность* (accuracy) классификации приложений на 7% *по сравнению с известными алгоритмами,* не требуя разметки фоновых приложений в случае их внезапного появления.

3) *Модель обнаружения смены концепта* классифицируемых мобильных приложений, *отличающаяся от известных* включением АК (для каждого приложения), в которой наличие дрейфа оценивается по ошибкам реконструкции анализируемых приложений и превышению пороговых значений, *что повышает точность обнаружения* смены концепта в потоковом режиме.
4) Алгоритм обнаружения смены концепта и классификации трафика мобильных приложений в потоковом режиме с обработкой в скользящем окне в режиме накопления с «конечной памятью» для равномерной и неравномерной интенсивности поступления данных, *отличающийся от известных* учетом «старения» данных»
5) Модифицированный адаптивный MARF, обучающий «запасные деревья» параллельно со всем ансамблем всякий раз, когда обнаруживается наличие дрейфа концепта потоковом режиме и осуществляется в 2–3 раза быстрее, чем стандартный алгоритм RF.

Теоретическая значимость исследования состоит в совершенствовании известных математических моделей позволяющих путём применения методов машинного обучения осуществлять в потоковом режиме классификацию неправомерных и нежелательных приложений в условиях априорной неопределенности относительно состава и количества классифицируемых приложений, в условиях возможного дрейфа концепта.

Практическая ценность работы заключается в разработке и программной реализации программного комплекса для классификации трафика мобильных устройств в потоковом режиме в условиях априорной неопределенности относительно состава и количества классифицируемых приложений, в условиях дрейфа концепта.

Сформированная экспериментальная база данных сетевого трафика типовых мобильных приложений, которая может быть использована в системах обнаружения вторжений, для фильтрации вредоносных и нежелательных приложений, блокировки заданных приложений, в том числе в виде зашифрованного трафика.

Достоверность результатов диссертационной работы подтверждается сходимостью результатов имитационного моделирования с результатами экспериментальных данных, корректным использованием современного математического аппарата, а также достаточно широким рядом публикаций, обсуждением основных положений со специалистами на научных конференциях.

Соответствие паспорту специальности.

Диссертация соответствует пунктам 15. «Методы и модели выявления и противодействия распространению ложной и вредоносной информации» и 16. «Принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности» паспорта специальности 2.3.6 – «Методы и системы защиты информации, информационная безопасность».

Личный вклад автора. Основные научные результаты, в том числе разработка алгоритмов классификации, а также разработка методических рекомендаций по подбору параметров алгоритмов получены автором лично. Вклад соавторов ограничивался постановкой задач на исследования и обсуждением полученных результатов

Связь работы с научными программами, темами, грантами. Исследования выполнялись в инициативном порядке, в рамках работы по гранту аспирантам, соискателям и

молодым ученым на исследования, направленные на обеспечение информационной безопасности для задач цифровой экономики и по государственной поддержке ведущих научных школ Российской Федерации в области информационной безопасности

ПУБЛИКАЦИИ

1. Шелухин О.И., Барков В.В., Маторин Ф.А. Повышение эффективности классификации противоправных и нежелательных приложений в условиях фонового трафика с помощью автокодировщиков. «Вестник Санкт-Петербургского государственного университета технологии и дизайна» Серия 1. Естественные и технические науки». 2023 № 3. С. 90–100.
2. Шелухин О.И., Барков В.В., Симонян А.Г. Обнаружение дрейфа концепта при классификации мобильных приложений с использованием автокодировщиков // Наукоемкие технологии в космических исследованиях Земли. 2023. Т. 15. № 3. С. 90–100
3. Шелухин О.И., Барков В.В., Полковников М.В. Сравнительный анализ алгоритмов оценки количества и структуры атрибутов в задачах классификации мобильных приложений // Наукоемкие технологии в космических исследованиях Земли. 2019. Т. 11. № 2. С. 90–100.
4. Sheluhin, O.I. Experimental Studies of Network Traffic of Mobile Devices with Android OS / O.I. Sheluhin, S.D. Erokhin, A.V. Osin, V.V. Barkov // Systems of Signals Generating and Processing in the Field of on Board Communications. – 2019
5. Свидетельства о государственной регистрации программы для ЭВМ
6. Шелухин, О.И., Ерохин, С.Д., Барков В.В. Программный комплекс для онлайн классификации сетевого трафика // Свидетельство о государственной регистрации программы для ЭВМ № 2019615330 от 24 апреля 2019 г.
7. Шелухин, О.И. Классификация зашифрованного трафика мобильных приложений методом машинного обучения / О.И. Шелухин, В.В. Барков, М.В. Полковников // Вопросы кибербезопасности. 2018. №4(28). С.21-28.
8. Sheluhin, O.I. Influence of Background Traffic on the Effectiveness of Mobile Applications Traffic Classification Using Data Mining Techniques / O.I. Sheluhin, V.V. Barkov // T-Comm. 2018. vol.12, no.10. pp.52-54
9. Шелухин, О.И. Создание базы данных сетевого трафика для автоматизации классификации мобильных приложений под управлением операционной системы Android / О.И. Шелухин, С.Д. Ерохин, В.В. Барков // Нейрокомпьютеры: разработка, применение. 2019. №1. С.40-51
10. Sheluhin O.I. The Online Classification of the Mobile Applications Traffic Using Data Mining Techniques. / O.I. Sheluhin, V.V. Barkov, S.A. Sekretarev // T-Comm. 2019. vol. 13. no.10. pp.60-67.
11. Шелухин, О.И., Барков, В.В., Секретарев, С.А. Алгоритмы обнаружения дрейфа концепта при потоковой классификации трафика мобильных приложений // REDS: Телекоммуникационные устройства и системы 2020. №3. С.19-27.
12. Шелухин, О.И. Разработка инфраструктуры для классификации сетевого трафика мобильных приложений с применением алгоритмов машинного обучения / О.И. Шелухин, В.В. Барков // Телекоммуникационные и вычислительные системы - 2017. Тр. межд. научно-тех. конф. – 2017. – С.180-181.

13. Шелухин, О.И. Экспериментальные исследования и создание базы данных сетевого трафика мобильных устройств под управлением операционной системы Android / О.И. Шелухин, В.В. Барков // Фундаментальные проблемы радиоэлектронного приборостроения: «INTERMATIC-2018». – М.: МИРЭА. 2018. Т. 18. №4. С.1011-1017.
14. Шелухин, О.И. Методы сбора сетевого трафика с мобильных устройств под управлением операционной системы Android с целью классификации по типам приложений / О.И. Шелухин, В.В. Барков //. Сб. тр. XII Межд. отраслевой науч.-тех. конф Технологии информационного общества (14-15 марта 2018 г., Москва). М.: МТУСИ. Т.2. С.20-21.
15. Барков, В.В. Проектирование и разработка экспертно-аналитической системы "Система анализа трафика" для исследования алгоритмов классификации трафика мобильных устройств под управлением операционной системы Android // Безопасные информационные технологии: Сб. тр. 9-й всерос. науч.-тех. конф. – М.: МГТУ им. Н.Э. Баумана, 4-5 декабря 2018 г., С. 2-12.
16. Барков, В.В. Исследование алгоритмов классификации зашифрованного трафика мобильных устройств по типам приложений методами машинного обучения / В.В. Барков, М.В. Полковников // Тр. Межд. научно-тех. конф. «Телекоммуникационные и вычислительные системы 2018». – М.: Горячая линия – Телеком, 2018. – С.310-312.
17. Барков, В.В. Классификация трафика мобильных устройств по типам приложений методами машинного обучений в режиме онлайн / В.В. Барков, С.А. Секретарёв // Межд. форум информатизации (МФИ-2018) 6 Тр. конф. «Телекоммуникационные и вычислительные системы 2018». – М.: Горячая линия – Телеком, 2018. – С.319-321.
18. Барков, В.В. Классификация трафика нежелательных мобильных приложений методом машинного обучения в потоковом режиме // Сб. научн. трудов II Всерос. науч. школы-семинара «Современные тенденции развития методов и технологии защиты информации». – М., 2022. – С. 167-174.

Белова Е. П.
УУНиТ, старший преподаватель
кафедры управления
информационной безопасностью
yelenabelova92@gmail.com

СИСТЕМА БИОМЕТРИЧЕСКОЙ АУТЕНТИФИКАЦИИ ПО ПАРАМЕТРАМ РЕЧИ И ВИДЕОИЗОБРАЖЕНИЮ НА ОСНОВЕ НЕЙРОСЕТЕВЫХ ТЕХНОЛОГИЙ

Аннотация: В статье представлены актуальность, степень разработанности темы, цель и задачи исследования. Приводятся 3 вида научной новизны: биометрического образа, методического комплекса и системы биометрической аутентификации. Также статья содержит теоретическую значимость, практическую значимость, основные положения, выносимые на защиту. Говорится о степени достоверности исследования и апробации результатов. Приводится краткое содержание кандидатской диссертации. Основная роль отводится комбинации различных биометрических методов без привлечения дополнительного оборудования.

Ключевые слова: биометрическая аутентификация, голос, речь, видеоизображение, геометрия лица, жесты рук, формантные характеристики, фонема, результаты вейвлет-преобразования, искусственная нейронная сеть.

На сегодняшний день активно идёт развертывание информационного и цифрового общества. Важную роль в защите информационных систем играют системы аутентификации. Согласно [1] каждое предприятие подлежит информатизации, то есть все основные бизнес-процессы должны обеспечиваться информационными системами учреждений, документация представлена в цифровом виде, личность каждого сотрудника при выполнении им его непосредственных служебных обязанностей в информационной системе предприятия-работодателя подлежит обязательной верификации.

Биометрические методы аутентификации являются наиболее перспективными, так как они неотделимы от самого человека.

Именно по личным физиологическим характеристикам люди и животные узнают друга. Для этого мозг анализирует различные параметры. Научиться классифицировать различные признаки и распознавать личность пользователя, подобно тому, как это делается в живом мире, могут и искусственные нейронные сети. Весьма эффективными являются и различные комбинации нейросетевых технологий с другими алгоритмами и методами машинного интеллекта [2-4].

Актуальность системы биометрической аутентификации по параметрам речи и геометрии лица, базирующейся на ведущих методах и алгоритмах аутентификации с использованием уникальных биометрических образов заключается в том, что данная система позволяет обеспечить высокую эффективную процедуру аутентификации с минимальными затратами. Она может быть использована во многих сферах, таких как банковское дело, государственные учреждения, здравоохранение и другие, в которых нужна надёжная и безопасная аутентификация. Кроме того, такая система может значительно упростить процедуру аутентификации, ускорить процессы аутентификации и повысить удобство использования.

Степень разработанности темы заключается в том, что в настоящее время выносимый на защиту программный комплекс не имеет аналогов. Схожими в некоторых аспектах можно назвать работы [5, 6].

Исследование использования различных речевых параметров в рамках решения задач биометрической аутентификации проводят в своих трудах В. Н. Сорокин, Ю. Н. Матвеев, С. Л. Марпл, Л. Р. Рабинер и Р. В. Шафер [7-10].

К известным системам аутентификации по голосу относятся [11-13].

Работ, посвящённых комбинированному использованию формантных характеристик в рамках 2-х различных программных модулей, в одном из которых частоты семи первых формант комплексируются с кепстральными и дельта- коэффициентами, в совокупности с модулем, обрабатывающим результаты вейвлет-преобразования не выявлено.

Распознаванию по лицу посвящены следующие работы [14-18].

Целью диссертационной работы является повышение эффективности аутентификации пользователей в информационной системе при помощи биометрической системы аутентификации по параметрам речи и геометрии лица.

Для достижения поставленной цели необходимо выполнить следующие **задачи**:

1. Провести глубокий анализ литературных источников, ГОСТов и нормативных документов.
2. Разработать уникальный биометрический образ личности пользователя для системы аутентификации по голосу.
3. Разработать уникальный биометрический образ личности пользователя для системы аутентификации по видеоизображению лица.
4. Разработать архитектуру системы аутентификации пользователя по голосу на базе комплекса искусственных нейронных сетей, алгоритмов и методов машинного обучения.
5. Разработать архитектуру системы аутентификации пользователя по видеоизображению лица при помощи свёрточной искусственной нейронной сети.
6. Разработать систему распознавания жестов по их видеоизображению.
7. Разработать программный комплекс системы биометрической аутентификации по параметрам речи и видеоизображению на основе нейросетевых технологий, алгоритмов и методов машинного обучения.

Новизна биометрического образа пользователя информационной системы, основанного на анализе характеристик спектров гласных звуков и дифтонгов, кепстральном анализе, результатах вейвлет-преобразования фраз и чисел и комбинации данных геометрии лица пользователя, выделенных при помощи метода Виолы-Джонса и модели бинарной классификации изображений, заключается в комплексировании характеристик семи первых формант и частот лидирующих формант, кепстральных и дельта- коэффициентов с частотами семи первых формант, произнесённых пользователем гласных звуков и дифтонгов, анализе временных рядов в реальном времени и комплексировании метода Виолы-Джонса и модели бинарной классификации изображений, что позволяет обеспечить уникальность образа для системы биометрической аутентификации по параметрам речи и геометрии лица.

Новизна методического комплекса биометрической аутентификации по параметрам речи и геометрии лица заключается в разработке базы данных биометрических образов и мэтчера для реализации процесса аутентификации пользователей при помощи ансамбля алгоритмов, построенных на основе Гауссовых смесей моделей и свёрточных искусственных нейронных сетей.

Новизна системы биометрической аутентификации по параметрам речи и геометрии лица заключается в разработанной архитектуре системы, включающей экстракторы, базы биометрических данных и мэтчеры, что позволяет, используя модульное строение, реализовать систему программно, а также повысить эффективность аутентификации за счёт уменьшения ошибок 1-го и 2-го рода по сравнению с данными показателями известных систем биометрической аутентификации по голосу.

Теоретическая значимость работы заключается:

1. в сформированном биометрическом образе пользователя информационной системы посредством комбинации биометрических параметров, что позволяет обеспечить уникальность образа для системы биометрической аутентификации по параметрам речи и геометрии лица;
2. в методическом комплексе биометрической аутентификации, основанном на использовании предложенного уникального биометрического образа, что позволяет обеспечить высокую эффективность процедуры аутентификации.

Практическая значимость работы заключается:

1. в разработанной на основе UML технологии моделях процесса проектирования системы биометрической аутентификации по параметрам речи и геометрии лица, отображающей наглядно последовательность действий разработчика и особенности взаимодействия элементов внутри системы, что позволяет сократить время разработки системы и смоделировать поведение системы и её элементов в процессе функционирования;
2. в разработанных архитектуре системы биометрической аутентификации по параметрам речи и геометрии лица и реализующем её комплексе программ, написанных на высокоуровневым языке программирования Python, что позволяет подтвердить эффективность теоретических положений и метода аутентификации, а также использовать программное обеспечение при решении задачи многофакторной аутентификации пользователей в информационной системе.

Для реализации диссертационного проекта используются следующие **методы**:

1. быстрое преобразование Фурье,
2. спектрально-формантный метод,
3. кепстральный анализ,
4. искусственная нейронная сеть (многослойный перцептрон и свёрточная нейронная сеть),
5. Гауссовые смеси,
6. алгоритм «Случайный лес»,
7. логистическая регрессия,
8. метод k-ближайших соседей,
9. метод опорных векторов,
10. стохастический градиентный спуск,
11. стакинг,
12. вотинг.

Основные положения, выносимые на защиту

1. Разработанный уникальный биометрический образ личности пользователя для ключевых модулей системы биометрической аутентификации по параметрам речи и геометрии лица.

2. Разработанный методический комплекс, обеспечивающий функционирование системы аутентификации по параметрам речи и геометрии лица, основанный на использовании уникального биометрического образа.

3. Модель процесса проектирования системы биометрической аутентификации по параметрам речи и геометрии лица.

4. Архитектура системы биометрической аутентификации по параметрам речи и геометрии лица.

5. Программный комплекс системы биометрической аутентификации по параметрам речи и геометрии лица.

Для исследования **степени достоверности** каждый модуль был протестирован на группах испытуемых, кроме того сам программный комплекс проходит испытание в режиме реального времени.

Для **апробации результатов** осуществляется выбор компании.

Краткое содержание диссертации с упором на результаты, полученные за период реализации научного проекта в рамках гранта:

1. Глава 1 содержит анализ биометрических методов, нормативно-правовой базы и имеющихся информационных систем;
2. Во 2-ой главе формируется методический комплекс биометрической аутентификации, приводятся результаты первых испытаний модулей.
3. Третья глава содержит UML-диаграммы системы биометрической аутентификации по параметрам речи и геометрии лица.
4. Четвертая глава посвящена самой системе биометрической аутентификации по параметрам речи и геометрии лица, результатам её тестирования апробации.

Биометрическая система аутентификации состоит из четырёх модулей. Трое из которых используют речевые параметры: формантные характеристики гласных звуков, комплексирование кепстральных и дельта- коэффициентов с частотами семи первых формант и результаты вейвлет-преобразования. Четвёртый модуль предназначен для распознавания пользователя по геометрии лица по видеоизображению посредством комплексирования метода Виолы-Джонса и модели бинарной классификации изображений.

Отдельно стоит отметить многоуровневую систему защиты биометрических данных от фальсификаций:

1. В ходе работы модуля аутентификации по формантным характеристикам гласных звуков, специальный генератор случайным образом предлагает пользователю произнести некую последовательность гласных звуков. Полученные результаты используются как для верификации личности пользователя, так и для доказательства того, что процедура проходит в режиме реального времени.
2. Аналогично работе модуля аутентификации по формантным характеристикам, модуль распознавания по результатам вейвлет-преобразования также включает встроенную защиту от фальсификаций. Для этого генерируются числа в определённом порядке и проверяется совпадает ли произносимое пользователем с заданием.
3. В модуле аутентификации по видеоизображению лица для проверки подлинности предъявления биометрических данных аутентифицируемым, ему предлагается показать случайные жесты.

СПИСОК ЛИТЕРАТУРЫ

1. Указ Президента РФ от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы».
2. Q. N. Tran, B. P. Turnbull, M. Wang, and J. Hu “A privacy-preserving biometric authentication system with Binary classification in a Zero knowledge proof protocol”, IEEE Open Journal of the Computer Society, vol. 3, pp. 1–10, 2021.
3. D. Munikrishna, R. Kiran Kumar, Y. Preetham, K. B. Raja, K. Venugopal “A facial recognition system using KNN based on DWT segmentation combined with ULBPH”, International Journal for Research in Applied Science & Engineering Technology (IJRASET), vol. 8, no. 8, pp. 808–821, Aug 2020.
4. Ankur, M. R. Bharti, V. Bhateja, X. S.Yang, J. Chun-Wei Lin, and R. Das “ECG biometric recognition by Convolutional neural networks with Transfer learning using Random forest approach”, Intelligent Data Engineering and Analytics. FICTA 2022. Smart Innovation, Systems and Technologies, vol 327. Springer, Singapore. https://doi.org/10.1007/978-981-19-7524-0_16.
5. Единая биометрическая система от Ростелеком. — Режим доступа: https://habr.com/ru/company/rostelecom/blog/424751/.
6. Система учёта идентификации и аутентификации личности по голосу и лицу в Эквадоре. — Режим доступа: https://rg.ru/2020/03/24/reg-szfo/rossijskaia-sistema-identifikacii-po-golosu-ne-ostavit-shansov-prestupnikam.html.
7. Сорокин В. Н. Распознавание личности по голосу: аналитический обзор [Текст] / В. Н. Сорокин, В. В. Вьюгин, А. А. Тананыкин // Информационные процессы. – 2012. – Т. 12, №1. – С. 1-30.
8. Матвеев, Ю. Н. Исследование информативности признаков речи для систем автоматической идентификации дикторов [Текст] / Ю. Н. Матвеев // Известия вузов. Приборостроение. – 2013. – Т. 56, №2. – С. 47-51.
9. Марпл С. Л. Цифровой спектральный анализ и его приложения. / С. Л. Марпл. – М.: Мир, 1990.
10. Рабинер Л. Р. Цифровая обработка речевых сигналов. /Л. Р. Рабинер, Р. В. Шафер – М.: Радио и связь, 1981. – 496 с.
11. Аппаратно-программный комплекс криминалистического исследования фонограмм речи «ИКАР Лаб», разработанный компанией «Центр речевых технологий» [Электронный ресурс]. – Режим доступа: http://www.speechpro.ru/upload/productspecificationdocument/file/ikar_lab_broshyura.pdf.
12. Программное обеспечение «GritTec Speaker-ID» от компании ООО «ГритТек» [Электронный ресурс]. – Режим доступа: http://www.grittec.ru/pdf/Manual_GritTec's%20Speaker-ID_The%20mobile%20Client_RU.pdf.
13. Платформа мультимодальной биометрической аутентификации пользователей в каналах дистанционного обслуживания «VoiceKey» от компании «Центр речевых технологий» [Электронный ресурс]. – Режим доступа: http://www.speetech.by/technologies/voice-key#fragment-1.
14. Smith R. S. Facial Expression Detection using Filtered Local Binary Pattern Features with ECOC Classifiers and Platt. / Raymond S. Smith, Terry Windeatt – 2010 [Электронный ресурс]. – Режим доступа: http://proceedings.mlr.press/v11/smith10a/smith10a.pdf.

15. Trigeorgis G. A Deep Semi-NMF Model for Learning Hidden Representations. / George Trigeorgis, Konstantinos Bousmalis, Stefanos Zafeiriou, Bjorn W. Schuller [Электронный ресурс]. – Режим доступа: http://proceedings.mlr.press/v32/trigeorgis14.pdf.
16. Wang H. Robust and Discriminative Self-Taught Learning. / Hua Wang, Feiping, Heng Huang [Электронный ресурс]. – Режим доступа: http://proceedings.mlr.press/v28/wang13g.pdf.
17. Masood M. A. A Particle-Based Variational Approach to Bayesian Non-negative Matrix Factorization. / Muhammad A Masood, Finale Doshi-Velez – 2019 [Электронный ресурс]. – Режим доступа: https://www.jmlr.org/papers/volume20/18-153/18-153.pdf.
18. Larsen A. B. L. Autoencoding beyond pixels using a learned similarity metric. / Anders Boesen Lindbo Larsen, Søren Kaae Sønderby, Hugo Larochell, Ole Winther.[Электронный ресурс]. – Режим доступа: http://proceedings.mlr.press/v48/larsen16.pdf.

Бирих Э.В.
СПбГУТ, старший преподаватель кафедры ЗСС
be1982@mail.ru

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ДАННЫХ, ПЕРЕДАВАЕМЫХ ЧЕРЕЗ ОТКРЫТЫЕ ТЕЛЕКОММУНИКАЦИОННЫЕ КАНАЛЫ СВЯЗИ

Аннотация: На сегодняшний день существуют правила и требования по обеспечению безопасности, но они с учетом развития информационных технологий и новых угроз национальной безопасности (в том числе военные угрозы, угрозы утраты национальной и культурной идентичности российских граждан) полноценно не охватывают информационную безопасность данных, передаваемых по открытым телекоммуникационным каналам связи.

Ключевые слова: информационная безопасность (ИБ), угрозы ИБ, модель нарушителя ИБ, критически важные объекты (КВО), модель угроз ИБ, телекоммуникационная безопасность, кибернетическая разведка (КР).

Цель работы. Систематизация информации об анализе и оценке рисков, их важности для построения системы защиты; изучение рекомендаций в области риск-менеджмента и проектирования защищенных информационно-вычислительных сетей (далее ИВС) с учетом прогнозирующих моделей; анализ и сравнение широко используемых методик оценки и анализа рисков ИБ в контексте построения системы управления ИБ организации.

Задача – разработать методику оценки безопасности масштабируемой ИВС организации для принятия решения о необходимости категорирования на основе Банка данных угроз безопасности информации, разработанного Федеральной службой по техническому и экспортному контролю (ФСТЭК России).

Предмет исследования. Обеспечение информационной безопасности данных, передаваемых в масштабируемой ИВС организации, развернутой на открытых телекоммуникационных каналах связи (далее - ОТКС).

Значительный вклад в решение вопросов, связанных с созданием теоретического и практического задела обеспечения информационной безопасности данных, передаваемых по ОТКС, внесли работы отечественных ученых И.В. Котенко, В.И. Коржика, Н.А. Соколова, В.Г. Шведа, В.А. Яковлева, В.А. Липатникова, А.В. Красова. Работы Б.С. Гольдштейна, Д.В. Сахарова подняли тему возникновения угроз ИБ в процессе использования общего канала сигнализации (далее – ОКС) [1, 2]. Однако научных исследований в данном направлении проводится недостаточно. Вопросы обеспечения информационной безопасности данных, передаваемых в масштабируемой ИВС организации, в процессе использования ОКС ОТКС требуют дальнейшего разрешения. Появилась потребность в поиске способов повышения скрытности работы интегрированных ИВС организации, обеспечения безопасности информации с учетом развития методов и средств КР. Актуальность данной работы значительной возрастает с учетом проведения в настоящее время специальной военной операции, использования иностранными государствами против РФ методов ведения информационной войны, в том числе на ОТКС.

Переходя к предмету исследования можно сказать, что ОКС осуществляет обмен сигнальными сообщениями систем разнообразных применений, включая телефонию,

передачу данных, услуги ISDN, услуги для абонентов сетей мобильной связи, а также функции эксплуатационного управления сетью ОКС.

Общеканальная сигнализация – это метод сигнализации, в котором один канал путем адресации сообщений, в специально построенной выделенной сети в Единой сети электросвязи Российской Федерации (далее – ЕСЭ), передает сигнальную информацию, относящуюся к множеству каналов или другую информацию для управления ЕСЭ. ОКС может рассматриваться как форма передачи данных, которая специализирована для различных типов сигнализации и передачи информации между распределенными в пространстве процессорами, управляющими различными ресурсами ЕСЭ.

Общеканальная сигнализация полностью удаляет сигнализацию из разговорного тракта, используя отдельный общий канал сигнализации для передачи всех сигналов нескольких трактов.

Отличительной чертой протокола ОКС является высокая надежность передачи информации с минимальной задержкой, без потерь и без дублирования сигнальных сообщений.

В ОКС присутствуют данные об информационных каналах и об абонентах ЕСЭ. Сведения о характеристиках и параметрах канала ОКС (сигнальных сообщениях – типах, структурах и длинах сообщений), чувствительная информация, связанная с информацией загрузки и биллинга, со структурой сети, управлением ее оборудованием или с данными пользователей могут использоваться для деструктивных воздействий на ОКС ЕСЭ и на информационные каналы и абонентов.

Система ОКС предназначена для управления информационными каналами и подключения (соединения и разъединения) абонентов путем обмена служебными сообщениями, а информационные потоки – только для обмена информационными сообщениями. Информационные каналы являются объектом управления от ОКС.

Сеть ОКС не является закрытой сетью. Доступ к ней имеют пользователи других сетей, построенных на разных технологиях, например, традиционная телефония, интеллектуальные сети, сети сотовой связи, сети VoIP, ATM, ISDN, сети телекоммуникаций NGN и сети мобильной связи. Рост числа точек доступа между сетью ОКС и другими сетями увеличивает потенциальные угрозы безопасности и подверженность сетей ОКС внешним атакам. Например, конвергенция телефонных сетей общего пользования и сети Интернет позволяет применять разные технологии взлома с учетом уязвимостей ОКС. Злоумышленник может модифицировать или перехватывать данные, а также вносить глобальные изменения в подсистему управления сигнализацией. Уязвимости в ОКС позволяют нарушать установление соединения, блокировать с большой степенью вероятности процесс передачи информации и управления сетью [2].

Атака на ОКС ОТКС и входящие в нее объекты может повлечь за собой непоправимые последствия – по нарушению целостности, доступности данных защищаемой ИВС как коммерческих, так и государственных организаций. Многие субъекты из категорий критической информационной инфраструктуры могут коммерческими. К примеру, атака на субъекты коммерческого здравоохранения или коммерческого транспорта может повлечь за собой человеческие жертвы.

Таким образом, причинами основных уязвимостей сетей ОКС является большое количество и сложность интерфейсов, использование новых сервисов, подключение к сети Интернет.

Вышеуказанным определяется актуальность исследования.

Изучение потенциальных угроз ИБ и их классификация необходимы для научно-обоснованного выбора мероприятий, методов, механизмов и средств обеспечения ИБ, а также для выявления наиболее опасных угроз, противодействовать которым должна система обеспечения ИБ сети ОКС.

В задачу обеспечения ИБ сетей ОКС входит защита их функционирования от угроз безопасности и защита программно-аппаратного обеспечения сетей ОКС, так как основным источником отказов сети являются ошибки в программном обеспечении реализации ОКС. Необходимо с высокой достоверностью определять факты удаленных атак. Признаками наличия атак являются несанкционированные цифровые последовательности, путем выявления которых реализуется обнаружение преднамеренных деструктивных воздействий.

Методы исследования базируются на положениях теории вероятности, математического моделирования, теории системного анализа и методологии теории рисков.

В работе будут разрабатываться риск-модели для экстремальных значений критических переменных состояния. В сравнении с порогами их допустимости оцениваются ожидаемые ущербы и вероятности их возникновения [3].

Современные методологии риск - анализа систем сейчас во многом ориентированы на анализ ущербов. В этой связи будет сделана попытка осуществить оценку переменных состояния. Динамика критических переменных и ее прогнозирование обязательны для мониторинга систем, функционирующих в реальном времени, в том числе объектов критической инфраструктуры.

Следующим шагом описывается линейная модель, а затем находится ущерб в нормированном виде и рассчитывается риски, определяется дискретизация значений КПС, повышается ее точность. Приводятся альтернативные варианты подхода к дискретизации на основе математического ожидания. Рассматриваются параметры и характеристики риска одной из переменных состояния. После этого рассчитывается оценка риска для множества переменных состояния, затем проводится Аналитическая оценка функций чувствительности критичных переменных состояния. Все методы подкрепляются формулами и графиками.

Заключительным этапом является управление рисками атакуемой информационно-технологической инфраструктуры критически важных объектов, т.е. рассматриваются аспекты управления рисками превышения критичных переменных состояния пороговых значений кризисного диапазона для информационно-технологической инфраструктуры критически важного объекта.

Исследование проведено в соответствии с темой диссертационной работы, целью исследования и поставленной научной задачей.

По результатам проведенного в рамках диссертационной работы научного исследования получен ряд новых, взаимосвязанных теоретических и практических результатов, позволяющих утверждать, что актуальная научная задача решена.

В соответствии с целями исследования в работе решены следующие частные задачи:

1. Проведенный анализ условий построения и функционирования ИТКС в подведомственном учреждении исполнительного органа государственной власти показал, что назрела необходимость разрешения противоречия между возникновением необходимости существующей ИТКС для решения специфических трудоемких задач, связанных с выполнением поставленных перед ней задач и обеспечением безопасности ресурсов сети в условиях воздействий нарушителей на ОКС;

2. В работе показано что, при функционировании существующей ИТКС появляются новые и приобретают более значимое значение угрозы информации. При этом нарушитель имеет возможность реализовывать несанкционированное воздействие на систему обработки, хранения и передачи данных. Реализуя НСВ на ИТКС, нарушитель действует на ОКС, выполняет свои стратегии по нарушению функционирования ОКС, целью которой является нарушение доступности ресурсов сети. Что приведет к нарушению функционирования ИТКС и, следовательно, к невыполнению поставленных перед нею задач.

3. Анализ традиционных средств и систем защиты информации показал, что их многообразие и большое количество не могут в полной мере обеспечить функционирование ИТКС, требуется подробное рассмотрение условий реализации того или иного воздействия с целью формирования рекомендаций и способов по обеспечению безопасности информации;

4. На основе анализа статистических данных по реализации угроз на уязвимые места ИТКС - ОКС ИТКС сделан вывод о месте НСВ на ОКС, нарушающего доступность информации, циркулирующей в ИТКС;

5. Разработана вероятно-временная модель функционирования ИТКС в условиях НСВ нарушителя на ОКС. Модель отличается от известных тем, что в ней учитываются возможные воздействия нарушителя на ОКС ИТКС и зависимость показателей защищенности ИТКС от параметров ОКС.

На основе модели была разработана методика оценки защищенности ИТКС; была проведена оценка защищенности ИТКС. Выявлено, что чем больше времени нарушитель тратит на осуществление компрометации системы защиты ИТКС, тем выше вероятность того, что ИТКС будет функционировать с требуемым качеством в течение заданного времени. Доказано что, чем меньше времени система защиты тратит на обнаружение НСВ на ИТКС, тем выше вероятность того, что ИТКС будет функционировать с требуемым качеством.

6. Определен показатель защищенности ИТКС при НСВ – вероятность функционирования ИТКС с требуемой эффективностью в течение заданного времени в условиях НСВ нарушителя на ОКС. Разработан математический аппарат для его количественной оценки;

7.Разработаны функционально-логическая модель процесса защиты функционирования ИТКС от НСВ с учетом воздействий нарушителя на ОКС, алгоритм противодействия НСВ и рекомендации по практической реализации алгоритма противодействия НСВ в условиях различного вида воздействий нарушителя на ОКС. Модель отличается от известных тем, что в ней учитываются протоколы ОКС и ЦП, циркулирующий в ней, и возможные воздействия нарушителя на зависимость на них.

Для решения задач вскрытия стратегий нарушителя по воздействию на ИТКС, анализа и распознавания нарушений нарушителя протоколов ИТКС и ОКС разработаны обобщенные модели физической и функционально-логической архитектур защищаемой сети и частные модели топологии, уровневых протоколов ИТКС и ОКС.

8. На основе разработанной модели и методики предложен алгоритм безопасного функционирования ИТКС, разработаны алгоритмы работы системы защиты ОКС при функционировании ИТКС в различных режимах: режиме «отчетов», режиме «запросов и отчетов» и режиме «централизованного запроса»;

9. Предложены рекомендации по типовому построению сегментов ИТКС;

10. Сформулированы научно-технические предложения по повышению защиты ИТКС с ОКС на основе способов распознавания искажений управляющей и протокольной информации, выявления НСВ с использованием признаков ЦП и протоколов:

А. Способ обнаружения НСВ нарушителя на управляющую и протокольную информацию, циркулирующую в ОКС ИТКС;

Б. Устройство, реализующее способ распознавания искажения ЦП в ОКС;

В. Способ защиты ОКС ИТКС от НСВ нарушителя;

Г. Способ контроля ЦП ОКС в ИТКС;

Д. Способ контроля состояния ОКС ИТКС как многопараметрического объекта.

Предлагаемые научно-технические предложения направлены на уменьшение (сокращение) среднего времени обнаружения НСВ нарушителя на ОКС, при этом увеличивается вероятность функционирования ИТКС с требуемым качеством.

Новизна предложений заключается в обеспечении повышения степени защищенности ИТКС в условиях воздействия нарушителя на ОКС ИТКС;

11. Проведена оценка эффективности научно-технических предложений с помощью разработанной методики оценки защищенности, применив, в качестве исходных данных, данные, используемые для оценки защищенности типовой ИТКС. Эффективность увеличивается за счет сокращения среднего времени реакции СЗ ОКС ИТКС на НСВ нарушителя. При этом увеличивается вероятность функционирования ИТКС с требуемым качеством.

Анализ затрат на реализацию научно-технических предложений показал, что их уровень не превышает выделенных средств для достижения поставленной цели по обеспечению защищенности ИТКС от НСВ нарушителя на ОКС.

Достоверность научных результатов, полученных в диссертационной работе, обеспечивается и подтверждается значительной совокупностью взаимосвязанных факторов, среди которых: способы решения сформулированных в работе задач опираются на общепринятые научные методы (в работе в основном использованы методы теории вероятностей, теории распознавания образов (формальные грамматики), теории графов и теории массового обслуживания). А также системностью исследуемых вопросов на основе выбора многократно проверенных, в том числе и на практике, исходных данных, обоснованным введением ограничений и допущений, позволяющих выделить и исследовать основные факторы, влияющие на основы организации и обеспечения безопасного функционирования ИТКС при НСВ нарушителя на ОКС.

Результаты, полученные в диссертационной работе, не противоречат предшествующим исследованиям, но существенно их дополняют, расширяют и могут быть использованы при оценке безопасности информации, обрабатываемой в локальных вычислительных сетях.

Основные научные результаты диссертационных исследований апробированы в докладах на научно-технических семинарах и конференциях, опубликованы в печатных работах, а также будут использованы в интересах государства.

В дальнейшем результаты исследования можно будет применять в преподавании дисциплин по программам подготовки инженеров и преподавателей исследователей по специальностям 10.03.01 «Информационная безопасность» и 10.06.01 «Информационная безопасность», а также учитывать при внедрении в цифровую экономику.

В настоящее время основные результаты работы опубликованы в 11 печатных трудах, рецензируемых журналах ВАК, РИНЦ и Scopus [4-18].

Принимая во внимание, что данная диссертационная работа не в состоянии охватить весь спектр проблем, связанных с организацией и обеспечением работы ИТКС в качестве дальнейших направлений научных исследований целесообразно выделить следующие: оптимизация маршрутных обновлений; анализ и конфигурация метрик маршрутизации масштабируемых сетей; разработка и совершенствование аппаратурно-программных средств обеспечения безопасного функционирования ИТКС и др.

СПИСОК ЛИТЕРАТУРЫ

1. *Гойхман В.Ю., Гольдштейн Б.С., Сибирякова Н.Г.* Протоколы стека ОКС7: подсистема МАР. Серия «Телекоммуникационные протоколы». Книга 10. – СПб.: БХВ-Петербург, 2014. – 200 с.: ил.
2. *Глуховский М.Д., Сахаров Д.В.* К вопросам информационной безопасности SS7 в современном мире // В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020). IX Международная научно-техническая и научно-методическая конференция: сборник научных статей. Санкт-Петербург, 2020. С. 331-335.
3. *Ермилов Е.В.,* Анализ и управление рисками нарушения информационной безопасности критически важного объекта: автореферат дис. ... кандидата технических наук: 05.13.19 / Ермилов Евгений Викторович; [Место защиты: Воронеж. гос. техн. ун-т]. - Воронеж, 2014. - 17 с.
4. *Pavel Sh., Audrey K., Artem G., Ernest B.* A technique for detecting the substitution of a java-module of an information system prone to pharming with using a hidden embedding of a digital watermark resistant to decompilation // В сборнике: International Congress on Ultra Modern Telecommunications and Control Systems and Workshops. 13. Сер. "2021 13th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops, ICUMT 2021" 2021. С. 219-223.
5. *Сахаров Д.В., Красов А.В., Ушаков И.А., Бирих Э.В.* Моделирование защищенной масштабируемой сети предприятия с динамической маршрутизацией на основе ipv6 // Защита информации. Инсайд. 2020. № 1 (91). С. 51-57.
6. *Бирих Э.В., Гаврилов А.С., Сацук Е.Н.* Современные проблемы обеспечения внутренней безопасности распределенной сети органов государственной власти // В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018). VII Международная научно-техническая и научно-методическая конференция. Сборник научных статей. В 4-х томах. Под редакцией С.В. Бачевского. 2018. С. 104-107.
7. *Бирих Э.В., Кошурин А.Д., Кушнир Д.В., Стародубова Д.Д.* Исследование вопросов повышения уровня защищенности органов исполнительной власти // В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018). VII Международная научно-техническая и научно-методическая конференция. Сборник научных статей. В 4-х томах. Под редакцией С.В. Бачевского. 2018. С. 107-110.
8. *Бирих Э.В., Ферапонтова С.С.* К вопросу об аудите персональных данных // В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018). VII Международная научно-техническая и научно-методическая конференция. Сборник научных статей. В 4-х томах. Под редакцией С.В. Бачевского. 2018. С. 111-114.
9. *Бирих Э.В., Виткова Л.А., Сахаров Д.В., Шашкин В.С.* Алгоритмы BIG DATA и мониторинг ит инфраструктуры предприятия // В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2017). Сборник научных статей VI

Международной научно-технической и научно-методической конференции. В 4-х томах. Под редакцией С.В. Бачевского. 2017. С. 100-103.

10. *Бирих Э.В., Рябов Е.Ю., Сахаров Д.В.* Методология формирования модели угроз безопасности информационных систем // В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2017). Сборник научных статей VI Международной научно-технической и научно-методической конференции. В 4-х томах. Под редакцией С.В. Бачевского. 2017. С. 103-107.

11. *Бирих Э.В., Виткова Л.А., Гореленко В.В., Казаков Д.Б.* Защита информации в базах данных // В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2017). Сборник научных статей VI Международной научно-технической и научно-методической конференции. В 4-х томах. Под редакцией С.В. Бачевского. 2017. С. 89-92.

12. *Бирих Э.В., Виткова Л.А., Левин М.В., Чмутов М.В.* Развитие стандартов и руководств в сфере облачных технологий // В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2017). Сборник научных статей VI Международной научно-технической и научно-методической конференции. В 4-х томах. Под редакцией С.В. Бачевского. 2017. С. 92-95.

13. *Бирих Э.В., Виткова Л.А., Сахаров Д.В., Сергеева И.Ю.* Метод повышения безопасности распределенной вычислительной системы на базе СППР и с учетом прогнозирования состояния // В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2017). Сборник научных статей VI Международной научно-технической и научно-методической конференции. В 4-х томах. Под редакцией С.В. Бачевского. 2017. С. 96-100.

14. *Герлинг Е.Ю., Кулишкина Е.И., Бирих Э.В., Виткова Л.А.* Модели нарушителей информационной безопасности // Известия высших учебных заведений. Технология легкой промышленности. 2017. Т. 35. № 1. С. 27-30.

15. *Бирих Э.В., Сахаров Д.В.* Модель нарушителя распределенной информационно-вычислительной сети // В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании. сборник научных статей V международной научно-технической и научно-методической конференции. 2016. С. 235-238.

16. *Карев А.С., Бирих Э.В., Сахаров Д.В., Виткова Л.А.* Проблемы информационной безопасности в интернете вещей // В сборнике: Интернет вещей и 5G. 2016. С. 66-70.

17. *Бирих Э.В., Богомедова К.М., Сахаров Д. В.* Модель безопасности для медицинских коммерческих учреждений // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2023) : Сборник научных статей. XII Международная научно-техническая и научно-методическая конференция. В 4 т., Санкт-Петербург, 28 февраля – 01 марта 2023 года. Том 1. – Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2023. – С. 172-176.

18. *Бирих Э.В., Сахаров Д.В., Таров Е.В.* Применение криптографических методов защиты информации в открытых телекоммуникационных каналах связи // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2023) : Сборник научных статей. XII Международная научно-техническая и научно-методическая конференция. В 4 т., Санкт-Петербург, 28 февраля – 01 марта 2023 года. Том 1. – Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2023. – С. 177-180.

Голембиовский М.М.
Аспирант кафедры”СИБ”
Брянский государственный технический университет
maksim32region@yandex.ru

МОДЕЛИ И АЛГОРИТМЫ РАССЛЕДОВАНИЯ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В КОМПЬЮТЕРНЫХ СИСТЕМАХ

Аннотация: Аннотация проекта.

Проект выполняется в рамках национальной программы «Цифровая экономика Российской Федерации» (федеральные проекты "Информационная безопасность", "Искусственный интеллект").

Основным направлением является обеспечение информационной безопасности на основе отечественных разработок при передаче, обработке и хранении данных, гарантирующей защиту интересов личности, бизнеса и государства.

Проект направлен на разработку методики, позволяющей выявить следы инцидента информационной безопасности, ведущие к возможному злоумышленнику.

Ключевые слова: информационная безопасность, классификация инцидентов ИБ.

Целью исследования является повышение качества расследования компьютерных преступлений с помощью разработки частных моделей расследования.

Для достижения поставленной цели необходимо решить следующие задачи:

1. Разработать модель расследования инцидентов ИБ.
2. Разработать алгоритм расследования инцидентов ИБ.
3. Разработать детализированный подход к классификации инцидентов ИБ.
4. Разработать на основе предложенной классификации инцидентов ИБ частные модели расследования и сформулировать порядок компиляции уникальной методики.

Научная новизна диссертационного исследования заключается в следующем:

1.Разработана методика расследования инцидентов информационной безопасности в компьютерных системах, отличающаяся от известных с применением шкалы Харрингтона в отличие от известных ИБ.

2. Разработаны алгоритмы расследования инцидентов информационной безопасности в компьютерных системах, отличающиеся наличием новой классификации компьютерных инцидентов с подбором соответствующей модели расследования для каждого.

Основные положения, выносимые на защиту.

1. Модели и алгоритмы расследования инцидентов ИБ, обеспечивающие универсальность расследования инцидентов ИБ.
2. Классификация компьютерных преступлений и разработка частных моделей расследования инцидентов информационной безопасности в компьютерных системах, позволяющие оперативно реагировать на различные классы компьютерных преступлений (инцидентов ИБ) и поэтапно осуществить следственные действия, касаемые анализа устройств и данных.

Практическая значимость работы заключается в реализации предложенных моделей и алгоритмов расследования инцидентов информационной безопасности в компьютерных системах.

3. **Внедрение результатов работы.** Результаты диссертации использованы при выполнении следующих научно-исследовательских работ: Грант ИБ (Ордена Трудового Красного Знамени федеральное государственное бюджетное образовательное учреждение высшего образования «Московский технический университет связи и информатики») МТУСИ.

4. **Апробация результатов исследования.** Результаты, полученные в рамках работы над диссертацией, представлялись и обсуждались на следующих научно-методических конференциях:

1. V Юбилейной Международной научно-практической конференции. Брянск, 2023.
2. Информационная безопасность и защита персональных данных. Проблемы и пути их решения. XV межрегиональной научно-практической конференции.
3. Новые горизонты. X научно-практическая конференции с международным участием. Брянск.

Введение

Глобальная информатизация общества с каждым годом набирает обороты. Все большее количество данных переводится в электронный вид, в котором после хранится и обрабатывается. Это в свою очередь упрощает процесс их уничтожения или кражи и значительно усложняет процессы расследования подобных преступлений, поскольку данные действия нарушитель может совершить, не имея физического доступа к объекту.

Согласно статистике МВД, число киберпреступлений за 2021 поднялось на треть. По приведенной ведомством информации, злоумышленники на 39% чаще использовали мобильные сети для осуществления своих целей, а сеть интернет - на 51,3% чаще. Кроме того, наибольшая доля прироста показателей подобных преступлений зафиксирована в Северной Осетии (87%), а также в Севастополе - 77% и Тульской области - 71%. Ранее в СК заявили о росте уровня киберпреступности в 20 раз за семь лет.

Данная статистика показывает, что проблема расследования компьютерных инцидентов стоит очень остро. Необходимо внедрение новых подходов и методик.

Компьютерная криминалистика является относительно новым направлением как в правовом поле, так и в качестве ответвления сферы информационной безопасности. Тем не менее само понятие компьютерного преступления существует уже достаточно давно в Российской Федерации имеется ряд статей УК РФ, регламентирующих порядок их расследования и назначения наказаний (Ст. 272. Неправомерный доступ к компьютерной информации и другие), а также рекомендации по проведению процедуры расследования.

Во введении обоснована актуальность темы диссертации, сформулированы цели и задачи исследования, определена научная новизна работы, излагается краткое содержание каждой главы работы.

В первой главе основной части проведен обзор нормативно-правовой базы, научных статей и диссертационных работ в области компьютерной криминалистики.

В рамках данной главы отмечено, что за на основе анализа существующих моделей и алгоритмов расследования инцидентов информационной безопасности, можно сделать вывод, о том, что на данный момент времени нет единой методики, содержащей структурированный подход к расследованию, учитывающей одновременно все необходимые аспекты. Предложенные механизмы разрозненны и их использование в рамках предприятий затруднительно. В то время как вопрос борьбы с инцидентами неуклонно набирает

актуальность. Общемировая обстановка и экономический кризис оказывают непосредственное влияние на то, что вопрос обнаружения, расследования и системной борьбы с инцидентами информационной безопасности становится важным не только для крупномасштабных объектов, но и для предприятий среднего и малого масштаба. В стране реализуется непростой, но необходимый период импортозамещения в сфере защиты информации, многие предприятия перестраивают порядок защиты своих активов и совпадение данного переходного периода с возросшим количеством попыток реализации кибератак делает как никогда актуальной необходимость разработки методики по расследованию инцидентов ИБ.

Во второй главе диссертации основной части разработана методика предотвращения и расследования компьютерных преступлений. Также приведены практические инструкции методов расследования согласно алгоритму.

Рисунок 1 — Алгоритм расследования компьютерного преступления

Для более четкого понимания поэтапности процессов специфичных для расследования компьютерных преступлений (инцидента ИБ), предлагается общая модель и алгоритм расследования, выполняемого с привлечением специалистов в области информационной безопасности.

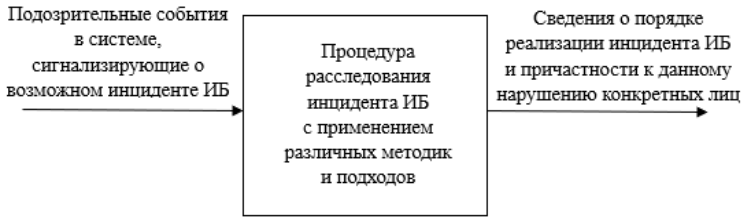


Рисунок 2 — Общая модель расследования компьютерного преступления

В пункте практические инструкции методов расследования согласно алгоритму, представлены более подробные инструкции для каждого этапа расследования, приведены рекомендуемые к использованию программные средства и утилиты.

Модель и алгоритм приведенного расследования показывают, что методика предотвращения и расследования компьютерных преступлений вносит больше точности для получения сведений при расследовании компьютерных инцидентов.

Третья глава диссертации описывает классификацию компьютерных преступлений и разработку частных моделей расследования.

Предлагаемая классификация и модель расследования включает идентификацию, определение, отслеживание, формирование отчета, результат исследования. Пример представлен на рисунке 3.

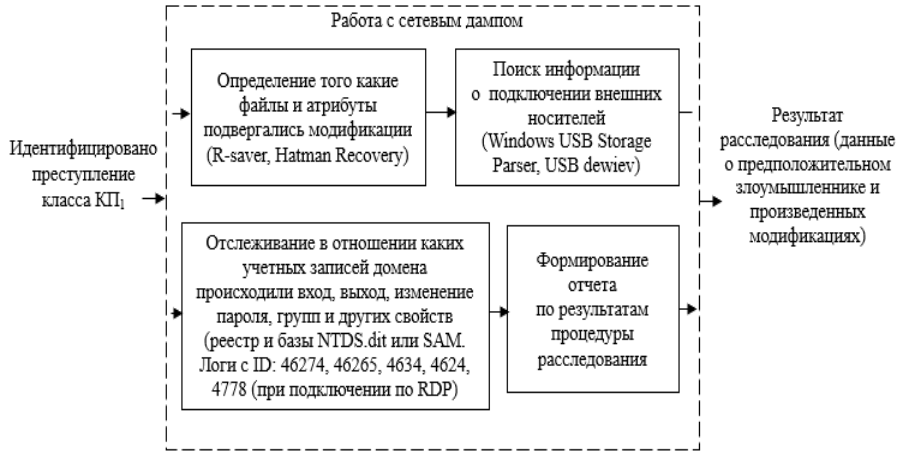


Рисунок 3 — Модель расследования преступления класса КП 1

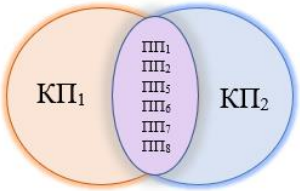
Классификация состоит из следующих параметров:

1. Класс преступления (КП).
2. Подкласс преступления (ПП).
3. Пример из судебной практики.
4. Модель расследования преступления.

Разработан порядок выбора алгоритма расследования компьютерного преступления (инцидента ИБ).

Классы преступлений КП1 – КП10 являются пересекающимися множествами.

$A \cap B = \{x \mid x \in A \wedge x \in B\}$, где x – ПП1-ПП8, А и В – КП1-КП10.



То есть их составляющие – подклассы ПП1 - ПП8 могут входить в несколько классов одновременно. После того, как выявлен подкласс преступления необходимо в соответствии с таблицей (рисунок 6) определить к какому классу он относится. В случае если подкласс относится к нескольким классам – из них выделяется один наиболее подходящий в зависимости от выявленных последствий преступления. При невозможности выделить только один класс, процедура расследования строится за счет компиляции средств и методов расследования каждого из подходящих классов.

Подкласс преступления (ПП) определяется в начале расследования за счет оценки отдельных, указывающих на него критериев. Для каждого критерия необходимо вычислить показатель его важности.

Важность отдельных критериев подклассов компьютерных преступлений определяется несколькими факторами и может быть определена путем внедрения весовой функции Z. Z есть монотонно возрастающая функция таких аргументов как Ок – опасность критерия и Ак – актуальность критерия. Чем выше значение показателей, тем больше важность рассматриваемого критерия.

Методика расследования компьютерного преступления включает в себя следующие этапы:

1. Анкетирование пользователя для сбора исходных данных об объекте, позволяющих оценить вероятность реализации факторов риска отдельных критериев.

2. Расчёт показателя Z_k по каждому из существующих критериев.

3. Расчёт показателя P (вероятность реализации компьютерного преступления).

4. Формирование рекомендаций по расследованию компьютерного преступления.

5. Формирование рекомендаций по нейтрализации (или значительному снижению) вероятности реализации компьютерного преступления.

На основании результатов работы с данной методикой можно будет сделать вывод о том, почему произошло (может произойти) преступление и какие методики будут наиболее эффективны для его расследования.

В **четвертой главе представлены модели и алгоритмы расследования инцидентов информационной безопасности в компьютерных системах**

Ключевая цель разработки, – сокращение количества инцидентов ИБ на предприятии.

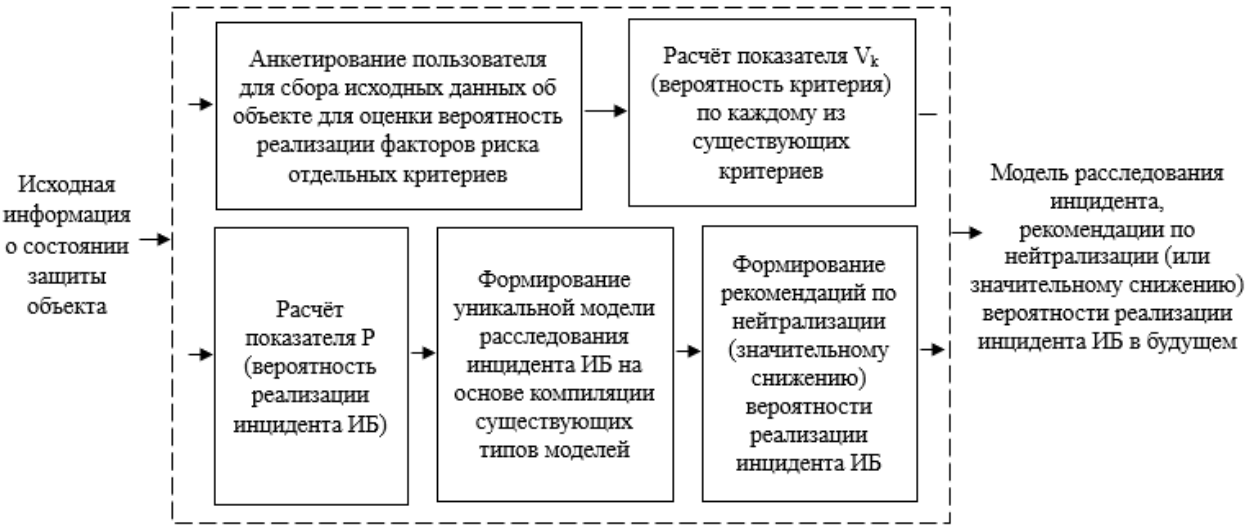


Рисунок 4 — Структурная модель формирования этапов расследования инцидентов ИБ

СПИСОК ЛИТЕРАТУРЫ

1. Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и средства / Шаньгин В.Ф.. — Саратов : Профобразование, 2019. — 543 c. — ISBN 978-5-4488-0074-0.
2. Селезнев А.В. Современные проблемы криминалистики: учебное пособие / Селезнев А.В., Сысоев Э.В.. — Тамбов : Тамбовский государственный технический университет, ЭБС АСВ, 2012. — 160 c.
3. Мальцагов, И. Д. Современные технологии в расследовании преступлений: компьютерная криминалистика / И. Д. Мальцагов // Экономика. Бизнес. Право. – 2018. – № 4-6(26). – С. 44-48.
4. Шевченко Е.С. Тактика производства следственных действий при расследовании киберпреступлений[Электронный ресурс] – URL:https://www.dissercat.com/content/taktika-proizvodstva-sledstvennykh-deistvii-pri-rassledovanii-kiberprestuplenii

(Дата обращения: 8.07.2022).

5. Баранов В.А. Обнаружение инцидентов информационной безопасности как разладки процесса функционирования системы [Электронный ресурс] – URL: https://www.dissercat.com/content/modeli-i-algoritmy-kontrolya-intsidentov-informatsionnoi-bezopasnosti-v-korporativnoi-teleko (Дата обращения: 10.07.2022).
6. Кришталюк, А. Н. Правовые аспекты системы безопасности: курс лекций / А. Н. Кришталюк. — Орел: Межрегиональная Академия безопасности и выживания (МАБИВ), 2014. — 204 c.
7. Монахова М.М. Модели и алгоритмы контроля инцидентов информационной безопасности в корпоративной телекоммуникационной сети [Электронный ресурс] – URL: https://www.dissercat.com/content/modeli-i-algoritmy-kontrolya-intsidentov-informatsionnoi-bezopasnosti-v-korporativnoi-teleko (Дата обращения: 8.07.2022).
8. Майорова, Е. В. Методические аспекты реагирования на инциденты информационной безопасности в условиях цифровой экономики / Е. В. Майорова // Петербургский экономический журнал. – 2020. – № 1. – С. 155-162.

9. Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации, 30.05.2014 г.
10. Ваценко, А. А. Обзор техник компьютерной криминалистики / А. А. Ваценко // Бюллетень науки и практики. – 2020. – Т. 6. – № 6. – С. 167-174.

Домуховский Н.А.
Уральский федеральный университет, младший научный сотрудник,
N.A.Domukhovsky@urfu.ru

РАЗРАБОТКА МЕТОДИКИ ОЦЕНКИ УРОВНЯ ЗАЩИЩЕННОСТИ КОМПЬЮТЕРНЫХ СИСТЕМ ПУТЕМ МОДЕЛИРОВАНИЯ КОМПЛЕКСНЫХ АТАК

Аннотация: в работе рассматривается метод проектирования киберзащищенных автоматизированных систем управления технологическими процессами (АСУ ТП), основанный на построении модели создаваемой АСУ ТП с последующим анализом возможных действий нарушителя информационной безопасности (ИБ), которые могут привести к ущербу для всей системы. Приводится описания методов моделирования комплексных атак на АСУ ТП, вычисления ожидаемого ущерба, определения наиболее вероятных действий нарушителя на основе многокритериальной оптимизации оценок, отражающих эффективность элементарной атаки.

Ключевые слова: кибербезопасность, анализ рисков, моделирование безопасности, оценка ущерба.

Чтобы создать защищенную систему, необходимо еще на самых ранних этапах ее разработки определить оптимальный состав мер, который нейтрализует все основные сценарии реализации угроз информационной безопасности (ИБ) в отношении системы. Фактически в данном случае речь идет о многокритериальной оптимизационной задаче – задаче Парето[1]: состав защитных мер с одной стороны влияет на стоимость разработки системы, количество потребляемых ресурсов (вычислительных, хранения и пр.), а в некоторых ситуациях это еще и ухудшение показателей назначения создаваемой системы (увеличение времени передачи сигнала, ограничение доступных функций для пользователя и пр.). С другой стороны – недостаток защитных мер создает вероятность того, что системе будет нанесен ущерб действиями злоумышленника, т.е. влияет на ожидаемый размер ущерба системе.

Таким образом, упрощенно оптимизационную задачу создания автоматизированной системы в защищенном исполнении можно сформулировать следующим образом: определить оптимальный состав защитных мер (с точки зрения стоимости, количества, влияния на систему), которые снижают математическое ожидание ущерба от действий нарушителя до приемлемого уровня.

ГОСТ Р 56939 «Защита информации. Разработка безопасного программного обеспечения. Общие требования» определяет как один из этапов разработки архитектуры системы и требований к безопасности – выполнение процедуры моделирования угроз ИБ [2]. Однако стандарт не определяет конкретный метод моделирования угроз ИБ, оставляя это решение на усмотрение разработчика системы.

Представленная работа содержит описание метода моделирования угроз и расчета ожидаемого уровня потерь (для последующего подбора защитных мер), который реализует требования к процедуре моделирования угроз, определяемой в [2].

Вопросам моделирования угроз при разработке безопасного ПО посвящена книга Адама Шостака[3], где автор описывает 4 шага, которые должны присутствовать в процессе моделирования угроз:

- описание анализируемой системы (ответ на вопрос: что мы создаем?);

- описание возможных угроз системе (ответ на вопрос: что может пойти не так?);
- применение контрмер для нейтрализации угроз (ответ на вопрос: что можно сделать с тем, что может пойти не так?);
- валидация результата (ответ на вопрос: в полной мере ли мы провели анализ возможных угроз?).

В качестве основного недостатка автор упомянул низкую степень автоматизации каждого из перечисленных шагов, что при увеличении сложности создаваемых систем, приводит к недостаточному уровню их защищенности.

Целью настоящей работы является разработка методов, автоматизирующих анализ возможных угроз ИБ в отношении создаваемых автоматизированных систем управления технологическими процессами (АСУ ТП). При этом методы должны быть универсальны по отношению к анализируемой АСУ ТП, минимально зависеть от оценок экспертов, позволять учитывать комплексные атаки, включающие множество действий нарушителя.

Метод включает следующие шаги:

- определение исходных данных: компонентов системы, их взаимосвязи, уязвимостей компонентов, реализованных защитных мерах;
- описание деревьев неисправностей [4], позволяющих определить степень ущерба моделируемой системе, в зависимости от проведенных атак в отношении отдельных компонент системы;
- моделирование (симуляция) действий нарушителя для заданных параметров нарушителя (начальное положение, доступные элементарные вредоносные воздействия и пр.) – определение математического ожидания размера ущерба системе для заданных архитектуры и размещения средств защиты информации;
- расчет эффективности средств защиты информации для формирования оптимального состава защитных мер для системы в целом.

Исходные данные для метода включают два класса информации: первый – это справочная информация, содержащая сведения и экспертные оценки, не относящиеся к конкретным системам. Сюда входят типовые компоненты систем (как программные, так и аппаратные), каталог уязвимостей (при этом используются публичные каталоги уязвимостей, например, Банк данных угроз и уязвимостей ФСТЭК России [5]) и связанные с ними оценки (которые могут опираться на оценки внешних баз данных, например, Common Vulnerability Scoring System[6] или определяться экспертом).

Второй класс данных включает сведения о конкретной анализируемой АСУ ТП. Сюда входит информация об архитектуре системы: составе ее компонентов и связях между ними, а также структура дерева неисправностей системы, позволяющая определить совокупный ущерб системе на основе информации об исходах элементарных атак.

Архитектура системы представляется в виде неориентированного взвешенного графа, в котором в качестве вершин выступают компоненты системы, а в качестве ребер – отношения между компонентами. Ребра нулевого веса соответствуют компонентам, которые размещены на одном средстве вычислительной техники (например, сервер, на котором установлена ОС и ПО – SCADA), ребра единичного веса соответствуют компонентам, размещенным в одном сетевом сегменте, а ребрам с весом $+\infty$ соответствуют компоненты, расположенные в одном физическом объекте. Пример графа, описывающего архитектуру системы, представлен на Рис. 1.

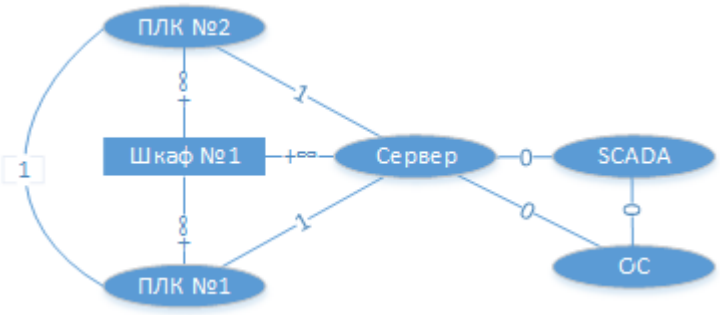


Рис. 1. Пример графа связности системы. Здесь «ПЛК №1», «ПЛК №2» и «Сервер» – компоненты, размещенные в физическом расположении «Шкаф №1». Также указанные компоненты логически связаны (размещены в одном сетевом сегменте), а на сервере установлено ПО: некоторая операционная система и SCADA – соответственно эти компоненты имеют локальную связность

Дерево неисправностей содержит сведения о негативных последствиях реализации той или иной уязвимости в отношении компонентов системы (например, отказ компонента или ограничение выполнения какой-то его функции) в качестве базовых событий. Эксперт, обладающий знанием о работе анализируемой АСУ ТП, далее строит развитие базовых событий в промежуточные и корневое событие, а также он должен представить оценку ущерба при наступлении каждого из событий. Пример дерева неисправностей приведен на Рис. 2.

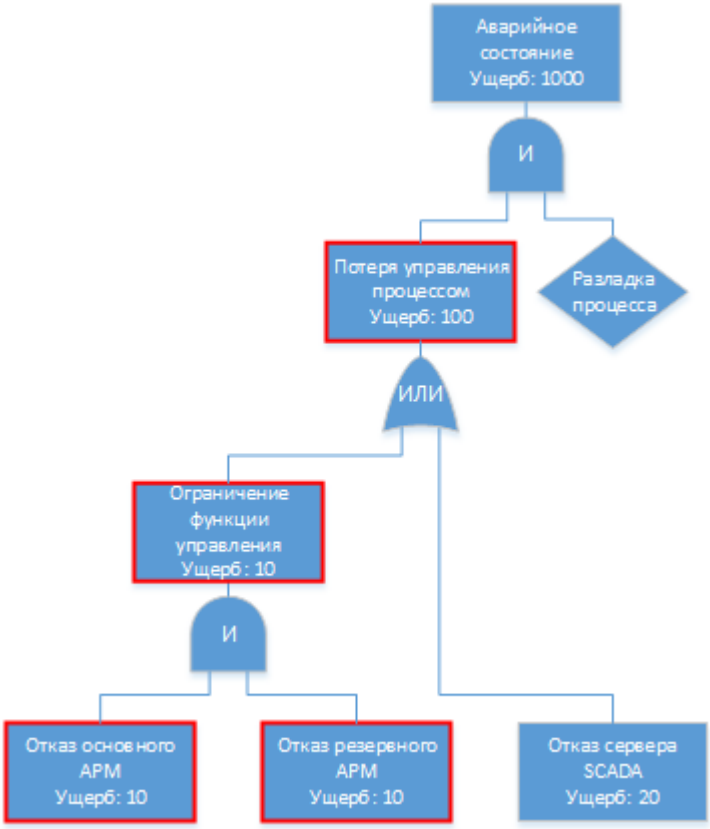


Рис. 2. Пример дерева неисправностей для моделирования размера ущерба системе. Красной рамкой выделены события, наступившие в результате атаки нарушителя. Наступление базовых событий «Отказ основного АРМ» и «Отказ резервного АРМ» вызвано действиями нарушителя. Промежуточные события «Ограничение функции управления» и «Потеря управления процессом» наступают вследствие выполнения условий соответствующего логического вентиля. Событие «Разладка процесса» является внешним – если оно наступает, то это приводит к наступлению корневого события «Аварийное состояние»

На основе справочников о типовых уязвимостях и графе связности системы производится построение графа атак (развитие концепции дерева атак, представленного в [7]) по алгоритму, описанному в [8]. Граф атак позволяет объединить сведения о реальной топологии системы, условия для эксплуатации той или иной уязвимости в отношении конкретного актива, а также о последствиях ее реализации, что позволяет рассматривать на графе атак комплексные атаки, включающие эксплуатацию нескольких уязвимостей в отношении различных компонентов системы. Граф атак – ориентированный мультиграф $G=(V,E)$, где $V=A\times AV\times PR\times ST$ – описание состояния компонента системы, A-множество компонентов, AV – текущий вектор атаки нарушителя в отношении компонента (в соответствии с [6]), PR – текущий уровень привилегий нарушителя на этом компоненте (в соответствии с [6]), ST – состояние компонента после эксплуатации уязвимости (в простейшем случае может принимать только 2 значения: компонент исправен и компонент находится в состоянии отказа). Дуги графа атак символизируют элементарную атаку – эксплуатацию уязвимости v. Пример графа атак приведен на Рис. 3.

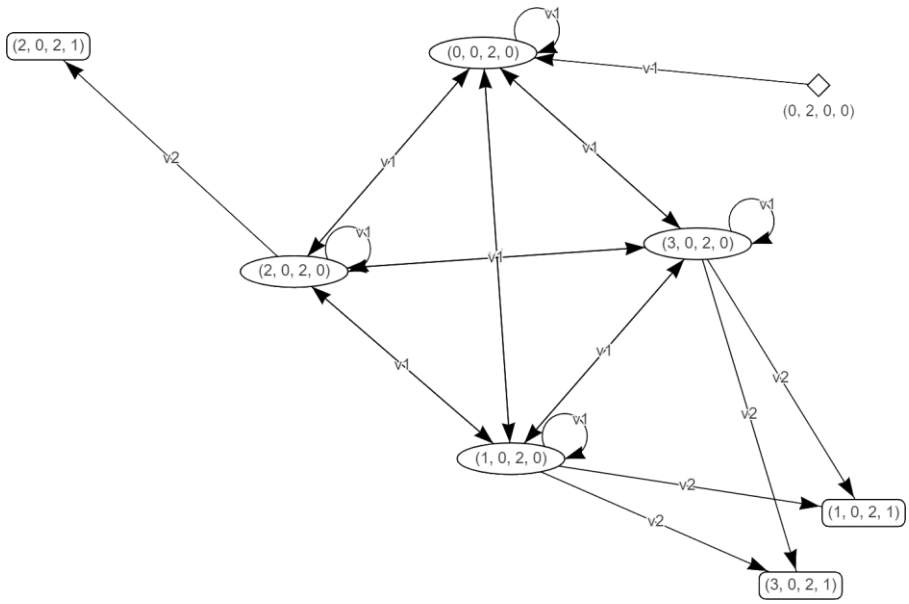


Рис. 3. Пример графа атак. Компоненты и из состояния описаны числовыми кодами, уязвимости, соответствующие дугам обозначены как v_i. Ромбовидная вершина символизирует стартовую позицию нарушителя, прямоугольные вершины символизируют достижения состояния отказа соответствубющего компонента

С каждой уязвимостью связан ряд параметров, определяемых экспертом или на основе значения параметров CVSS: это вероятность успешной эксплуатации уязвимости c_1, вероятность обнаружения попытки эксплуатации уязвимости c_2, ожидаемое время обнаружения успешной эксплуатации уязвимости в отношении компонента c_3, ожидаемое время восстановления компонента c_4 и ожидаемое время, затрачиваемое нарушителем, на эксплуатацию уязвимости c_5. Вектор (c_1,c_2,c_3,c_4,c_5) является весовой функцией для задачи многкритериальной оптимизации поиска оптимальной цепочки атак в отношении заданного компонента системы. При этом для различных компонентов этой векторной весовой функции решается различная оптимизационная задача: для вероятностей предполагается независимость исходов элементарных атак, соответственно для c_1 оптимизационным критерием является максимальное произведение (MAXPROD), а для c_2 – минимальное

произведение (MINPROD). Для времени обнаружения атаки на компонент принимается критерий наиболее широкого пути (MAXMIN) – так как нарушителю требуется как можно дольше проводить свою атаку незамеченным, чтобы максимизировать шансы нанесения наибольшего ущерба. Аналогичный критерий оптимизации применяется для время восстановления компонента (c_4). Для времени атаки применяется критерий MINSUM – т.е. общее время комплексной атаки должно быть минимальным.

Для решения задачи многокритериальной оптимизации предполагается, что компоненты весовой функции $(c_1, c_2, c_3, c_4, c_5)$ имеют лексикографический порядок, т.е. компоненты, стоящие в начале вектора имеют вес заведомо более высокий, чем компоненты, расположенные правее.

Известно, что для многокритериальной лексикографической дискретной задачи оптимизации можно построить функцию свертки, которая сведет многокритериальную задачу к однокритериальной [9]. Однако для реализации подхода, представленного в [9] отдельные задачи оптимизации должны быть задачами поиска оптимальной суммы (MINSUM или MAXSUM). Поэтому для критериев c_3 и c_4 необходимо дополнительно воспользоваться алгоритмом, приведенным в [10] для сведения задачи MAXMIN к задаче MAXSUM. Таким образом, итоговый граф атак представляет собой взвешенный ориентированный мультиграф со скалярной весовой функцией.

Для определения наиболее вероятных действий нарушителя на следующем шаге рассчитывается значение весовой функции комплексной атаки для атак, соответствующих достижению базовых событий дерева неисправностей. После чего для дерева неисправностей определяется минимальное сечение с максимальным совокупным весом, например, с использованием алгоритма MOCUS [11].

Далее для нарушителя строится оптимальная кампания атаки по алгоритму, описанному в [12] и в последствии выполняются симуляции действий нарушителя на графе атак с целью определения функции распределения ущерба системе в целом.

Описанный метод реализован в программном продукте для анализа рисков информационной безопасности АСУ ТП.

В рамках дальнейшей разработки планируется добавление функций определения наиболее уязвимых мест системы (тех компонентов, через которые проходит набольшее количество цепочек атак) и определения оптимального состава средств защиты информации (снижающих ущерб до приемлемого уровня при минимальной совокупной стоимости).

Основными положениями, выносимыми на защиту, по итогам реализации проекта являются:

1. метод представления компьютерной системы в виде графа атак для возможности отображения комплексных атак, включая физические атаки;
2. метод многокритериальной оптимизации комплексной атаки нарушителя, позволяющий выявить наиболее вероятные направления атак нарушителя;
3. метод определения ожидаемого уровня ущерба от реализации комплексной атаки в отношении моделируемой системы;
4. метод количественной оценки рисков для конкретной системы, учитывающий ее архитектуру и степень влияния базовых событий на ущерб системе в целом.

СПИСОК ЛИТЕРАТУРЫ

1. Sawaragi Y., NAKAYAMA H., TANINO T. Theory of Multiobjective Optimization / Y. Sawaragi, H. NAKAYAMA, T. TANINO, Elsevier Science, 1985. 320 c.
2. ГОСТ Р 56939 Защита информации. Разработка безопасного программного обеспечения. Общие положения Москва: Стандартинформ, 2016.
3. Shostack A. Threat modeling: designing for security / A. Shostack, Indianapolis, IN: Wiley, 2014. 590 c.
4. ГОСТ Р 27.302-2009 Надежность в технике. Анализ дерева неисправностей Москва: Стандартинформ, 2012.
5. БДУ ФСТЭК России [Электронный ресурс]. URL: https://bdu.fstec.ru/ (дата обращения: 28.04.2023).
6. CVSS v3.1 Specification Document // FIRST — Forum of Incident Response and Security Teams [Электронный ресурс]. URL: https://www.first.org/cvss/v3.1/specification-document (дата обращения: 26.08.2022).
7. Schneier B. Attack trees - modeling security threats // Dr. Dobb’s Journal. 1999. (24).
8. Domukhovskii N. Optimal Attack Chain Building Algorithm 2022.С. 317–319.
9. Бондаренко В. А., Клоеден П. Е., Краснов М. В. О Лексикографической Оптимизации В Многокритериальных Дискретных Задачах // Автоматика И Телемеханика. 2000. № 2. С. 29–34.
10. Burkard R. E., Rendl F. Lexicographic bottleneck problems // Operations Research Letters. 1991. № 5 (10). С. 303–308.
11. Vatn J. Finding minimal cut sets in a fault tree // Reliability Engineering & System Safety. 1992. № 1 (36). С. 59–62.
12. Domukhovskii N. Best Computer System Attack Strategy Finding Method 2023.С. 286–288.

Жерлицын С.А.
КубГТУ, аспирант,
kpytoooooo@gmail.com

МЕТОДЫ ПОСТРОЕНИЯ СИСТЕМ БИОМЕТРИЧЕСКОЙ ИДЕНТИФИКАЦИИ ЛИЧНОСТИ ДЛЯ РАСПРЕДЕЛЕННЫХ СИСТЕМ.

Аннотация: в данной работе описывается система биометрической идентификации личности, пригодной для эксплуатации в распределенных информационных системах. Описываются основные цели исследования, а также задачи, поставленные в ходе разработки. В качестве основных задач исследования выделяется непосредственно разработка модулей для идентификации личности по рисунку вен ладони, сетчатке и радужке глаза, отпечатку пальца, геометрии лица, клавиатурному и экранному почерку и другим биометрическим характеристикам. Приводится описание основных механизмов, методов и подходов, применяемых в ходе разработки. Для реализации опознающих нейросетевых модулей предлагается использовать глубокую нейронную сеть, структура которой зависит непосредственно от рассматриваемого биометрического идентификатора и включает в свой состав несколько компонентов: вариативную часть и общую. Архитектура вариативного компонента сети является индивидуальной для каждого отдельного типа идентификатора (рекуррентная для голоса и поведенческих признаков, свёрточная для рисунка вен ладони и т.д.), его цель состоит в первичной обработке предоставленного образца, удалении шумов и посторонней информации а также приведению выделенной информации к единому для всех видов идентификаторов формату карты признаков. Общая часть имеет единую архитектуру, но отличается весами от модуля к модулю, её задача заключается в установлении соответствия между полученной от вариативного блока карты признаков и пространством субъектов. Приводится решение основных проблем, связанных с удаленным применением нейросетевых алгоритмов в задачах обработки биометрии, характерных для работы с распределенными системами. Для реализации безопасного обмена биометрическими параметрами в условиях работы с удалённым сервером идентификации предлагается использовать систему полностью гомоморфного шифрования. Предлагается модульная архитектура системы, состоящая из нескольких блоков: модели, гибридизатор, модуль алгоритмов обучения, модуль тестирования, каждый из которых решает свою подзадачу. Также в исследовании представлены анализ современного состояния исследований в области, новизна предлагаемой методологии и ожидаемые научные результаты реализации проекта.

Ключевые слова: идентификация личности, биометрия, информационная безопасность, машинное обучение, искусственный интеллект, роевой интеллект, нейронные сети, анализ данных.

Основной целью исследования является разработка методов построения систем биометрической идентификации личности для распределенных систем, обладающих рядом свойств. Во главе данного списка находится надежность и безопасность, достигаемая путем построения защищенной централизованной архитектуры для идентификации личности, пригодной для применения в распределенных системах [1]. Также не менее важной характеристикой является унифицированный обобщенный механизм реализации

идентификации личности по биометрическим характеристикам разного вида в целях достижения масштабируемости, гибкости и единообразия.

В качестве основных задач исследования выделяется непосредственно разработка модулей для идентификации личности по рисунку вен ладони, сетчатке и радужке глаза, отпечатку пальца, геометрии лица, клавиатурному и экранному почерку и другим биометрическим характеристикам. Исследование способов повышения автономности нейросетевых систем для возможности безопасного применения на оконечных устройствах, в том числе защищенной системы удаленной обработки биометрических данных. Разработка системы автоматизированного обучения и дообучения опознающих модулей, программная и программно-аппаратная реализация оконечных устройств биометрической идентификации, а также централизованного сервера биометрической идентификации. Для надежного взаимодействия полученных компонентов выделяется этап разработки протокола авторизации на основе разработанных систем.

В числе последних тенденций развития механизмов аутентификации нельзя не выделить повышение спроса на методы, использующие биометрические характеристики субъекта [2, 3, 4]. Среди их особенностей можно выделить следующие пункты:

- неотъемлемость – носителем данных является сам человек, за счёт чего носитель нельзя забыть или потерять, за исключением критических случаев, зачастую опасных для здоровья;
- нечёткость – биометрические характеристики не всегда могут быть определены точно и имеют естественный диапазон допустимого колебания;
- невозможность перевыпуска – при компрометации данных такого типа становится невозможно использовать соответствующий тип биометрической аутентификации, так как злоумышленник сможет в любой момент получить выдать себя за истинного носителя.

Существует целый ряд публикаций, описывающих математический аппарат или детали реализации идентификации личности по тому или иному биометрическому параметру: на основе распознавания лиц [4], по рисунку вен ладони [5], по голосу [6], на основе анализа поведения [7] и многие другие. Однако ни в одной из них не решается задача унификации и разработки единого подхода к идентификации по нескольким различным биометрическим характеристикам.

Также в рамках исследования было проведен анализ способов идентификации личности по одной из биометрических характеристик – рисунку вен ладони. В данный момент существует 2 наиболее популярных метода идентификации личности по рисунку вен ладони: на основе вычисления расстояния (с учетом таких параметров, как косинусное расстояние, евклидово расстояние, масштабирование и поворот изображения на произвольный угол) и графовый метод.

Недостатками данных методов являются высокая вычислительная сложность при эксплуатации из-за необходимости сравнения предъявленного образца с каждым из эталонных изображений, необходимость доступа к базе эталонных биометрических данных при прохождении процедуры идентификации и зависимость от качества освещения, угла и изгиба ладони, зашумлённости изображения, фона, общая неустойчивость работы [8].

В исследовании Р. Фуксис [9] представлена информация по изучению влияния типа освещения руки на качество изображения (отражение и пропускание): схема пропускания

более громоздка в реализации, однако полученные изображения отличаются более высокой контрастностью и точностью.

Предложенные в исследовании методы были построены на основе ресурсоёмких математический преобразований по нахождению сходства исходного изображения с элементарными фильтрами, вследствие чего полученная система для успешного сопоставления нуждалась в хранении некого шаблона, идеального образца, по которому и вычисляется проверка личности. При данном подходе сокращается время обучения модели, однако не применяются последние достижения машинного обучения: элементарные фильтры составляются вручную, в следствие чего создаётся жёсткая завязка программной и аппаратной реализаций, повышается прихотливость и неустойчивость работы модели, затрудняется процесс модернизации и модификации.

Для реализации опознающих нейросетевых модулей предлагается использовать глубокую нейронную сеть, структура которой зависит непосредственно от рассматриваемого биометрического идентификатора и включает в свой состав несколько компонентов: вариативную часть и общую. Архитектура вариативного компонента сети является индивидуальной для каждого отдельного типа идентификатора (рекуррентная для голоса и поведенческих признаков, свёрточная для рисунка вен ладони и т.д.), его цель состоит в первичной обработке предоставленного образца, удалении шумов и посторонней информации а также приведению выделенной информации к единому для всех видов идентификаторов формату карты признаков. Общая часть имеет единую архитектуру, но отличается весами от модуля к модулю, её задача заключается в установлении соответствия между полученной от вариативного блока карты признаков и пространством субъектов.

Наглядно рассмотреть вариативность входных данных можно на примере двух изображений рисунка вен ладони, снятого с помощью разработанного в ходе исследование программно-аппаратного комплекса, у одного и того же субъекта в разное время.

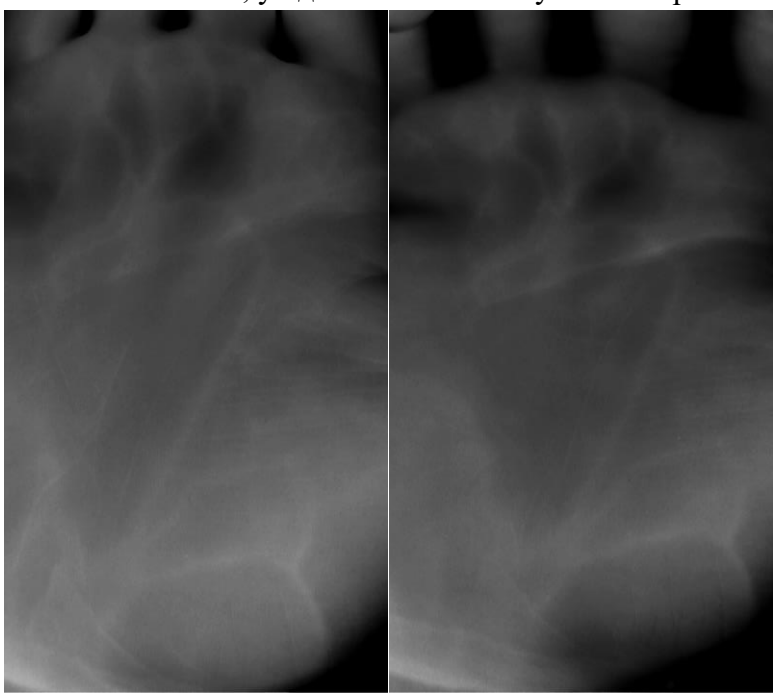


Рис.1 – Снимки рисунка вен ладони одного субъекта, снятые с помощью разработанного программно-аппаратного комплекса

Как можно заметить, изображение имеет неравномерные нелинейные геометрические деформации, посторонние шумы и изменчивые уровни контрастности на отдельных

фрагментах, что затрудняет применение классических способов распознания и сопоставления, понижая их эффективность. Аналогичная особенность возникает при рассмотрении практически каждого биометрического фактора, что и привело к разработке единого подхода к биометрической идентификации.

В силу изменчивости как самих биометрических идентификаторов, так и набора пользователей системы, для недопущения деградации её надёжности и эффективности необходима система автоматизированного обучения и дообучения распознающих модулей. Для реализации данной системы предлагается использовать модульную систему автоматизированного машинного обучения с применением как классических, так и эвристических алгоритмов. Предложенная система состоит из нескольких блоков: модели, гибридизатор, модуль алгоритмов обучения, модуль тестирования, каждый из которых решает свою подзадачу. Отдельно стоит обратить внимание на модуль гибридизации, позволяющий вносить изменения как в способ обучения модели, так и в её строение, если показатели точности по результатам проверок в модуле тестирования перестают расти. Особенно эффективно раскрываются в данной системе алгоритмы роевого интеллекта, также включенные в модуль алгоритмов обучения в силу простоты их гибридизации и адаптивности.

Для реализации безопасного обмена биометрическими параметрами в условиях работы с удалённым сервером идентификации предлагается использовать систему полностью гомоморфного шифрования [10], позволяющую отправить на сервер биометрические персональные данные в зашифрованном виде, обработать их при помощи нейронной сети, получить зашифрованный результат вычислений и уже локально расшифровывать его и сравнивать с пространством субъектов идентификации.

Новизна исследования складывается из следующих характеристик и особенностей разрабатываемой технологии:

- Построение инновационной безопасной клиент-серверная архитектуры системы биометрической идентификации личности.
- Разработка единого универсального подхода к обработке биометрических идентификаторов на основе нейронных сетей [18].
- Использование современных актуальных и эффективных моделей и архитектур нейронных сетей [20].
- Применение новых, мало исследованных, но показавших свою эффективность в ряде прикладных задач эволюционных алгоритмов и алгоритмов роевого интеллекта.
- Разработка систем идентификации по ряду слабо проработанных и редко применяемых биометрических характеристик с использованием современных технологий и возможностей методов искусственного интеллекта (например, идентификация по рисунку вен ладони, по экранному почерку, по радужке глаза и так далее).
- Построение модульной системы автоматизированного машинного обучения для распознающих модулей.
- Исследование и практическая реализация способов гибридизации алгоритмов обучения для повышения их эффективности в рамках работы с конкретной моделью.
- Разработка протокола биометрической идентификации личности с применением новых систем гомоморфного шифрования.

В рамках исследования проведен анализ и патентный поиск, разработаны и получены патенты на способы биометрической идентификации личности по рисунку вен ладони (RU 2761776 C1, RU 2788590 C1).

По итогам исследования была разработана система, способная обеспечить безопасное применение идентификации личности по биометрическим параметрам, затруднить компрометацию биометрических идентификаторов. Унифицирован подход к применению систем биометрической идентификации. Применение разработанных методов повышает уровень безопасности биометрических персональных данных в системах идентификации. Разработанные технологии способствуют улучшению надежности и эргономичности систем разграничения и предоставления доступа, в том числе по рисунку вен ладони.

Разработаны программы для ЭВМ «Программа для конфигурирования и управления алгоритмами глобальной оптимизации» (№2020617995), «Программный комплекс агрегации обучающей выборки нейросети для идентификации личности по рисунку вен ладони» (№2020617996), базы данных «База данных для хранения параметров идентификации личности по рисунку вен ладони» (№2020621227) и «База данных конфигураций алгоритмов роевого интеллекта» (№2020621230). На все программы и базы данных получены свидетельства о государственной регистрации.

Теоретические и практические результаты будут использованы в лекционном, лабораторном и практическом курсах дисциплины «Технологии искусственного интеллекта в области безопасности и защиты информации» для студентов специальностей 10.05.01 Компьютерная безопасность, 10.05.03 Информационная безопасность автоматизированных систем и магистров направления подготовки 10.04.01 Информационная безопасность кафедры компьютерных технологий и информационной безопасности КубГТУ. Программно-методические комплексы данных дисциплин разработаны для новых учебных планов ФГОС ВО 3++, введенных с 2021 г.

СПИСОК ЛИТЕРАТУРЫ

1. Jain, A K, Ross A and Pankanti S Biometrics: a tool for information security, Trans. Inf. Forensics Secur 1(2), 2006, p. 125–143.
2. Hassanat, A.B., Albustanji, A., Tarawneh, A.S., Alrashidi, M., Alharbi, H., Alanazi, M., Alghamdi, M., Alkhazi, I.S., & Prasath, V., Deep learning for identification and face, gender, expression recognition under constraints, ArXiv, abs/2111.01930, 2021.
3. Soleymani, S., Dabouei, A., Taherkhani, F., Iranmanesh, S.M., Dawson, J.M., & Nasrabadi, N.M., Quality-Aware Multimodal Biometric Recognition, ArXiv, abs/2112.05827, 2021.
4. Mugalu, B.W., Wamala, R.C., Serugunda, J., & Katumba, A. (2021). Face Recognition as a Method of Authentication in a Web-Based System. ArXiv, abs/2103.15144.
5. Marattukalam, F., Abdulla, W.H., & Swain, A.K. (2021). N-shot Palm Vein Verification Using Siamese Networks. 2021 International Conference of the Biometrics Special Interest Group (BIOSIG), 1-5.
6. Meng, Z., Altaf, M.U., & Juang, B. (2020). Active voice authentication. ArXiv, abs/2004.12071.
7. Stragapede, G., Vera-Rodríguez, R., Tolosana, R., Morales, A., Acien, A., & Lan, G.L. (2022). Mobile Behavioral Biometrics for Passive Authentication. ArXiv, abs/2203.07300.
8. Im S, Park H, Kim Y, Han S, Kim S, Kang C, Chung C, A Biometric identification system by extracting hand vein patterns, J Korean Phys Soc 28(3), 2001, p. 268-272

9. R. Fuksis, M. Pudzs, M. Greitans, Palm Vein Biometrics Based on Palm Infrared Imaging and Complex Matched Filtering, The 12th ACM Workshop on Multimedia and Security, Rome, 2009, p. 27.
10. Частикова, В.А. Разработка архитектуры машинного обучения с использованием гомоморфного шифрования для обеспечения конфиденциальности данных / В.А. Частикова, С. А. Жерлицын, А. Н. Пешков, А. С. Карапетян // Электронный сетевой политематический журнал "Научные труды КубГТУ". — 2022. — №2. — 135-147.
11. Частикова, В. А., Жерлицын, С. А., Воля, Я. И. Нейросетевой метод идентификации личности по неформализованной семантической характеристике Вестник УрФО. Безопасность в информационной сфере. – 2018. – № 4(30). – С. 20-26. – DOI 10.14529/secur180403. – EDN YUNKCL.
12. Частикова, В. А., Жерлицын, С. А., Воля Я. И., Сотников, В. В. Нейросетевая технология обнаружения аномального сетевого трафика Прикаспийский журнал: управление и высокие технологии – № 1(49). – С. 20-32. – DOI 10.21672/2074-1707.2020.49.4.020-032. – EDN WUCDII.
13. Jain, A K, Ross A and Pankanti S Biometrics: a tool for information security Trans. Inf. Forensics Secur 1(2) 125–143
14. Malatras, A, Geneiatakis, D and Vakalis, I On the efficiency of user identification: a system-based approach Int. J. Inf. Secur. 16 653–671
15. Im S, Park H, Kim Y, Han S, Kim S, Kang C, Chung C A Biometric identification system by extracting hand vein patterns J Korean Phys Soc 28(3) 268-272
16. Sarkar A and Singh B K A review on performance, security and various biometric template protection schemes for biometric authentication systems Multimed Tools Appl 79 27721–76
17. Hancock J T and Khoshgoftaar T M Survey on categorical data for neural networks. J Big Data 7 no.28
18. Chastikova V. A., Zherlitsyn S. A., Volya Y.I. Neural network method of identification by unformalized semantic characteristics News of Volgograd State Technical University no. 8(218) 63–67
19. Blokus A and Krawczyk H Systematic approach to binary classification of images in video streams using shifting time windows SIViP 13 341–348
20. Chastikova V. A., Zherlitsyn S. A., Volya Y.I. Analysis of training of deep neural networks with heterogeneous architecture while detecting malicious network traffic IOP Conference Series: Materials Science and Engineering, Krasnoyarsk, Russian Federation: IOP Publishing Ltd, 2021. – P. 12135. – DOI 10.1088/1757-899X/1047/1/012135.

Иванов С.О.
ФГБОУ ВО ЧГУ им. И.Н. Ульянова, старший преподаватель
v101-11@mail.ru

НЕЙРОСЕТЕВОЕ МОДЕЛИРОВАНИЕ И ПРОГРАММНО-АППАРАТНОЕ ОБЕСПЕЧЕНИЕ КОНТРОЛЯ АНОМАЛИЙ В ИНФОРМАЦИОННОМ ОБМЕНЕ ЗАЩИТНОЙ АВТОМАТИКИ

Аннотация: Целью проекта является изучение возможности применения методов распознавания аномалий в информационном обмене систем автоматического управления технологическим процессом с помощью искусственных нейронных сетей для создания и повышения эффективности алгоритмов функционирования программно-аппаратного комплекса контроля механизмов защитной автоматики. Теоретическими результатами являются предложенные методы обучения и тестирования искусственной нейронной сети распознаванию аномалий в сетевом трафике; результаты применения искусственных нейронных сетей различной конфигурации к задаче контроля механизмов пороговой защиты; результаты применения искусственной нейронной сети прямого распространения к обнаружению аномалий сетевого потока. На практике результаты работы могут быть использованы для создания программно-аппаратного комплекса на основе искусственных нейронных сетей для выявления некорректной работы механизмов защитной автоматики автоматизированной системы управления технологическим процессом.

Ключевые слова: информационная безопасность, искусственные нейронные сети, выявление аномалий, АСУТП.

Актуальность темы исследования. Внедрение информационных технологий (ИТ) в рамках четвертой промышленной революции и стратегии цифровизации в промышленность привело к появлению новых угроз информационной безопасности, которые раньше были отделены от операционных технологий (ОТ). Цифровизация автоматизированных систем управления технологическим процессом (АСУТП) основана на включении в ее инфраструктуру компьютерных сетей для унификации всех взаимодействий, в связи с чем повышается роль средств контроля сетевой инфраструктуры. Средства защиты, применяемые в ИТ, неэффективны или не предназначены для работы в промышленных сетях. Также многие автоматизированные системы управления технологическим процессом по значимости относятся к объектам критической информационной инфраструктуры (КИИ) и поэтому применяемые для них средства должны соответствовать требованиям приказа ФСТЭК России №239 от 25 декабря 2017 [1] по обеспечению безопасности объектов КИИ.

Возникает необходимость разработки программно-аппаратного средства, предназначенного для работы в инфраструктуре АСУТП, которое позволит выявить некорректную работу механизмов защитной автоматики вследствии ошибок конфигурации, сбоев или сетевых атак без вмешательства в работу АСУТП с помощью выявления аномалий в сетевом трафике.

Современный подход к анализу сетевого трафика – применение различных методов машинного обучения, описанные во многих работах: многопараметрическое обнаружение сетевых атак, детектирование на основе модели информационного процесса, деревья решений, метод изолирующего леса, elliptic envelope и статистические методы, метрические методы (k

ближайших соседей, k-средних), кластерные методы, алгоритмы нечёткой кластеризации Fuzzy C-means, метод главных компонент, методы аппроксимации данных, алгоритмы на основе прогнозирования временных рядов, обучение с учителем (регрессия, классификация), модельные тесты, машина опорных векторов, метод опорных векторов с одним классом (One-Class SVM), самоорганизующиеся карты, искусственные нейронные сети, репликаторы с длительной памятью, автокодировщики, списки "белых" (разрешеных) протоколов.

Чаще всего для обнаружения аномалий сетевого трафика используются искусственные нейронные сети, например, для обнаружения вторжений и сетевых атак, наиболее часто используется многослойный персептрон (MLP) и радиальная базисная функция (RBF). В работах авторов Жигулин П.В., Подворчан Д.Э, Кожевникова И.С, Podder Prajoy, Subrato Bharati, M. Rubaiyat Hossain Mondal, Pinto Kumar Paul, Utku Kose [2, 3, 4], показано, что для атак типа отказ в обслуживании, несанкционированный удаленный доступ, сканирование портов, получение привилегий искусственные нейронные сети различных типов показали точность до 99.2% на произвольном наборе данных. В работе Araceli Barradas-Acosta, Eleazar Aguirre-Anaya, Mariko Nakano-Miytake Hector Perez-Meana [5] показано, что для атак Man-in-the-Middle и Session Hijackin подходят рекуррентные искусственные нейронные сети.

Машинное обучение успешно применяется в автоматизированных системах управления технологическим процессом для различных задач. В работах авторов Bhattacharya B., Sinha A., Yadav A., Dash Y., Kulikov A.L., Loskutov A.A., Mitrovic M., Bychkov A., Slavutskii L., Slavutskaya E. Ashrafi A., Shahrtash S.M. Z. He, S. Lin, Y. Deng, X. Li, Q. Qian, Лоскутов А.А., Митрович М., Осокин В.Ю [6, 7, 8, 9, 10, 11, 12] машинное обучение применяется для: детектирования, классификации, локализации неисправностей, улучшения работы защитной автоматики, для импульсного ультразвукового виброконтроля электротехнического оборудования, динамического управления напряжением на большой территории, классификации неисправностей, контроля правильности срабатывания максимальной токовой защиты, повышения надежности и распознаваемости нормальных и аварийных режимов работы.

Таким образом применение искусственных нейронных сетей позволит выявлять некорректную работы механизмов защитной автоматики из-за ошибок конфигурации, сбоев или сетевых атак.

Цель научного проекта является развитие методов распознавания аномалий в информационном обмене систем автоматического управления технологическим процессом с помощью искусственных нейронных сетей и повышение эффективности соответствующих алгоритмов функционирования программно-аппаратного комплекса контроля механизмов защитной автоматики.

Основные задачи:

– оценка возможности применения методов машинного обучения и искусственных нейронных сетей для анализа сетевого трафика;

– проектирование программно-аппаратного стенда для исследования особенностей сетевого взаимодействия компонентов автоматизированных систем управления технологическим процессом;

– моделирование искусственных нейронных сетей для выявления аномалий в информационном обмене механизмов защитной автоматики автоматизированной системы управления технологическим процессом;

– разработка алгоритмов работы программно-аппаратного комплекса на основе искусственных нейронных сетей для определения некорректной работы механизмов защитной автоматики автоматизированной системы управления технологическим процессом.

Новизна исследования:

1. Разработаны новые алгоритмы и архитектура для программно-аппаратного стенда, моделирующего системы автоматического управления технологическим процессом, позволяющие выявлять аномалии в информационном обмене, на основе искусственных нейронных сетей.

2. Предложена конфигурация, методы обучения и тестирования искусственной нейронной сети прямого распространения для выявления аномалий в работе релейных и кибернетических защит.

3. При вычислительных экспериментах выявлены статистические особенности применения искусственных нейронных сетей для контроля механизмов защиты вблизи порога срабатывания, позволяющие обнаружить аномалии в передаваемых данных.

Теоретическая значимость. Теоретическими результатами являются предложенные методы обучения и тестирования искусственной нейронной сети распознаванию аномалий в сетевом трафике; результаты применения искусственных нейронных сетей различной конфигурации к задаче контроля механизмов пороговой защиты; результаты применения искусственной нейронной сети прямого распространения к обнаружению аномалий сетевого потока.

Практическая значимость. На практике результаты работы могут быть использованы для создания программно-аппаратного комплекса на основе искусственных нейронных сетей для выявления некорректной работы механизмов защитной автоматики автоматизированной системы управления технологическим процессом.

Методы исследования:

Помимо общих, теоретических и эмпирических методов исследования применялись математические методы и программное обеспечение: язык программирования python, фреймворк pytorch для работы с искусственными нейронными сетями, средства захвата и анализа сетевого трафика.

Положения, выносимые на защиту:

1. Алгоритмы и программное обеспечение для программно-аппаратного стенда, моделирующего системы автоматического управления технологическим процессом, позволяющие выявлять аномалии в информационном обмене на основе искусственных нейронных сетей.

2. Результаты вычислительных экспериментов по использованию искусственных нейронных сетей для выявления аномалий в информационном обмене механизмов защиты вблизи порога срабатывания.

3. Алгоритмы работы программно-аппаратного комплекса на основе искусственных нейронных сетей для обнаружения аномалий в информационном обмене автоматизированной системы управления технологическим процессом.

Степень достоверности и апробация результатов. Основные положения и результаты проекта докладывались на:

– XIII всероссийской научно-технической конференции "Информационные технологии в электротехнике и электроэнергетике" (ДНДС-2022).

– International Ural Conference on Electrical Power Engineering. Proceedings - 2021 (UralCon 2021).

– XIV Всероссийская научно-техническая конференция "Динамика нелинейных дискретных электротехнических и электронных систем" (ДНДС-2021).

– VI Международная научно-практическая конференция «Релейная защита и автоматизация электроэнергетических систем России» 2021 (РЕЛАВЭКСПО-2021).

– XII Всероссийская научно-техническая конференция "Информационные технологии в электротехнике и электроэнергетике" (ИТЭЭ-2020).

Основные результаты по теме проекта изложены в 11 печатных изданиях, 5 из которых которых изданы в журналах, рекомендованных ВАК, 1 в издании которое индексируются Scopus. зарегистрированы 4 программы для ЭВМ.

Результаты, полученные за период реализации научного проекта.

1. Разработаны новые алгоритмы и программное обеспечение для программно-аппаратного стенда, моделирующего системы автоматического управления технологическим процессом, позволяющие выявлять аномалии в информационном обмене на основе искусственных нейронных сетей. По основным программным модулям оформлена государственная регистрация интеллектуальной деятельности [13, 14, 15, 16].

2. Предложена методика конфигурации, обучения и тестирования искусственной нейронной сети прямого распространения для задачи выявления аномалий в работе релейных и кибернетических защит. Методика успешно применена для создания искусственной нейронной сети определяющая различные аномалии сетевого потока ICMP с точностью около 98,6614%, успешность обучения по критерию F1 составила 0,964.

3. В ходе вычислительных экспериментов выявлены статистические особенности применения искусственных нейронных сетей для контроля механизмов защиты в близи порога срабатывания, позволяющие определить вмешательство в данные. При смещении данных за пределы диапазона обучения искусственная нейронная сеть перестаёт их распознавать, что можно использовать как средство контроля аномалий. Правильность работы созданных искусственных нейронных сетей для данных задач по критерию F1 составила 90-98%.

4. Разработаны алгоритмы программно-аппаратного комплекса на основе искусственных нейронных сетей для выявления аномалий в информационном обмене автоматизированной системы управления технологическим процессом. Описаны условия и особенности его применения. Алгоритм работы программно-аппаратного комплекса представлен в виде диаграммы последовательности (рис. 1).

– Разработанный программно-аппаратный комплекс имеет низкую стоимость, по сравнению с другими средствами защиты, не оказывает влияние на работу механизмов автоматизированной системы управления технологическим процессом, и поэтому может применяться в объектах критической информационной инфраструктуры. Результаты сравнения эффективности различных средств защиты, которые можно применять для контроля аномалий и разработанного программно-аппаратного комплекса, оцененных по шкале от 1 до 5, где 5 – максимальная эффективность, показаны в Табл. 1.

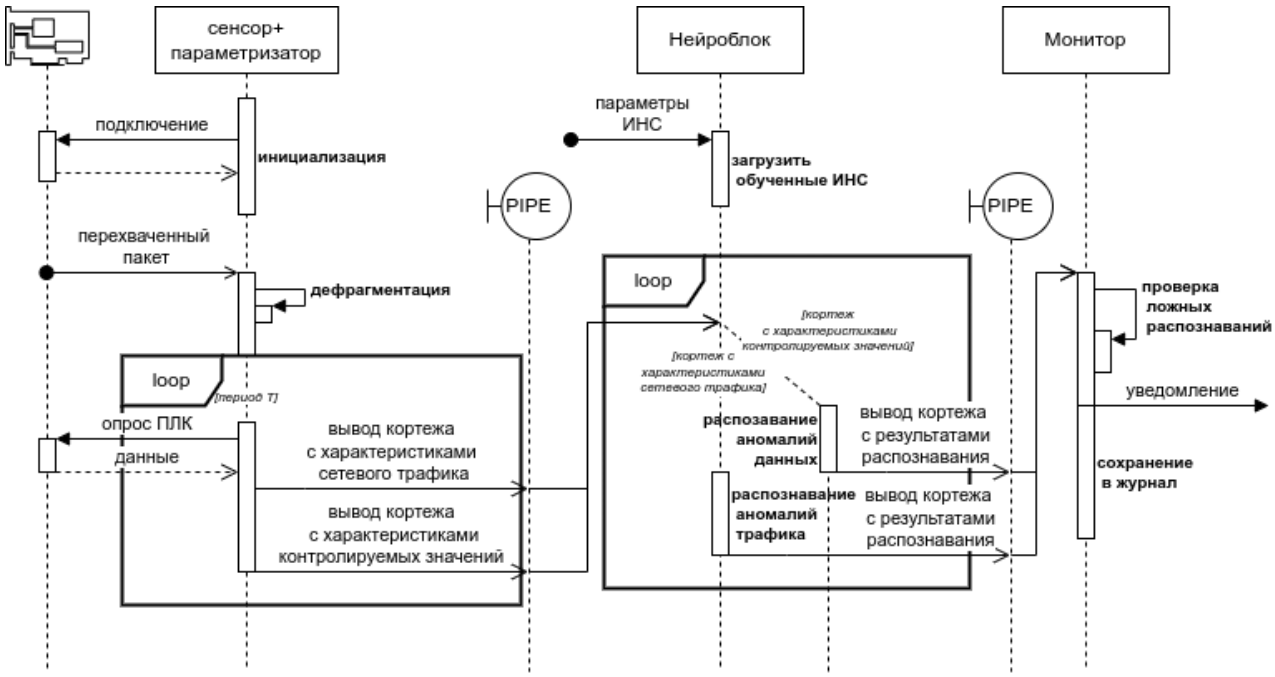


Рис. 1. Диаграмма последовательности взаимодействия модулей программно-аппаратного комплекса

Табл. 1. Оценка средств обнаружения аномалий

Средство защиты	Обнару-жение сетевых атак	Обнару-жение вмеша-тельства	Возмож-ность настрой-ки	Слож-ность внедре-ния	Защищен-ность	Производи-тельность, стоимость
Системы обнаружения вторжений	4	2	4	3	3	3
Криптошлюзы, криптомаршрутизаторы	1	4	2	1	5	3
Системы мониторинга событий	2	2	3	1	3	2
Межсетевые экраны	3	1	3	2	4	2
ПАК контроля аномалий на основе ИНС	3	5	3	5	4	4

Перспективы дальнейшей разработки темы:

– Для исследования сетевого трафика различных автоматизированных систем управления технологическим процессом необходимо добавление новых промышленных протоколов, увеличение разнообразия эмуляторов программируемых логических контроллеров и полевых устройств.

– В продолжение работы следует провести исследование различных промышленных сетевых протоколов, возможно с применением машинного обучения, для выявления существенных параметров их сетевого трафика, которые можно использовать для обнаружения аномалий.

– В дальнейшем изучить возможности других видов искусственных нейронных сетей: рекурсивных, с краткосрочной памятью, трансформеров. С учитом успехов языковых моделей, типа ChatGPT, требуется разработка новых методик подготовки данных для обучения искусственных нейронных сетей для выявления аномалий.

– Требуется провести работы по расширению возможностей программно-аппаратного комплекса и повысить его производительность, чтобы довести его до промышленного образца.

СПИСОК ЛИТЕРАТУРЫ

1. Приказ от 25 декабря 2017 г. №239 "Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации" [электронный ресурс]. – URL: https://fstec.ru/en/53-normotvorcheskaya/akty/prikazy/1592-prikaz-fstek-rossii-ot-25-dekabrya-2017-g-n-239
2. Жигулин П.В., Подворчан Д.Э. Анализ сетевого трафика с помощью нейронных сетей // Электронные средства и системы управления. – № 2. – 2013. – С. 44-48.
3. Кожевникова И.С. Контролируемые методы машинного обучения как средство детектирования сетевых вторжений / И.С. Кожевникова, Е.В. Ананьин, А.В. Лысенко, А.В. Никишова // Молодой ученый. - №27 (131), 2016. - С.20-23. - URL: https://moluch.ru/archive/131/36300/
4. Podder Prajoy. Artificial Neural Network for Cybersecurity: A Comprehensive Review / Podder Prajoy, Subrato Bharati, M. Rubaiyat Hossain Mondal, Pinto Kumar Paul, Utku Kose // arXiv e-prints. - 2021. - doi:10.48550/arXiv.2107.01185
5. Araceli Barradas-Acosta, Eleazar Aguirre-Anaya, Mariko Nakano-Miytake Hector Perez-Meana. Attacks recognition using recurrent neural network // International conference on Computational and information science 2009 (CIS'09). World Scientific and Engineering Academy and Society (WSEAS). - Wisconsin, 2009. - pp. 402-409.
6. Bhattacharya B., Sinha A. Intelligent Fault Analysis in Electrical Power Grids // IEEE 29th International Conference on Tools with Artificial Intelligence (ICTAI), Boston. - 2017. - pp. 985-990. - doi: 10.1109/ICTAI.2017.00151
7. Yadav A., Dash Y. An overview of transmission line protection by artificial neural network: fault detection, fault classification, fault location, and fault direction discrimination // Advances in Artificial Neural Systems. - 2014. - pp. 20.
8. Kulikov A.L., Loskutov A.A., Mitrovic M. Improvement of the technical excellence of multiparameter relay protection by combining the signals of the measuring fault detectors using artificial intelligence methods // International Scientific and Technical Conference Smart Energy Systems 2019 (SES-2019). - 124, 2019. - doi:https://doi.org/10.1051/e3sconf/201912401039
9. Bychkov A., Slavutskii L., Slavutskaya E. Neural Network for Pulsed Ultrasonic Vibration Control of Electrical Equipment // 2020 International Ural Conference on Electrical Power Engineering (UralCon). - 2020. - pp.24-28. - doi: 10.1109/UralCon49858.2020.9216248.
10. Ashrafi A., Shahrtash S.M. Dynamic Wide Area Voltage Control Strategy Based on Organized Multi-Agent System // IEEE Transactions on Power Systems. - 2014. - vol. 29, no. 6. - pp. 2590-2601. - DOI:10.1109/TPWRS.2014.2313607.
11. He Z. A rough membership neural network approach for fault classification in transmission lines / Z. He, S. Lin, Y. Deng, X. Li, Q. Qian // International Journal of Electrical Power and Energy Systems. - 61, 2014. - pp. 429-439.
12. Лоскутов А.А., Митрович М., Осокин В.Ю. Повышение распознаваемости режимов функционирования системы электроснабжения на основе методов машинного обучения // НГТУ им. Р.Е. Алексеева, г. Нижний Новгород, Россия. Номер: 4 (41) Год: 2020 Страницы: 26-34
13. Копышева Т.Н., Иванов С.О., Артемьев В.А. iGNAD v.1. - Номер свидетельства: RU 2022683892. 2022.

14. Копышева Т.Н., Иванов С.О., Иванов А.В. Павлов Д.В. iGscada v.1. - Номер свидетельства: RU 2022683890. 2022.
15. Копышева Т.Н., Иванов С.О., Иванов А.Ю. Павлов Д.В. Андреев И.И. iGPLC v.1. - Номер свидетельства: RU 2022683891. 2022.
16. Иванов С.О., Ларюхин А.А., Никандров М.В., Славутский Л.А. Программа для нейромоделирования характеристик релейной и кибернетических защит CPNEUROSIM-1. – Номер свидетельства: RU 2021664193. – 2021.

Иниватов Д.П.
ОмГТУ, младший научный сотрудник,
daniilini@mail.ru

ИДЕНТИФИКАЦИЯ ДИКТОРА С УЧЁТОМ ПСИХОЭМОЦИОНАЛЬНОГО СОСТОЯНИЯ НА ОСНОВЕ АНСАМБЛЯ ИСКУССТВЕННЫХ НЕЙРОННЫХ СЕТЕЙ

Аннотация: В данной работе описывается подход к идентификации диктора с использованием ансамбля искусственных нейронных сетей, который учитывает психоэмоциональное состояние диктора. Для решения указанной задачи была использована архитектура, включающая в себя автокодировщик, нейросетевой преобразователь биометрий-код, а также метод ансамблирования. В ансамбль были включены различные архитектуры нейронных сетей, обученные на разных репрезентациях голосовых образов, что приводит к снижению равновероятной ошибки. Использование нейросетевого преобразователя биометрия-код в архитектуре решения позволяет обеспечить сохранность биометрических данных дикторов в случае атаки на классификатор. Приводятся сравнительные таблицы результатов исследований, проведенных в области распознавания субъекта по голосовым характеристикам, включая текущее.

Ключевые слова: Идентификация диктора, ансамблирование, машинное обучение, психоэмоциональное состояние.

Введение

Защита конфиденциальных данных является одной из наиболее актуальных проблем в современном мире. Важность данной темы подтверждается статистикой компьютерных преступлений, в которых несанкционированный доступ к конфиденциальным данным является одной из основных причин утечки информации, также данными о росте ущерба от киберпреступлений [1]. Стандартным решением для обеспечения безопасности информации является парольная аутентификация, однако данный метод не всегда гарантирует достаточный уровень защиты, так как несанкционированные лица могут получить доступ к паролю и использовать его для своих целей. Для устранения данной угрозы всё чаще используются более надежные методы аутентификации, такие как системы на основе биометрических данных. Указанные системы позволяют использовать уникальные физические или поведенческие особенности человека для подтверждения его личности и, следовательно, обеспечения более высокого уровня защиты. Таким образом, разработка более надежных методов аутентификации, например, на основе биометрических данных, представляет собой важное направление в области информационной безопасности (ИБ). Рынок голосовой биометрии стремительно развивается и ожидается его значительный рост в ближайшие годы [2], что делает данную тему еще более актуальной.

Особый интерес вызывает голосовая биометрия, которая позволяет идентифицировать человека по особенностям его речи. Но, к сожалению, голосовые характеристики считаются малоинформативными и изменчивыми в зависимости от психофизиологического состояния (ПФС) субъекта.

Настоящее исследование посвящено решению комплекса проблем, связанных с надежностью биометрической аутентификации, защищенностью биометрических образов от

компрометации и обучением биометрических систем на малых выборках биометрических данных.

Целью работы является разработка системы биометрической аутентификации диктора по голосу с учётом его психоэмоционального состояния на основе нейросетевых моделей доверенного искусственного интеллекта.

Задачи:

- Разработать метод извлечения информативных признаков из голосового сигнала, характеризующих пользователя на основе нейронных сетей;
- Разработать модель нейросетевого преобразователя биометрия-код (НПБК) для аутентификации по голосу;
- Разработать алгоритм автоматического синтеза и обучения НПБК на малых выборках;
- Разработать программный комплекс для биометрической аутентификации диктора по голосу с учётом его психоэмоционального состояния на основе предложенных моделей и алгоритмов.

Научной новизной считается разработанный метод извлечения признаков, основанный на ансамблировании нескольких различных архитектур нейронных сетей. На последующую защиту планируется выносить алгоритм обучения НПБК, метод ансамблирорования, который позволяет снизить вероятность ошибок без роста объема обучающей выборки, основанный на комплексировании автокодировщиков, а также технологию защищенного исполнения процедур биометрической аутентификации по голосу. Теоретическая значимость заключается в предложенной концепции, моделях и процедуре обучения. Практической значимостью считается повышение надёжности биометрической аутентификации субъекта по голосу и защищённости компьютерных ресурсов от неавторизованного доступа при помощи разработанного программного комплекса.

Теория

С зарождением идеи распознавания человека по голосу в середине XX века исследователи сталкивались с ограниченными вычислительными ресурсами и методами, что влияло на точность разрабатываемых систем. В 1962 году возникла концепция сопоставления голосовых спектрограмм, однако данную задачу приходилось решать вручную, с привлечением людей [3]. Проведённые эксперименты продемонстрировали эффективность использования спектрограмм в качестве идентифицирующей формы представления голоса.

Расширение вычислительных возможностей в 1980-х позволило применить статистические и методы машинного обучения. Точность распознавания разрабатываемых методов достигала 54–95% [4]. В 1990-х и 2000-х акцент сместился на эмоциональную и когнитивную голосовую аналитику, стала актуальной задача защиты биометрических данных [5]. В последние десятилетия, развитие нейронных сетей и глубокого обучения принесло повышение точности и эффективности. Одновременно с увеличением качества распознавания, исследователи стали уделять больше внимания другим проблемам, в частности, обеспечению конфиденциальности биометрических данных диктора и изменчивости голосовых характеристик в зависимости от здоровья и психоэмоционального состояния человека.

На параметры человеческой речи оказывают влияние многие факторы: пол, возраст, перенесённые болезни, индивидуальные особенности организма, строение голосового тракта, а также текущее ПФС [6, 7]. В свою очередь, на ПФС способны воздействовать такие обстоятельства как сонливость, эмоциональная напряжённость, употребление алкогольных

напитков. Алкогольное опьянение может оказывать заметный эффект на когнитивную и сенсомоторную функции, что существенно отражается и на произносимой речи:

- по мере увеличения концентрации алкоголя в крови происходит замедление мыслительных процессов, что снижает темп речи;
- наличие нехарактерных для человека пауз, изменение высоты голоса;
- при низких концентрациях алкоголя проявляется увеличение силы голоса, но при дальнейшем употреблении напитков сила голоса уменьшается;
- отрывистая речь с наличием запинок, самоповторов и исправлений;
- более длительное произношение ударных звуков в словах;
- обеднение синтаксических конструкций, использование простых предложений [8].

Появление таких признаков алкогольного опьянения как изменение силы и высоты голоса, появления хриплости представлено на рис. 1. В левой части изображения располагается осциллограмма и спектрограмма голосового образа диктора в нормальном состоянии, в правой части – под воздействием спиртных напитков. Уменьшение силы голоса хорошо заметно при обзоре осциллограмм, а увеличение высоты тона можно проследить исходя из анализа спектральной плотности мощности сигнала внизу изображения.

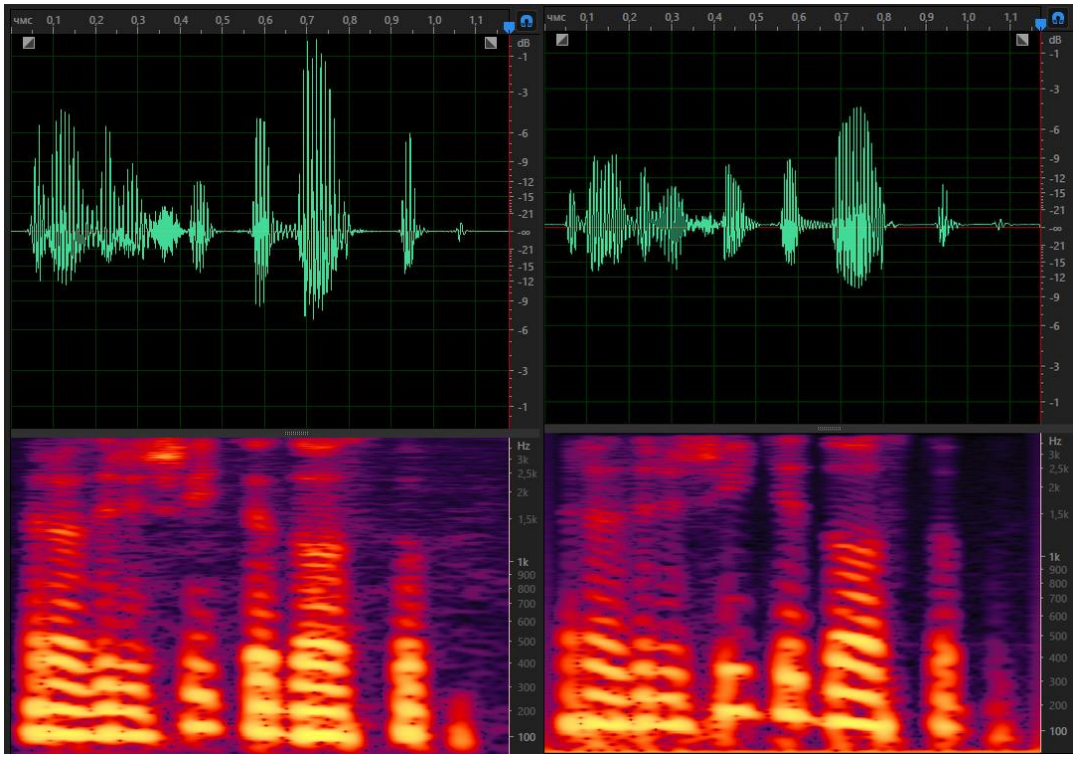


Рис. 1. Иллюстрация изменения голосового образа и его спектрограммы под воздействием алкоголя.

Достигнутые результаты

Для проведения эксперимента был собран голосовой архив. Возраст дикторов, принявших участие в создании базы, варьировался от 18 до 35 лет, а число участников достигло 86 при условии равного соотношения между полами. Голосовые файлы спикеров имеют частоту дискретизации 8 кГц и глубину кодирования 16 бит. В архиве было определено несколько состояний, при которых осуществлялась запись речи испытуемых:

1) Нормальное;
2) Состояние опьянения;

3) Состояние сонливости.

Для решения задачи предлагается использовать метод ансамблирования нескольких предобученных моделей сверточных нейронных сетей, обучение которых осуществляется на разных репрезентациях голосовых записей. В результате было спроектировано 5 автокодировщиков с различными архитектурами, в основу которых заложены свёрточные нейронные сети. Каждый автокодировщик ориентирован на извлечение признаков из спектров, получаемых с использованием различных оконных функций. Сформированный вектор признаков подаётся в НПБК, который создаёт уникальный код, связанный с ключом. В дальнейшем для аутентификации пользователя должен применяться данный ключ. В ходе эксперимента было замечено, что при увеличении количества нейронных сетей в ансамбле происходит снижение EER. Ниже приведена сравнительная таблица различных подходов и их результатов по задаче идентификации пользователя и некоторых побочных (Табл. 1).

Табл. 1. Достигнутые результаты в задаче распознавания диктора

Применяемые методы	**EER, %**	**Архив данных**	**Задача**
АП + СО + спектрограмма [10]	6,67	ASVspoof 2019	Идентификация и обнаружение атаки подделки
x-vector + PLDA + расширение данных [11]	5,71	VoxCeleb, SWBD и NIST SRE 2016	Идентификация
x-vector с уменьшенными 6 и 7 слоями + глубокие НС + расширение данных [12]	13,35	NIST2010	Идентификация по коротким высказываниям
ResNet + AAM-Softmax [13]	5,19	VoxSRC 2020	Идентификация
x-vector + GFCC + многоканальное взвешенное предсказание + MVDR + GCRN [14]	2,62	NIST SRE 2010	Идентификация и борьба с шумом
Извлечение признаков, разделение речи, DOVER, Res2Net, AM-Softmax [15]	0,83	VoxCeleb	Идентификация и диаризация
Объединение 4 топологий свёрточных НС (ResNet) + PLDA [16]	1,26	VoxCeleb	Идентификация
x-vector + ResNet [17]	8,95 – 18,15	MSP-Podcast	Идентификация говорящего и эмоции
Thin ResNet-34 + Softmax [18]	3,13	VoxCeleb2	Идентификация и борьба с шумом
спектр и логарифмический спектр + LSTM-RNN [19]	1,3	Chinese Mandarin Corpus	Идентификация и борьба с шумом
предварительно обученная речевая модель Wav2Vec2 + fine-tuning [20]	1,88	Voxceleb1	Идентификация говорящего
i-vector + Гауссовский PLDA [21]	22,32	NIST SRE 2008	Идентификация по коротким высказываниям
SpoTNet + СО [46]	0,95	Нет данных	Идентификация и обнаружение атаки подделки
Автокодировщик + НПБК + ансамблирование	**1,24**	Собственная	Идентификация по коротким высказываниям, защита биометрии с учётом ПФС

Заключение

Представленный в исследовании результат свидетельствует об эффективности предложенного подхода к распознаванию диктора. Создание ансамблей моделей позволяет использовать в своих классификаторах неглубокие архитектуры и проводить обучение модели на малых выборках, а использование НПБК усложняет подделку голоса поскольку позволяет связать кодовую фразу пользователя с его ключом и использовать ключ вместо биометрического образа, что обеспечит в дальнейшем сохранность биометрии. Определение работоспособности подходов упирается в применяемый в обучении и тестировании корпус голосовых данных (размер этой базы, число дикторов, их возраст, языковой акцент, уровень шумов). К сожалению, использование авторами в своих исследованиях различных архивов записей не даёт полноценной возможности сравнивать полученные ими результаты друг с другом. Перспектива по дальнейшим исследованиям состоит в применении различных методов предобработки обучающих данных не только на разных репрезентациях усреднённых спектров, но и, например, спектрограмм. Это позволит получить более высокую репрезентативность и снизить текущую величину равновероятной ошибки.

СПИСОК ЛИТЕРАТУРЫ

1. Генпрокуратура РФ: число киберпреступлений в 2022 году снизилось на 4,9% Об этом сообщает "Рамблер" // Рамблер URL: https://finance.rambler.ru/business/49984464-genprokuratura-rf-chislo-kiberprestupleniy-v-2022-godu-snizilos-na-4-9/ (дата обращения: 12.09.2023).
2. Исследование. Рынок разговорного ИИ в России 2020-2025 // Just AI URL: https://just-ai.com/blog/issledovanie-rynok-razgovornogo-ii-v-rossii-2020-2025 (дата обращения: 15.09.2023).
3. Kersta L. G. Voiceprint identification //The Journal of the Acoustical Society of America. – 1962. – Т. 34. – №. 5_Supplement. – С. 725-725.
4. Wohlford R., Wrench E., Landell B. A comparison of four techniques for automatic speaker recognition //ICASSP'80. IEEE International Conference on Acoustics, Speech, and Signal Processing. – IEEE, 1980. – Т. 5. – С. 908-911.
5. Monrose F. et al. Cryptographic key generation from voice //Proceedings 2001 IEEE Symposium on Security and Privacy. S&P 2001. – IEEE, 2000. – С. 202-213.
6. Галяшина Е. И. Судебно-экспертное исследование обликовых характеристик личности по фонограммам речи: правовые и методические аспекты. – 2017.
7. Лебедева А. К. Обзор состояния судебно-экспертного исследования обликовых характеристик личности по фонограммам речи //Вестник Нижегородского университета им. НИ Лобачевского. – 2015. – №. 3. – С. 138-142.
8. Авдеева Ю. В. Экспериментальное исследование речи людей, находящихся в состоянии ситуативного алкогольного опьянения //Мир науки, культуры, образования. – 2012. – №. 4. – С. 49-51.
9. Gao Y. et al. Detection and evaluation of human and machine generated speech in spoofing attacks on automatic speaker verification systems //2021 IEEE Spoken Language Technology Workshop (SLT). – IEEE, 2021. – С. 544-551.
10. Snyder D. et al. X-vectors: Robust dnn embeddings for speaker recognition //2018 IEEE international conference on acoustics, speech and signal processing (ICASSP). – IEEE, 2018. – С. 5329-5333.

11. Kanagasundaram A. et al. A study of x-vector based speaker recognition on short utterances //Proceedings of the 20th Annual Conference of the International Speech Communication Association, INTERSPEECH 2019. Vol. 2019-September. – ISCA (International Speech Communication Association), 2019. – C. 2943-2947.
12. Heo H. S. et al. Clova baseline system for the voxceleb speaker recognition challenge 2020 //arXiv preprint arXiv:2009.14153. – 2020.
13. Taherian H. et al. Robust speaker recognition based on single-channel and multi-channel speech enhancement //IEEE/ACM Transactions on Audio, Speech, and Language Processing. – 2020. – T. 28. – C. 1293-1302.
14. Xiao X. et al. Microsoft speaker diarization system for the voxceleb speaker recognition challenge 2020 //ICASSP 2021-2021 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). – IEEE, 2021. – C. 5824-5828.
15. Zeinali H. et al. But system description to voxceleb speaker recognition challenge 2019 //arXiv preprint arXiv:1910.12592. – 2019.
16. Pappagari R. et al. x-vectors meet emotions: A study on dependencies between emotion and speaker recognition //ICASSP 2020-2020 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). – IEEE, 2020. – C. 7169-7173.
17. Xie W. et al. Utterance-level aggregation for speaker recognition in the wild //ICASSP 2019-2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). – IEEE, 2019. – C. 5791-5795.
18. El-Moneim S. A. et al. Text-independent speaker recognition using LSTM-RNN and speech enhancement //Multimedia Tools and Applications. – 2020. – T. 79. – C. 24013-24028.
19. Vaessen N., Van Leeuwen D. A. Fine-tuning wav2vec2 for speaker recognition //ICASSP 2022-2022 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). – IEEE, 2022. – C. 7967-7971.
20. Kanagasundaram A. et al. PLDA based speaker recognition on short utterances //Proceedings of The Speaker and Language Recognition Workshop: Odyssey 2012. – International Speech Communication Association, 2012. – C. 28-33.
21. Khan A., Malik K. M. SpoTNet: A spoofing-aware Transformer Network for Effective Synthetic Speech Detection //Proceedings of the 2nd ACM International Workshop on Multimedia AI against Disinformation. – 2023. – C. 10-18.

Караулова О.А.
ФГБОУ ВО ПГУТИ, старший преподаватель каф. ИБ.
olya4369@yandex.ru

ИССЛЕДОВАНИЕ И РАЗРАБОТКА МЕТОДА СОКРЫТИЯ ИНФОРМАЦИИ В СЕТЯХ ПЕРЕДАЧИ ДАННЫХ НА ОСНОВЕ ИНВАРИАНТНЫХ ДВУХКОМПОНЕНТНЫХ СТЕГАНОГРАФИЧЕСКИХ СИСТЕМ

Аннотация: На основе анализа существующих стенанографических алгоритмов, которые используют однокомпонентные контейнеры для встраивания и извлечения скрытой информации предложен новый подход к формированию стеганографических систем, который заключается в разработке методов встраивания и извлечения сигнала в двухкомпонентный звуковой контейнер для форматов аудиоформатов без сжатия и со сжатием в реальном времени. Данный подход позволит повысить защищенность, увеличить пропускную способность каналов при потоковом кодировании информации без снижения устойчивости к стеганографическому анализу, а также эффективно маскировать сообщения в младшем битном слое стеганографических систем, которые работают в системе реального времени за счет использования двухкомпонентного контейнера.

Ключевые слова: стеганография, стегоанализ, метод наименьших значащих бит, двухкомпонентная стеганографическая система, контейнер, звук, система реального времени, аудиоформаты, WAVE, MP3.

Актуальность темы исследования

В телекоммуникационных сетях для защиты информации от несанкционированного доступа используется криптографическое кодирование, которое преобразовывает доступную для пользователя информацию с помощью шифрования. Криптографическое кодирование использует специальный ключ шифрования, который позволяет защитить зашифрованную информацию от злоумышленника. На сегодняшний день существует множество алгоритмов криптографического кодирования, которые способны передавать информацию доверенному лицу. Однако, если информация передается по открытому каналу, то злоумышленник может перехватить зашифрованную информацию или еще хуже, разорвать (разрушить) канал. Чтобы избежать этого, защита информации может быть обеспечена методами сокрытия информации (стеганографическими методами), которые позволяют тайно передавать важную информацию по открытому каналу связи таким образом, чтобы злоумышленник не смог уловить (зафиксировать, заметить, обнаружить) факт передачи и уничтожить сообщение. Информация отправляется в файл, называемым контейнером, который не представляет интереса для злоумышленника, а затем передается по каналу связи. Чаще всего в качестве контейнеров используются медиафайлы (аудиофайлы, видеофайлы или изображения) [1,2]. За последние годы из-за интенсивного внедрения средств интернет коммуникаций представляют больший интерес аудиофайлы, где ежедневно происходит активный обмен сообщениями между пользователями в реальный момент времени. Работа стеганографических систем в режиме реального времени имеет ряд ограничений в использовании современных методов, что приводит к слабой защите при встраивании сообщений в режиме реального времени. Повышение безопасности стеганографических систем в реальном времени можно достичь за

счет использования инвариантных двухкомпонентных контейнеров для сокрытия информации. Создание таких систем является актуальной научно-технической задачей.

Степень разработанности темы исследования:

Данная тема характеризуется анализом существующих файлов различных форматов (текст, аудио, видео, изображения), стандартов передачи данных, а также накопленной базы стеганографических алгоритмов. Значительный вклад в формирование теоретической и методологической основы исследований в области стеганографии внесли такие учёные как R. J. Anderson, W. Bender, C. Cachin, S. Craver, J. Fridrich, N. F. Johnson, N. Morimoto, B. Pfitzmann, I. Pitas, B. Schneier, G. J. Simmons, S. Voloshynovskiy. Среди отечественных учёных следует выделить следующих авторов С. В. Белим, И. С. Вершинин, В. Г. Грибунин, Г. Ф. Конахович, В. И. Коржик, И. Н. Оков, А. Ю. Пузыренко, В. А. Райхлин, Б. Я. Рябко, И. В. Туринцев, В. Н. Кустов, Л. К. Бабенко, В. В. Нечта и других.

В результате проведенного обзора можно сделать вывод о том, что больших успехов достигли исследования в области маскировки информации в изображениях. Большие перспективы в данном направлении получила работа [3], в которой представлены подходы развития стеганографии в стационарных изображениях. Несмотря на существующие методы скрытой передачи информации, с развитием цифровых систем это направление обрело новую жизнь в виде сокрытия цифровой информации. С конца XX века. это направление стало популярным, о чем можно судить по росту издательской деятельности в системе цитирования Scopus [4]. Начиная с 2020 года вырос спрос на использование программ видеосвязи, проведение online-конференций, семинаров, в результате чего увеличился обмен голосовыми сообщениями, благодаря этому возник интересен для разработки стеганографических методов в реальном времени, а именно, для VoIP-систем тем более, что по данному направлению публикации представлены в ограниченном количестве.

Объект исследования:

Двухкомпонентные стеганографические системы для звуковых объектов.

Предмет исследования:

Методы встраивания сообщений в звуковой контейнер со сжатием и без сжатия.

Цели и задачи исследования:

Основной целью исследования является разработать метод сокрытия информации для систем реального времени форматов со сжатием и без сжатия на основе инвариантной двухкомпонентной стеганографической системы. Для достижения поставленной цели в работе решаются следующие задачи:

– Разработка метода встраивания и извлечения сообщения в двухкомпонентный звуковой контейнер без сжатия;

– Разработка метода встраивания и извлечения сообщения в двухкомпонентный звуковой контейнер со сжатием;

– Разработка математических моделей подсистем встраивания и извлечения сигнала сообщения в двухкомпонентный контейнер;

– Исследовать устойчивость предложенных методов стегоанализа.

Методы исследования:

Для решения поставленных задач были использованы методы математического и численного моделирования, статистические методы, цифровая обработка сигналов, алгоритмы стеганографической защиты информации.

Положения, выносимые на защиту:

– Метод встраивания и извлечения сообщения в двухкомпонентный звуковой контейнер без сжатия;

– Метод встраивания и извлечения сообщения в двухкомпонентный звуковой контейнер со сжатием;

– Математические модели подсистем встраивания и извлечения сигнала сообщения в двухкомпонентный контейнер.

Научная новизна исследования:

Предложен метод встраивания и извлечения сообщения в двухкомпонентный звуковой контейнер без сжатия, позволяющий обеспечить маскировку сообщения в реальном времени за счёт искажения распределения значений встраиваемого сообщения;

Предложен метод встраивания и извлечения сообщения в двухкомпонентный звуковой контейнер со сжатием за счёт использования вариации сжимаемого сигнала на этапе реализации психоаккустической модели.

Разработаны математические модели подсистем встраивания и извлечения сигнала сообщения в двухкомпонентный контейнер, обеспечивающие реализацию двухкомпонентных стеганографических систем в звуковых сигналах бес сжатия и со сжатием.

Степень достоверности и апробация работы:

Полученные научные результаты по теме исследования опубликованы в журналах ВАК, получено свидетельство о регистрации программы для ЭВМ 2023610522 от 11.01.2023 г., подана заявка на патент «Способ сокрытия информации», а также результаты докладывались на российских и международных научно-технических конференциях: XIX Международная научно-практическая конференция «Инновационные, информационные и коммуникационные технологии» (Сочи, 2022 г.); II Всероссийская научно-практическая конференция «Теория и практика обеспечения информационной безопасности» (МТУСИ, Москва, 2022 г.); XXX Российская научно-техническая конференция «Актуальные проблемы информатики, радиотехники и связи» (ПГУТИ, Самара, 2023 г.); X Международная заочная научно-практическая конференция «Информационные технологии. Радиоэлектроника. Телекоммуникации (ITRT-2023) (ПВГУС, Тольятти, 2023); VI Всероссийская молодежная научно-практическая конференция с международным участием «Информационные технологии обеспечения комплексной безопасности в цифровом обществе» (Уфа, 2023 г.).

Результаты исследования представлены на конкурсе соискателей и молодых ученых на проведение научных исследований и разработок в области информационной безопасности для задач цифровой экономики «Гранты ИБ МТУСИ» (МТУСИ, Москва, 2022 г.) – грант на 2022-2023 гг.

Краткое содержание диссертации с упором на результаты, полученные за период реализации научного проекта в рамках гранта:

В ходе реализации проекта по гранту в диссертации представлена постановка задач исследования и обзор стеганографических систем в звуковых контейнерах. Приведен краткий обзор форматов файлов и кодеков. На сегодняшний день существует достаточное количество цифровых аудиоформатов, которые делятся на несколько категорий и определяются степенью сжатия данных и уровнем, связанным с потерей качества звука:

- Аудиоформаты без сжатия (WAVE, AIFF, DSD);
- Аудиоформаты использующие сжатие без потерь (FLAC, ALAC);
- Аудиоформаты использующие сжатие с потерями (MP3, AAC).

Чтобы добиться высококачественного звучания, необходимо иметь представление о формате аудиофайла. В работе приведена сравнительная характеристика аудиоформатов. Проведение исследований аудиосигналов предполагает тщательный анализ аудиоформатов со сжатием и без него.

Форматы без сжатия обеспечивают качественное сжатие сигнала с потерей и позволяют точно описать, что можно безопасно удалить из исходного сигнала, то есть без существенного ухудшения качества звука.

В рамках исследования рассмотрен аудиоформат без сжатия WAVE, который имеет отсчеты с заданной частотой дискретизации и уровнем квантования. Данный формат относится к самому простому и часто используемым. Формат WAVE можно проанализировать с помощью метода наименьших значащих бит (LSB-метод) для эффективного встраивания информации. LSB-метод реализован в среде Python [5]. Данный метод имеет недостаток, который заключается в предварительном анализе контейнера, что исключает свою работу в реальном времени. В качестве решения данного недостатка предлагается использовать инвариантную двухкомпонентную стеганографическую систему [6-11], реализация которой осуществляется при помощи математической модели (1.1).

$$\begin{cases} y_1 = X_K \\ y_2 = u \oplus y_1 \\ Y_{n \neq N} = X_n \\ Y_N = y_2 \end{cases}, \tag{1.1}$$

где y_1 и y_2 – две информационные компоненты, u – совокупность бит секретно передаваемой информации, X – покрывающий объект, Y – стеганографический контейнер.

В качестве носителя информации используются младшие биты отсчетов X, в которые встраиваются значения компоненты y_2, являющейся функцией u и первой компоненты y_1 двухкомпонентного контейнера, являющейся отсчетом старшего бита X. В качестве функции связи между информационными компонентами и секретно передаваемой информацией используется исключающее ИЛИ $\oplus$, которая позволяет получить распределение младших бит в заполненном стеганографическом контейнере максимально близкое к распределению бит в исходном X.

Метод встраивания реализуется следующим образом. На рис. 1 приведен младший битный слой X, значения которого определены генератором случайных чисел с равномерным распределением плотности вероятности.

Младший битный слой

0	0	1	0	0	0	0	1	1	1	0	0	0	1	0	1	1	0	11/7

Рис. 1. Младший битный слой покрывающего объекта X

Рассмотрены встраивание трех различных сообщений (рис.2). Для наглядности результатов в качестве сообщений выбраны: сообщение 1 – состоящее только из единиц, сообщение 2 – только из нулей, сообщение 3 – с равномерным распределением.

Сообщение 1

1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0/18

Сообщение 2

0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	18/0

Сообщение 3

1	0	1	0	1	1	1	1	0	0	1	1	0	0	1	0	0	1	8/10

Рис. 2. Три встраиваемых сообщения

На рис.3 показан результат встраивания указанных сообщений с использованием известного метода LSB. Цветом выделены модифицированные биты X. Видно, что количество

модифицированных бит не зависит от характера распределения, а определяется соотношением младшего слоя покрывающего объекта и сообщения.

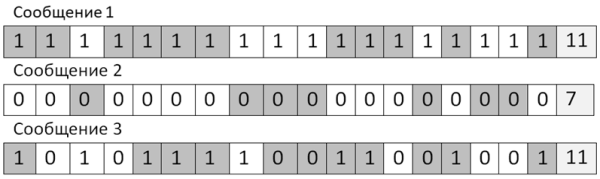


Рис. 3. Результат встраивания указанных сообщений методом LSB

Рис. 4 отражает результат встраивания сообщения в соответствии с предлагаемым методом. В качестве первой компоненты выбирается произвольный набор бит с помощью генератора случайных чисел и имитирует биты старших слоев X. Здесь цветом обозначены модифицированные биты младшего битного слоя X. Последний столбец обозначает соотношение нулей и единиц в младшем битном слое после встраивания. Как видно из рис. 5 после встраивания при использовании двухкомпонентной стеганографической системы распределение младшего битного слоя стало более равномерным, не зависимо от распределения значений сообщения. В этом случае достигается маскировка сообщения при встраивании.

Первая к.	1	0	1	1	0	1	0	0	1	0	1	1	0	1	0	0	1	0		
Сообщение 1	0	1	0	0	1	0	1	1	0	1	0	0	1	0	1	1	0	1	10	9/9
Сообщение 2	1	0	1	1	0	1	0	0	1	0	1	1	0	1	0	0	1	0	8	9/9
Сообщение 3	0	0	0	1	1	0	1	1	1	1	0	0	0	1	1	0	1	1	7	8/10

Рис. 4. Результат встраивания при использовании двухкомпонентной стеганографической системы

Для извлечения скрываемого сигнала можно воспользоваться обратным стеганографическим преобразованием, который использует следующий алгоритм (1.2):

$$\begin{cases} y_1' = Y_K \\ u' = Y_N \oplus y_1 \end{cases}, \qquad (1.2)$$

Использование предложенного способа сокрытия информации дает возможность более эффективно маскировать сообщение в младшем битном слое в реальном времени и передавать его по линии связи с последующим восстановлением. Разработана компьютерная модель в среде Python и рассмотрен вопрос маскировки встраиваемого сообщения в звуковой сигнал без сжатия с использованием двухкомпонентной стеганографической системой при варьируемом размере обрабатываемой выборки отсчетов [12]. Если встраивать отсчет в отсчет, то получается один уровень маскировки, за счет перемешивания бит. Если взять блок отсчетов, то уровень маскировки получится другой, за счет того, что есть больше вариантов откуда мы можем взять встраиваемый бит. Если данный метод применять для любого размера блока, то степень маскировки будет одинаковой. Эта система подходит как для одного отсчета звукового сигнала, так и для блока отсчетов для встраивания в реальном времени. Данный метод встраивания подходит для аудиоформата без сжатия.

Форматы со сжатием используют психологические и физиологические особенности восприятия звука человеком, так как при сжатии аудиоданных происходит снижение скорости цифрового потока за счет статистической и психоакустической избыточности. В связи с этим необходимо подробно изучить психоакустические модели всех форматов (Layer-1, Layer-2, Layer-3). Все три формата схожи, но используют разные уровни баланса между сжатием и сложностью. Уровень Layer-1 является самым простым, он не требует больших затрат на сжатие и обеспечивает небольшую степень сжатия. Уровень Layer-3 является наиболее

требовательным и обеспечивает наилучшее сжатие. В последнее время этот формат приобрел большую популярность. Его часто называют MP3.

За последние несколько лет предложено несколько эффективных моделей стандартов сжатия для высококачественного воспроизведения цифрового звука. Большинство этих алгоритмов основаны на общей структуре кодера MP3 (рис. 5). Для нас интересен блок «Преобразование», который используется для оценки временных и спектральных компонентов каждого кадра. Временную частоту часто сравнивают с характеристиками анализа слуховой системы человека, хотя это не всегда так. Цель состоит в том, чтобы извлечь набор частотно-временных параметров, которые могут быть эффективно замаскированы на основе параметров восприятия.

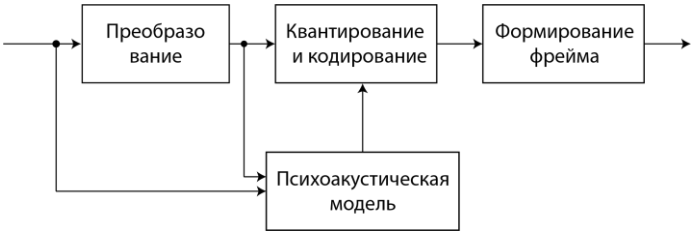


Рис. 5. Структура кодера MP3

Применение метода встраивания двухкомпонентного звукового контейнера со сжатием представляет интерес двух подходов встраивания. Первый подход заключается в встраивании перед сжатием таким образом, чтобы сжатие не искажало встраиваемое сообщение, а второй – встроить информацию в уже сжатый файл, используя психоаккустическую модель. Дело в том, что на входе алгоритма сжатия MPEG входной сигнал обрабатывается банком фильтров, что приводит к его искажению. Таким образом, встраивание сообщения перед обработкой банком фильтров приведёт к его искажению или, в случае учёта особенностей работы банка фильтров, к крайне низкой полезной нагрузке. Таким образом, предлагается реализация метода на основе модифицирования психоаккустической модели.

Рекомендации и перспективы дальнейшей разработки темы:

Аудиоформаты сжатия без потерь не представляют для нас особого интереса, потому что такие аудиоформаты работают как алгоритмы без сжатия, отличительной особенностью таких аудиоформатов является форма представления данных. А аудиоформаты, использующие сжатие с потерями представляют интересую и крайне важную задачу, так как в исследование таких аудиоформатов необходимо закладывать основу для встраивания двухкомпонентных контейнеров в VoIP системах, в частности в кодеки реального времени OPUS или SILK, или в кодек, который возможно появится в будущем. Данная работа является приоритетной задачей на будущее, которая закладывает основу для направления исследования в области стеганографии в звуке.

СПИСОК ЛИТЕРАТУРЫ

1. Грибунин, В.Г. Цифровая стеганография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев // - М.: Солон-Пресс, 2002. – 260 с.
2. Конахович, Г.Ф. Компьютерная стеганография. Теория и практика/ Г.Ф. Конахович, А.Ю. Пузыренко // - К.: «МК-пресс», 2006. – 288 с.
3. Fridrich, J. Steganography in digital media. Principles, Algorithms and applications / J.Fridrich // Cambridge university press, New York, 2010. – P. 437.
4. Караулова, О.А. Особенности оценки стеганографических систем с точки зрения стеганографического анализа / О.А. Караулова, М.В. Шакурский // Инновационные,

информационные и коммуникационные технологии: Сборник трудов XIX Международной научно-практической конференции. – 2022. – С. 66-70.
5. Караулова, О.А. Особенности использования стеганографии в звуке / О.А. Караулова, М.В. Шакурский // Теория и практика обеспечения информационной безопасности : сборник трудов II Всероссийской научно-практической конференции, Москва, 02 ноября 2022 года. – Москва: Без Издательства, 2022. – С. 14-21.
6. Shakurskiy M.V., Two-channel real-time steganographic system /Shakurskiy, M.V., Shakurskiy, V.K., Volovach, V.I.//Proceedings of IEEE East-West Design and Test Symposium, EWDTS 2014, 2014, 7027074.
7. Шакурский, М.В. Алгоритм сокрытия использования двухкомпонентного контейнера в стеганографической системе / М.В. Шакурский// Научно-практический журнал «Вопросы защиты информации». – 2020. – №3. – С. 3-5.
8. Шакурский М.В. Двухкомпонентная стеганографическая система встраивания информации в младшие биты звукового сигнала / М.В. Шакурский // Журнал «Проблемы информационной безопасности. Компьютерные системы». – 2021. – №4 (48). – С. 72-78.
9. Шакурский М.В. Двухкомпонентная стеганографическая система на основе отношения линейных функций двух сигналов, использующая аддитивный вид связи встраиваемых сигналов// Инфокоммуникационные технологии. – 2020. –Т. 18, №1 – С. 56-61.
10. Шакурский, М.В. Двухкомпонентная стеганографическая система на основе отношения линейных функций двух сигналов с размещением информативного сигнала в знаменателе функции встраивания сообщения / М.В. Шакурский, О.А. Караулова // Инфокоммуникационные технологии. – 2022. – Т. 20, № 1. – С. 118-124.
11. Шакурский, М.В. Устойчивость двухкомпонентной стеганографической системы к несанкционированному извлечению информации / М.В. Шакурский, О.А. Караулова, Е.С. Карташевская // Проблемы информационной безопасности. Компьютерные системы. – 2022. – № 4(52). – С. 20-27.
12. Шакурский, М.В. Оценка маскировки сигнала двухкомпонентной стеганографической системой при оконной обработке информации / М.В. Шакурский, О.А. Караулова // Проблемы информационной безопасности. Компьютерные системы. – 2023. – № 2(54). – С. 9-16.

Карташевская Е.С.
ФГБОУ ВО ПГУТИ, старший преподаватель кафедры программной инженерии
ka_es@bk.ru

МЕТОД ОБНАРУЖЕНИЯ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СИСТЕМАХ ИНТЕРНЕТА ВЕЩЕЙ НА ОСНОВЕ МАШИННОГО ОБУЧЕНИЯ

Аннотация: Рассматривается метод обучения «без учителя» на основе копул, использование которого помогает в полной мере раскрыть зависимость между анализируемыми факторами, что может быть успешно использовано при анализе сетевого трафика на предмет выявления аномалий. В качестве данных для исследования используется открытый набор данных IoT-23 Dataset. Набор размечен и содержит 23 фактора. Приводится сравнение точности использования указанных методов для выявления аномалий в сетях интернета вещей.

Ключевые слова: информационная безопасность, Интернет вещей, многомерные вероятностные распределения, копулы, машинное обучение.

Целью работы является исследование существующих методов и моделей машинного обучения, используемых для обнаружения угроз в сетях IoT, а также разработка модели машинного обучения, основанной на применении многомерных распределений зависимых случайных величин, выраженных через копула-функции, для обнаружения угроз информационной безопасности в сетях IoT. Задачами исследования являются: классификация угроз информационной безопасности сетей и устройств IoT, анализ применимости различных моделей машинного обучения к обнаружениям угроз в сетях IoT, разработка математической модели машинного обучения и ее программная реализация. Работы, проводимые в исследовании, являются основной частью диссертационной работы.

Научная новизна исследования заключается в использовании копул для построения моделей машинного обучения для выявления угроз информационной безопасности в сетях IoT. Выявления угроз проводится на основе анализа сетевого трафика, для описания которого применяется теория массового обслуживания и теория телетрафика, где трафик представляется в виде некоторого случайного процесса. Многомерные распределения зависимых случайных величин, выраженные через копула-функции, в полной мере раскрывают структуру зависимости между случайными величинами, поэтому оправдано их использование для выявления аномалий. Использование копул позволит существенно повысить скорость и точность вычислений для решения задач выявления угроз информационной безопасности.

Апробация работы проводилась на конференциях: Problems of Infocommunications. Science and Technology, 2019, Проблемы техники и технологии телекоммуникаций, Уфа, 2022 Телекоммуникации: теории и технологии, 2023, II Всероссийской научной школе-семинаре «Современные тенденции развития методов и технологий защиты информации», 2022

Машинное обучение представляется многообещающим решением для обнаружения угроз и защиты устройств IoT от кибератак. Данные методы могут быть применены, например, при разработке системы контроля и обеспечения безопасности сбора данных, реализующей мониторинг сетевого трафика в реальном времени [1,2], разработке системы обнаружения аномалий на основе алгоритмов машинного обучения для безопасности «умного города»[3];

создании распределенной системы обнаружения вторжений в системе сбора данных[4]; анализа сетевых аномалий для обнаружения утечек конфиденциальной информации в энергетической системе [5]. В данной работе предлагается использовать метод машинного обучения, основанный на копула-функциях, для обнаружения аномалий в сетях интернета вещей.

Копулы — это функции, которые позволяют нам отделить маргинальные распределения от структуры зависимостей данного многомерного распределения. K-мерная копула – это функция распределения случайного вектора $U = (U_1, U_2, ..., U_k)$, где маргинальные распределения являются равномерными распределениями $U(0,1)$.

$$C_U(u) = P(U_1 \le u_1, ..., U_k \le u_k),$$

где $P(U_j \le u_j) = u_j,\ j = 1, ..., k, u_j \in [0,1]$

Было доказано[6], что для любых случайных величин $(X_1, X_2, ..., X_k)$ с совместной функцией распределения $F(x_1, x_2, ..., x_k)$ и маргинальными распределениями $F_1, F_2, ..., F_k$, существует копула:

$$F(x) = C(F_1(x_1), ..., F_k(x_k))$$

Другими словами, копула позволяет нам описать совместное распределение случайных величин, используя только их маргинальные значения. Это дает большую гибкость при моделировании наборов данных большой размерности, поскольку мы можем моделировать каждое измерение отдельно, и существует гарантированный способ связать маргинальные распределения вместе для формирования совместного распределения.

Также было показано (теорема Склара) [7], что:

$$C(u) = P(F_{X_1}(X_1) \le u_1, ..., F_{X_k}(X_k) \le u_k) = F_X(F_{X_k}^{-1}(u_1), ..., F_{X_k}^{-1}(u_k))$$

Это гарантирует существование копулы для любого заданного многомерного распределения с непрерывными маргинальными распределениями.

Для разработки алгоритма выявлений аномалий используем подход, основанный эмпирических функциях.

Пусть X – набор данных размерности k, содержащий n наблюдений. Обозначим наблюдение i в измерении j как X_{ji}, X_j и X_i – измерение и наблюдение, соответственно. Эмпирическая функция распределения определяется как:

$$\hat{F}(x) = \frac{1}{n}\sum_{i=1}^{n} P(X_i \le x) \quad (1)$$

С учетом того, что равномерные распределения можно преобразовать в любые распределения:

$$X_j = F_j^{-1}(U_j) \sim F_j$$

можно получить для эмпирической копулы:

$$(\hat{U}_{1,i}, ..., \hat{U}_{k,i}) = (\hat{F}_1(X_{1,i}), ..., \hat{F}_k(X_{k,i})) \quad (2)$$

$$\hat{C}(u_1, ..., u_k) = \frac{1}{n}\sum_{i=1}^{n} P(\hat{U}_{1,i} \le u_1, ..., \hat{U}_{n,i} \le u_n)$$

Основанный на применении эмпирической копулы алгоритм включает в себя 3 шага. В качестве входного параметра используется набор данных размерности k $X = (X_{1,i}, X_{2,i}, ..., X_{k,i}), i = 1, ..., n$. Результатом является вектор оценки аномалий

$A(X) = [X_1, ..., X_n]$. Стоит отметить, что сама по себе оценка не указывает на вероятность того, что какой-либо X_i является аномалией, а является относительной мерой того, насколько более вероятно X_i является аномалией по сравнению с другими элементами в наборе данных.

На первом шаге определяются левые «хвосты» эмпирических распределений $\hat{F}_1(x), ..., \hat{F}_k(x)$ с использованием выражения (1) и правые хвосты $\hat{F}'_1(x), ..., \hat{F}'_k(x)$ путем замены *X* на *-X*. Также вычисляется вектор коэффициентов асимметрии $b = [b_1, ..., b_k]$, где:

$$b_i = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i - \bar{x}_i)^3}{\sqrt{\frac{1}{n-1}\sum_{i=1}^{n}(x_i - \bar{x}_i)^2}^3}$$

На втором шаге вычисляется эмпирическая копула согласно (2) для каждого X_i, где $\hat{U}_{k,i} = \hat{F}_k(x_i)$ и $\hat{V}_{k,i} = \hat{F}'_k(x_i)$ Далее вычисляется эмпирическая копула с поправкой на коэффициент асимметрии: если $b_k < 0$, то $\hat{W}_{k,i} = \hat{U}_{k,i}$, если $b_k \geq 0$, то $\hat{W}_{k,i} = \hat{V}_{k,i}$

На третьем шаге вычисляется непосредственно оценка аномалии. В качестве оценки принимается максимум отрицательного логарифма вероятности, определяемой левой хвостовой эмпирической копулой, правой хвостовой эмпирической копулой и эмпирической копулой с поправкой на коэффициент асимметрии.

Для оценки эффективности работы предложенной модели сравним ее с другими популярными методами обучения «без учителя», используемыми для обнаружения аномалий, такими как: метод k-ближайших соседей, оценка выбросов на основе гистограммы (Histogram-based outlier score, HBOS)[8], кластерный фактор локального выброса (Cluster-based local outlier factor, CBLOF), изолирующий лес[9]. Для анализа работы приведенных методов используем набор данных, представленный в [10]. IoT-23 Dataset — это набор данных о сетевом трафике устройств Интернета вещей (Internet of things, IoT). Впервые он был опубликован в январе 2020 года, а захваты проводились в период с 2018 по 2019 год. Сетевой трафик IoT был зафиксирован в лаборатории Stratosphere Чешского технического университета (Czech technical university, CTU). Набор данных IoT-23 состоит из двадцати трех записей (называемых сценариями) различного сетевого трафика IoT. Эти сценарии разделены на двадцать сетевых захватов (файлов *.pcap) с зараженных устройств IoT (которые имеют имя образца вредоносного программного обеспечения, выполняемого в каждом сценарии) и три сетевых захвата сетевого трафика реальных устройств IoT (с именами устройств, на которых трафик был захвачен).

Набор содержит размеченные данные об участии зараженного устройства в DDoS-атаке, в виде индикации подключений к таким ботнетам как Mirai, Okiru, Torii и др.

В данной работе использовался набор данных, который содержит 10447787 записей, которым присвоены метки «DDoS» или «Benign» (штатная работа).

Трафик «DDoS» содержит чуть больше 20% всего набора данных (2185302 элементов). Чтобы оценить точность алгоритмов обнаружения выбросов, были созданы разные наборы данных с различным содержанием пакетов, помеченных как «DDoS» в диапазоне от 0,01 до 0,99.

Теперь проанализируем работу представленных методов на сформированном наборе данных с точки зрения двух метрик. Первая - AUC (Area Under Curve, площадь под кривой)

является количественной интерпретацией кривой ошибок, т.е. площадью, ограниченной кривой ошибок и осью доли ложных положительных классификаций.

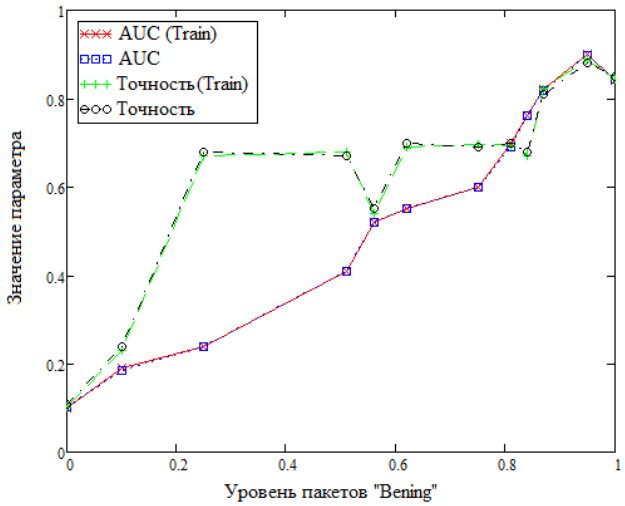


Рис. 3 – Метод CBLOF

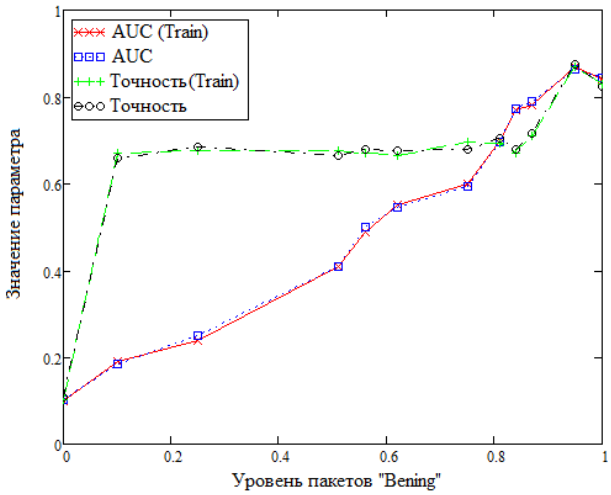


Рис. 4 – Метод HBOS

Вторая метрика – точность, показывающая количество правильно идентифицированных аномалий от общего количества событий, для каждого алгоритма. Анализ проведен на основе приложения, написанного на языке Python 3.8 с использованием библиотеки pyOD.

Также исходные данные поделены в соотношении на две выборки – «обучающую» и «тестовую» в соотношении 0.3–0.7. Поскольку используются методы машинного обучения, не предполагающие обучения, т.е. методы «без учителя», это разделение является формальным и призвано оценить эффективность работы алгоритмов на выборках разных объемов. Результаты приведены на рис.3-рис.7.

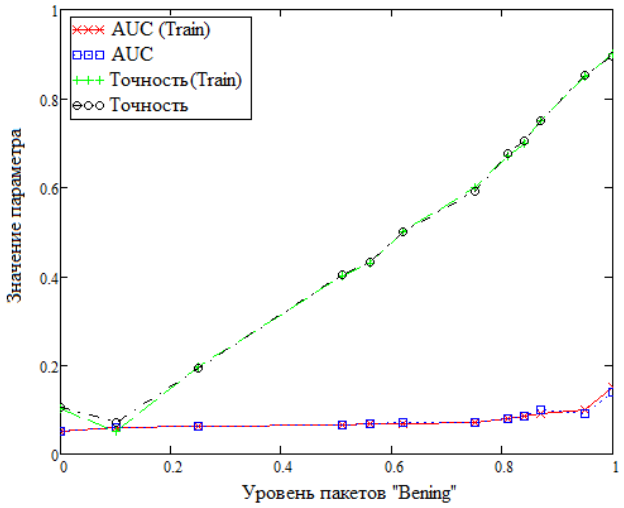


Рис. 5 – Метод *k*-ближайших соседей

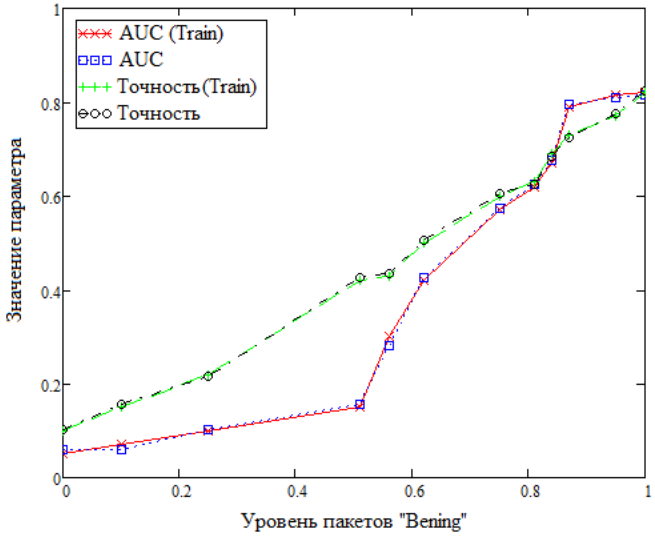


Рис. 6 – Метод изолирующего леса

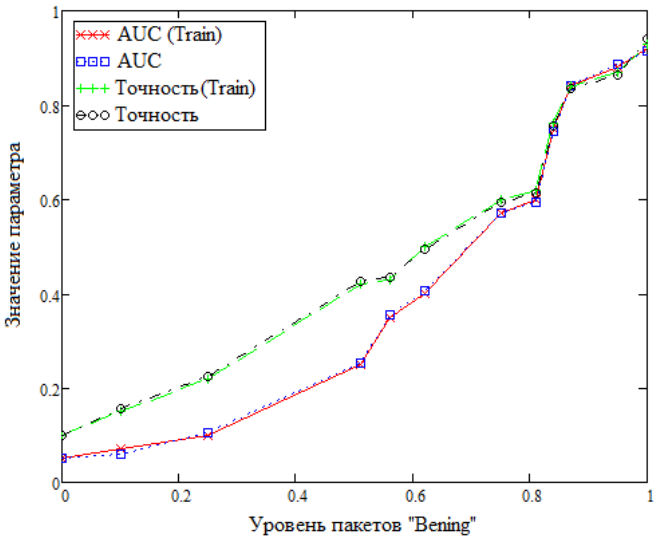


Рис. 7 – Метод на основе копул

В качестве более точного алгоритма из рассмотренных можно рассматривать алгоритм на основе копул, как имеющий наименьшее расхождение между показателями метрик и имеющий наибольшую точность при существенном увеличении количества пакетов, характеризующих штатную работу устройства. Рассмотренные методы могут выполняться без обучения, что особенно ценно для сетей Интернета вещей.

Высокая скорость работы (на исходном наборе данных, объемом 2185302 элементов, по методу на основе использования копул время выполнения составило 8.4432841 с. на процессоре AMD Athlon Gold 3150U 2.4 GHz) может позволить оптимизировать и разместить программное обеспечение в качестве HIDS, т.е. на самом устройстве IoT. В настоящее время завершаются работы по получению оценки эффективности работы данных алгоритмов на устройствах IoT, не обладающих достаточной вычислительной мощностью и оценке способности выявлять угрозы.

СПИСОК ЛИТЕРАТУРЫ

1. Ten C. W., Hong J., Liu C. C. Anomaly detection for cybersecurity of the substations // IEEE Transactions on Smart Grid. 2011. Vol. 2. № 4. P. 865-873.
2. Ten C. W., Manimaran G., Liu C. C. Cybersecurity for critical infrastructures: Attack and defense modeling // IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans. 2010. Vol. 40. № 4. P. 853-865.
3. Alrashdi I., Alqazzaz A., Aloufi E., Alharthi R., Zohdy M., Ming H. Ad-iot: Anomaly detection of iot cyberattacks in smart city using machine learning // 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC). IEEE. 2019. P. 305-310.
4. Cruz T., Rosa L., Proença J., Maglaras L., Aubigny M., Lev L., Simoes P. A cybersecurity detection framework for supervisory control and data acquisition systems // IEEE Transactions on Industrial Informatics. 2016. Vol. 12. № 6. P. 2236-2246.
5. Keshk M., Sitnikova E., Moustafa N., Hu J., Khalil I. An integrated framework for privacy-preserving based anomaly detection for cyber-physical systems // IEEE Transactions on Sustainable Computing. 2019. Vol. 6. № 1. P. 66-79.
6. Фантаццини, Д. Моделирование многомерных распределений с использованием копула-функций. II / Д. Фантаццини // Прикладная эконометрика. – 2011. – №3 (23). – с. 98-132.
7. Nelsen, R. B. An Introduction to Copulas / R.B. Nelsen // Springer Science. – 2007.- 272p.
8. He, Z. Discovering cluster-based local outliers / Z He., X. Xu, S. Deng // Pattern Recognition Letters. - vol.24(9-10). - pp.1641-1650. - 2003.
9. Ho, T.K. Random Decision Forests / T.K. Ho // Proceedings of the 3rd International Conference on Document Analysis and Recognition, Montreal, QC. – 1995. - pp. 278–282
10. Garcia, S., Parmisano A., Erquiaga M.J. IoT-23: A labeled dataset with malicious and benign IoT network traffic (Version 1.0.0) [Data set]. Zenodo. http://doi.org/10.5281/zenodo.4743746

Кучкарова Н.В.
ФГБОУ ВО «Уфимский государственный авиационный технический университет»,
старший преподаватель,
nailya_kuchkarov@mail.ru

МЕТОД И АЛГОРИТМЫ ОЦЕНКИ УЯЗВИМОСТЕЙ И УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ОСНОВЕ ТЕХНОЛОГИЙ СЕМАНТИЧЕСКОГО АНАЛИЗА ТЕКСТОВ

Аннотация: в работе проведен анализ современного состояния исследований в области применения технологии Text Mining для решения прикладных задач информационной безопасности (ИБ). Обозначены цели научного исследования, поставлены задачи, решение которых направлено на разработку интеллектуальной системы поддержки принятия решений для автоматизации оценки и приоритизации актуальных угроз, уязвимостей, тактик (техник) и построения сценариев возможных атак.

Ключевые слова: уязвимости программного обеспечения, угрозы информационной безопасности, Text Mining, векторное представление текстов, модели трансформеры, семантическая близость, сценарий реализации угроз.

Как показывает статистика последних лет, цифровизация различных отраслей экономики сопровождается ростом киберпреступлений. Так, по данным Лаборатории Касперского количество атакованных компьютеров АСУ увеличилось в 2021 г. по сравнению с 2020 г. на 2,8% [1]. Атакам подвергаются предприятия различных форм собственности и отраслей, чаще всего атакуются госсектор, энергетическая и промышленная отрасли, ВПК [2]. Предприятия упомянутых отраслей, как правило, относятся к объектам критической информационной инфраструктуры (КИИ). Большую группу объектов КИИ составляют промышленные автоматизированные системы управления технологическими процессами (АСУ ТП), требования к обеспечению информационной безопасности (ИБ) которых закреплены в ряде нормативно-правовых документов, принятых в России в последние годы, таких как: Федеральный закон «О безопасности критической информационной инфраструктуры» №187-ФЗ (2017г.), Приказы ФСТЭК России №№ 31, 235 и 239 (2017г.), «Методика оценки угроз безопасности информации» ФСТЭК России от 5 февраля 2021 г. Согласно последней Методике, одним из этапов оценки угроз безопасности информации (БИ) является оценка возможности реализации угроз БИ и определение их актуальности.

На практике при решении данной задачи специалисты по ИБ сталкиваются с необходимостью анализ угроз и уязвимостей в «ручном» режиме, что требует больших временных затрат и сопровождается ошибками обработки, обусловленными человеческим фактором, в связи с чем закономерно желание специалистов по ИБ автоматизировать процесс сопоставления угроз, уязвимостей, тактик и техник их эксплуатации. Одним из перспективных путей решения обозначенной проблемы является использование *методов и технологий интеллектуального анализа текстов (Text Mining)*.

Целью исследования является повышение достоверности и оперативности оценки актуальных угроз БИ и уязвимостей ПО объектов КИИ на основе открытых баз данных и технологий интеллектуального анализа текстов (Text Mining).

Для достижения поставленной цели необходимо решить следующие *задачи:*

1. Анализ современного состояния в области автоматизации процесса оценки и анализа актуальных угроз БИ и уязвимостей ПО объектов КИИ.

2. Разработка алгоритмов автоматической классификации и суммаризации текстов, содержащихся в специализированных открытых источниках в области информационной безопасности.

3. Разработка метода и алгоритма оценки и приоритизации множества угроз БИ для выявленных уязвимостей ПО АСУ ТП с использованием технологии семантического анализа текстов.

4. Разработка алгоритма построения графовой модели сценария реализации угроз БИ на основе алгоритмов векторного вложения и технологии трансформеров.

5. Разработка архитектуры и ПО исследовательского прототипа интеллектуальной системы поддержки принятия решений (ИСППР) в процессе оценки угроз БИ и уязвимостей ПО объектов КИИ, исследование эффективности ее применения при решении практических прикладных задач.

*Методы и методология исследования***.** Для решения поставленных в работе задач были использованы методы интеллектуального анализа данных и защиты информации, методы экспертных оценок, теории искусственных нейронных сетей, методология функционального моделирования (IDEF0), методы объектно-ориентированного анализа и проектирования, модели теории графов, методы имитационного моделирования.

Научная новизна предложенных решений:

1. Разработаны алгоритмы автоматической классификации и суммаризации текстов, содержащихся в специализированных открытых источниках в области ИБ, основанные на совместном применении алгоритмов кластеризации и извлечения признаков в виде векторов вложений, отличающиеся от известных алгоритмов возможностью осуществлять автоматизированную предобработку больших корпусов слабоструктурированных русскоязычных текстов и их последующий семантический анализ в соответствии с поставленной задачей выделения тематических направлений текстов и их автоматического реферирования на основе технологий трансформеров.

2. Разработаны метод и алгоритм автоматизированной оценки и приоритизации (ранжирования) множества релевантных угроз БИ для выявленных уязвимостей ПО на основе технологии семантического анализа текстов, отличающиеся использованием предложенного алгоритма кластеризации и оценки семантической близости текстовых описаний угроз БИ и уязвимостей ПО в многомерном векторном пространстве, применение которых позволяет сделать более содержательной работу эксперта, сократив время на поиск актуальных угроз БИ, обеспечивая при этом более высокую наглядность, полноту и достоверность результатов такого поиска.

3. Разработан алгоритм построения графовой модели сценария реализации актуальных угроз БИ на основе оценки семантической близости текстовых описаний соответствующих угроз БИ, уязвимостей ПО, тактик и техник действий нарушителя, отличающийся использованием алгоритмов векторного вложения и технологии трансформеров, что позволяет автоматизировать процесс построения графовой модели, снизить трудоемкость и когнитивную нагрузку на специалистов по ИБ, предоставляя им дополнительную информацию для формирования перечня актуальных угроз и уязвимостей объектов КИИ.

4. Предложены архитектура и состав программных модулей ИСППР, реализующих предложенные в работе метод и алгоритмы, применение которых позволяет снизить

временные затраты и повысить достоверность решений, принимаемых специалистом по ИБ при оценке и анализе актуальных угроз БИ и уязвимостей ПО объектов КИИ.

Далее будут представлены решенные в рамках научного исследования задачи.

В рамках решения задачи 1 проведен анализ современного состояния в области обеспечения ИБ АСУ ТП. Проанализированы требования современной нормативно-правовой базы в области ИБ АСУ ТП. Выполнен обзор научных публикаций в области автоматизации оценки, анализа и приоритизации угроз и уязвимостей с использованием методов интеллектуального анализа как зарубежных, так и отечественных ученых. Так, работы [3-7] посвящены выявлению уязвимостей и оценке степени их серьезности (критичности) на основе семантического анализа текстовых описаний уязвимостей. В статьях Селифанова В. В. и др. [8,9,10] предложена методика выявления взаимосвязей между обнаруженными уязвимостями и угрозами безопасности информации. Источником описаний угроз и уязвимостей является БДУ ФСТЭК России.

Дан краткий обзор открытых баз данных NDV, CVE, CAPEC, БДУ ФСТЭК России др., содержащих текстовые описания угроз ИБ, уязвимостей ПО, тактик (техник). Проведен сравнительный анализ алгоритмов для обработки текстовых описаний на естественном языке (ЕЯ): Word2Vec, Doc2Vec, TF-IDF, BERT (трансформеры).

Отмечено, что существующие методы и алгоритмы анализа и оценки угроз и уязвимостей не соответствуют в полной мере требованиям Методики ФСТЭК. Показана необходимость автоматизации процесса оценки и ранжирования (приоритезации) актуальных угроз БИ и уязвимостей ПО с использованием технологий интеллектуального анализа текстов (Text Mining), что позволит снизить трудоемкость работ связанных с определением актуальных угроз и уязвимостей.

В рамках решения задачи 2 исследуется возможность применения технологий Text Mining при решении задач автоматической классификации (тематического моделирования) и суммаризации текстов из открытых источников в области ИБ. Описываются общие подходы к решению задач автоматической классификации и суммаризации текстов [11-14]. Получены результаты экспериментов по автоматической классификации слабоструктурированой информации на примере корпуса текстов, сформированного из 438 полнотекстовых научных статей, опубликованных в журнале «Вопросы кибербезопасности» за 2013- 2022 гг. В процессе этих экспериментов исследовались различные подходы к классификации (кластеризации) указанных документов: с предварительным понижением размерности признакового пространства и использованием метода ближайших соседей (K-Means); с помощью скрытого распределения Дирихле (LDA) и неотрицательной матричной факторизации (NMF); на основе моделей векторных вложений (Text Rank, SBert). Были выполнены также эксперименты по автоматической суммаризации текстов для формирования кратких рефератов, раскрывающих смысловое содержание документа.

Были сделаны выводы о том, что использование данных технологий позволяет повысить качество анализа текстовых документов в области ИБ и одновременно снизить когнитивную нагрузку на эксперта.

Задача 3. Приведена функциональная модель процесса оценки и анализа актуальных угроз БИ в соответствии с Методикой ФСТЭК. Показано, что основные сложности при работе с данной Методикой связаны с определением сценариев реализации угроз БИ, в силу необходимости использования при этом разнородной слабоструктурированной информации, включающей перечни актуальных уязвимостей ПО, типы доступа к информационным

активам, типы нарушителей и т.п., а также ввиду отсутствия эффективных средств автоматизации, позволяющих формализовать и упростить процесс сопоставления имеющихся исходных данных (актуальных уязвимостей ПО, тактик (техник) их реализации, возможных угроз БИ).

Разработан метод и алгоритм решения задачи автоматизации оценки и приоритизации актуальных угроз БИ и уязвимостей ПО объектов КИИ с использованием технологий интеллектуального анализа текстов (Text Mining). Проанализированы ключевые этапы обработки текстовых описаний с применением указанных технологий, рассмотрены особенности использования алгоритмов Word2Vec, Doc2Vec, BERT в задачах обработки текстовых описаний угроз БИ и уязвимостей ПО.

Разработан алгоритм оценки и приоритизации актуальных угроз БИ и уязвимостей ПО с использованием технологий Text Mining. Для апробации предложенного метода и алгоритма анализировались текстовые данные из БДУ ФСТЭК. Из общего объема текстовых описаний в 740634 слова был сформирован словарь, содержащий 12884 слов. После процедуры предобработки и нормализации данных была построена модель векторных вложений Doc2Vec с помощью фреймворка Gensim.

В основе алгоритма оценки и приоритизации множества угроз БИ для выявленных уязвимостей ПО лежит построение матриц оценок попарной семантической близости элементов двух множеств: M^{TT_Vu} тактик (техник) (TT) и уязвимостей (Vul), M^{TT_Th} тактик (техник) (TT) и угроз (Th). Далее матрицы сортируются построчно в порядке убывания метрики семантической близости текстовых описаний элементов множеств, с обрезкой по количеству элементов в строке: для угроз БИ остается $p = 10$ наиболее схожих, для уязвимостей ПО $q = 25$ наиболее схожих с текстовым описанием тактик (техник). В качестве меры оценки семантической близости используется косинусная мера, позволяющая вычислить расстояние между двумя векторами в семантическом пространстве признаков

Разработан алгоритм построения графовой модели фрагмента сценария реализации угроз с использованием Word2Vec, Doc2Vec и технологии трансформера Построение графовой модели начинается с подготовки текстовых описаний угроз, уязвимостей, тактик и техник. Затем на основе ссылочных описаний устанавливаются связи между вершинами V_1, V_2, V_3 , V_4 . Далее строится матрица семантической близости описаний угроз БИ, уязвимостей ПО, тактик и техник, несуществующие связи прореживаются на основе порогового значения. В заключение производится оценка и приоритизация рассмотренных множеств угроз БИ и уязвимостей ПО.

Далее, при построении графовой модели, описывающей отношения множеств угроз БИ, уязвимостей ПО, тактик и техник их эксплуатации, используется технология трансформеров, в частности нейросетевая языковая модель BERT (Bidirectional Encoder Representations from Transformers), основанная на объединении стека нейросетевых кодировщиков с механизмом внутреннего внимания (Self-Attention). Особенностью построения трансформера является двунаправленная обработка входных слов, что сокращает вычислительные затраты и повышает качество обучения языковой модели.

Дальнейший анализ (сопоставление) формализованных представлений текстовых описаний угроз БИ, уязвимостей ПО, техник (тактик) основан на применении методов кластеризации многомерных данных. Визуализация полученной графовой модели показывает, что наилучший результат демонстрирует предобученная модель-трансформер BERT – Large Model. Модель ruBERT-tiny (дистиллированная модель-трансформер многозадачного

обучения) также демонстрирует заметное распределение на компактные группы объектов в семантическом векторном пространстве в соответствии с семантической близостью их описаний. Результаты проведения эксперимента с применением модели BERT- Large Model для заданной уязвимости BDU:2021-02033 показывают высокую степень совпадения экспертных оценок и предложенных сценариев реализации угроз БИ.

В рамках решения задачи 4. разработана структурно-функциональная схема исследовательского прототипа ИСППР, предназначенной для автоматизации процесса оценки актуальных угроз БИ.

Ключевым элементом системы является механизм сопоставления текстовых описаний уязвимостей, тактики (техник) и связанных с ними угроз БИ, что позволяет уточнить сценарий реализации угроз, и кроме того, осуществить приоритезацию указанных угроз с учетом дополнительной информации о наличии зависимостей между угрозами и уязвимостями ПО.

Получены результаты двух серий экспериментов, проведенных для АСУ ТП объекта нефтепереработки: сопоставления тактик (техник), наиболее близких угроз БИ и уязвимостей ПО, выявленных в ходе анализа ПО АСУ ТП с помощью сканеров безопасности или определенных экспертом.

Результаты проведенных экспериментов показали, что время, затраченное на построение сценариев экспертным способом, составило более 4 часов, при работе эксперта с применением ИСППР затрачено менее 40 минут, согласованность экспертной оценки и ИСППР F1 составила 0,59.

Семантический анализ текстовых описаний уязвимостей, угроз, тактик (техник) с использованием предлагаемых решений позволяет повысить достоверность и оперативность принимаемых решений, снизить когнитивную нагрузку на специалистов по ИБ в ходе проведения работ по оценке уровня защищенности объекта КИИ.

В рамках диссертационной работы получены следующие научные и практические *результаты:*

1.Разработаны алгоритмы автоматической классификации и суммаризации текстов, содержащихся в специализированных открытых источниках в области ИБ, отличающиеся от известных алгоритмов возможностью осуществлять автоматизированную предобработку больших корпусов слабоструктурированных русскоязычных текстов и их последующий семантический анализ в соответствии с поставленной задачей выделения тематических направлений текстов и их автоматического реферирования.

2. Разработаны метод и алгоритм автоматизированной оценки и приоритизации (ранжирования) множества релевантных угроз БИ для выявленных уязвимостей ПО на основе технологии семантического анализа текстов, отличающиеся использованием предложенного алгоритма кластеризации и оценки семантической близости текстовых описаний угроз БИ и уязвимостей ПО в многомерном векторном пространстве, применение которых позволяет сделать более содержательной работу эксперта, сократив время на поиск актуальных угроз БИ, обеспечивая при этом более высокую наглядность, полноту и достоверность результатов такого поиска.

3. Разработан алгоритм построения графовой модели сценария реализации актуальных угроз БИ на основе оценки семантической близости текстовых описаний соответствующих угроз БИ, уязвимостей ПО, тактик и техник действий нарушителя, отличающийся использованием алгоритмов векторного вложения и технологии трансформеров, что позволяет полностью автоматизировать процесс построения графовой модели, снизить

трудоемкость и когнитивную нагрузку на специалистов по ИБ, предоставляя ему дополнительную информацию для формирования перечня актуальных угроз и уязвимостей объектов КИИ.

4. Предложены архитектура и состав программных модулей ИСППР, реализующих предложенные в работе метод и алгоритмы, применение которых позволяет снизить временные затраты и повысить достоверность решений, принимаемых специалистом по ИБ при оценке и анализе актуальных угроз БИ и уязвимостей ПО объектов КИИ.

Результаты представленных разработок внедрены в производственные и бизнес-процессы предприятий г. Уфы: ЗАО «Республиканский центр защиты информации», ООО «УРАЛТЕХСИСТЕМЫ», ФГБОУ ВО «Уфимский университет науки и технологий».

Исследование выполнено при поддержке Гранта ИБ МТУСИ (Соглашение № 40469-18/2022-к).

СПИСОК ЛИТЕРАТУРЫ

1. Ландшафт угроз для систем промышленной автоматизации. Kaspersky ICS CERT. [Электронный ресурс]: — Режим доступа: https://ics-cert.kaspersky.ru/reports/2020/09/15/threat-landscape-for-industrial-automation-systems-h1-2020/#_Toc49436674 (дата обращения 01.08.2022).
2. Актуальные киберугрозы: итоги 2021 года. Positive Technologies. [Электронный ресурс]: — Режим доступа: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2021/ (дата обращения 01.08.2022).
3. Han, Z Learning to Predict Severity of Software Vulnerability Description / Z. Han, X. Li, Z. Xing, H. Liu, Z. Feng // Proceedings of the 2017 International Conference on Software Maintenance and Evolution (ICSME) — 2017. — P. 125-136.
4. Lee, Y.Toward Semantic Assessment of Vulnerability Severity: A Text Mining Approach / Y. Lee, S. Shin // Proceedings of ACM CIKM Workshop (EYRE’ 18) — 2018. [Электронный ресурс]. — Режим доступа: https://www.CEUR-WS.org/Vol1-2482/papers.pdf (дата обращения 01.08.2022).
5. Spanos, G. Assessment of Vulnerability Severity using Text Mining / G. Spanos, L. Angeis, D. Toloudis // Proceedings of the 21st Pan-Hellenic Conference. — 2017 — P. 1-6.
6. Tao, Wen A Novel Automatic Severity Vulnerability Assessment Framework / Wen Tao, Zhang Yuquing, Yang Gang. // Journal of Communications. — 2015. — Vol. 10. №5. — P. 320-329.
7. Доронин, А.К. Предсказательная модель машинного обучения для решения задачи классификации уязвимостей компьютерных систем / А.К. Доронин, В.А. Липницкий // Материалы Междунар. научн. конф. «Информационные технологии и системы» (ИТС 2018). — Минск: 2018. — С. 94-95.
8. Полетаева В.С. Информационно-аналитическая система прогнозирования угроз и уязвимостей информационной безопасности на основе анализа данных тематических интернет-ресурсов: автореферат на соискание ученой степени канд. техн. Наук. — Ульяновск: 2020. — 19 с.
9. Селифанов, В. В. Применение методов автоматизации при определении актуальных угроз безопасности информации в информационных система с применением банка

данных угроз ФСТЭК России / В. В. Селифанов [и др.] // Интерэкспо Гео-Сибирь. — 2017. — Т. 8. — С.202-209.
10. Селифанов, В.В. Методика автоматизированного выявления взаимосвязей уязвимостей и угроз безопасности информации в информационных системах / В.В. Селифанов, Я.В. Юракова, И.Н. Картамов // Интерэкспо Гео-Сибирь. — 2018. — С. 271–276.
11. Болодурина, И.П. Автоматизированное машинное обучение: обзор возможностей современных платформ анализа данных / И.П. Болодурина, Д.И. Парфенов, А.Е. Шухман, Л.С. Забродина // Системная инженерия и информационные технологии. – 2021. – Т. 3. – № 1(5). – С. 50–57.
12. Мусаев, А.А. Обзор современных технологий извлечения знаний из текстовых сообщений / А.А. Мусаев, Д.А. Григорьев // Компьютерные исследования и моделирование. – 2021. – Т. 13. – № 6. – С. 1291–1315. – DOI 10.20537/2076- 7633-2021-13-6-1291-1315.
13. Sethi, P. Automatic text summarization of news articles / P. Sethi, S. Sonawane, S. Khanwalker, R.B. Keskar // 2017 International Conference on Big Data, IoT and Data Science (BID). – IEEE. – 2017. – pp. 23–29.
14. Summarization with Transformers: Setting up for Success [Электронный ресурс]. – Режим доступа: https://www.sicara.fr/blog-technique/summarization-withtransformers-setting-up-for-success (дата обращения 20.12.2022).

Лансере Н.Н.
Санкт-Петербургский государственный университет телекоммуникаций
им. проф. М.А.Бонч-Бруевича, ассистент кафедры защищенных систем связи
Управление ФСТЭК России по Северо-Западному федеральному округу, начальник отдела
nlansere@yandex.ru

МОДЕЛИРОВАНИЕ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИМИ ПРОЦЕССАМИ НА КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТАХ

Аннотация: В исследовании рассматриваются субъекты критической информационной инфраструктуры (КИИ), использующие автоматизированные системы управления (АСУ) на критически важных объектах (КВО), которые функционируют в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической, химической промышленности, а также в сфере здравоохранения, науки, транспорта, связи, и энергетики в пределах Северо-Западного федерального округа. АСУ представляют собой комплекс программных и программно-аппаратных средств, предназначенных для контроля за технологическим, производственным оборудованием и производимыми ими процессами. Определены и конкретизированы применительно к особенностям функционирования АСУ ТП КВО типовые компьютерные инциденты относительно источников угроз безопасности информации, в том числе потенциальный ущерб от непроизводительных потерь, заключающийся в уменьшении объема, ухудшении качества добываемой или производимой продукции в определенный отрезок времени.

Ключевые слова: автоматизированная система управления, критическая информационная инфраструктура, критически важные объекты, деструктивные воздействия, сетевые атаки, угрозы безопасности информации, информационная безопасность, базовая модель угроз, риски безопасности, модель нарушителя, квалиметрия.

Благодаря развитию общества и цифровых технологий, создаются новые антропогенные угрозы безопасности информации и увеличивается количество интерфейсов воздействия [1]. Условием, позволяющим нарушителям использовать способы реализации угроз безопасности информации, является наличие у них возможности доступа к интерфейсам объектов воздействия.

Постановление Правительства Российской Федерации [2] обязывает все субъекты критической информационной инфраструктуры, в отношении принадлежавших им на праве собственности, аренды или любых других законных основаниях (информационные системы (ИС), информационно-телекоммуникационные сети (ИТКС), автоматические системы управления (АСУ)), функционирующие в 13 основных направлениях деятельности, а также проводить категорирование объектов критической информационной инфраструктуры [3].

В исследовании будут рассматриваться субъекты критической информационной инфраструктуры, использующие АСУ ТП на критически важных объектах (КВО), при этом исследование не ограничивается значимыми объектами, а охватывает все АСУ ТП функционирующие в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической, химической промышленности, а также в сферах здравоохранения, науки, транспорта, связи, и энергетики. Серьезной угрозой для таких

предприятий является возможность деструктивного воздействия на элементы АСУ ТП КВО верхнего уровня (серверы, пользовательские АРМ), включая особенности удаленного доступа и технического обслуживания.

Количество сетевых атак на промышленные информационные системы продолжает возрастать, соответственно увеличивается заинтересованность предприятий в защите своей информационной инфраструктуры. Всего за 2022 год в промышленных компаниях было зафиксировано 223 инцидента, вызванных атаками злоумышленников, что на 7% больше, чем в 2021. (Почти все атаки (97%) были целевыми)

Важным фактором эффективной работы АСУ ТП КВО является ее состояние защищенности, которое будет оцениваться в устойчивом (бесперебойном) функционировании всех систем и сетей, в том числе при воздействии на неё целевых компьютерных атак.

В рамках исследования будут определены критически важные объекты, где отсутствие комплексной защиты АСУ ТП представляет повышенную опасность для жизни и здоровья людей и для окружающей природной среды, дополнительно результатом успешно проведенной компьютерной атаки может быть нанесение вреда в экономической сфере, в обеспечении обороны страны, безопасности государства и правопорядка.

Причины, по которым задачи по защите АСУ ТП КВО являются актуальными по мнению автора следующие:

− открытость и доступность универсальных технологий и протоколов, которые применяются в АСУ ТП;

− общая с АСУ ТП информационная инфраструктура предприятий;

− большое количество импортного оборудования и программного обеспечения, применяемого в АСУ ТП;

− совершенствование производственных процессов путем внедрения цифровых технологий и появление новых нормативных требований по защите АСУ ТП и обеспечению безопасности критической информационной инфраструктуры Российской Федерации;

отсутствие мероприятий по информационной безопасности в случае неправильного категорирования АСУ ТП или бездействия должностных лиц (отсутствие мероприятий по категорированию и созданию систем безопасности).

В соответствии с темой диссертационной работы «Модели и методика оценки защищенности информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах (АСУ ТП КВО)» в рамках проводимого исследования проанализированы результаты мониторинга сведений о публикуемых критических уязвимостях программного обеспечения критической информационной инфраструктуры, а также связанных с ними компьютерными атаками.

На основании сведений, полученных из общедоступных источников информации в период с 28 февраля 2022 г. по настоящее время оценено влияние целевых компьютерных атак на состояние защищенности критической информационной инфраструктуры Российской Федерации.

Анализ сведений об угрозах безопасности информации, проводимый специалистами ФСТЭК России в условиях сложившейся обстановки, показывает, что зарубежными хакерскими группировками при реализации компьютерных атак на информационную инфраструктуру Российской Федерации активно эксплуатируются следующие уязвимости программного обеспечения:

Уязвимости микропрограммного обеспечения веб-панелей для управления

и мониторинга процессов в промышленных системах;

уязвимости операционных систем, связанные с ошибками при управлении доступом.

Инциденты, приведшие к масштабным негативным последствиям, в 48% случаев были связаны с действиями внутренних нарушителей или обусловлены недостаточной парольной защитой. Число предоставляемых доступов к инфраструктуре организаций (индентификациооные и аутентификационные данные), выставленных в 2022 году на продажу, выросло более чем на 40% с 86 до 122. Доступы составляют 75% процентов всех объявлений о продаже пар логин-пароль, относящихся к АСУ ТП, а их стоимость обычно колеблется от 500 до 5000 долларов [4].

«Лаборатория Касперского» сообщила, что в первые 5 месяцев текущего года на территории РФ процентное соотношение блокированных вредоносных программ на ПК АСУ ТП достигла 31,3%. Это на 4,5% больше, чем в том же природе 2022 года (26,8%). Эксперты утверждают, что рост обусловлен увеличением числа компьютерных атак. Даже если промышленная сеть изолирована, атаки могут проходить через устройства, с помощью которых работники заходят в Интернет. Отчет Kaspersky ICS CERT выделяет три основные области с наибольшей долей зараженных компьютеров АСУ ТП: инжиниринг и интеграция АСУ (33,8%), автоматизация зданий (32%) и энергетический сектор (30,6%). Основные угрозы безопасности на промышленных предприятиях связанны с устаревшим ПО, отключением или отсутствием защиты и неправильной настройкой сети [5].

Цель научного исследования заключается в совершенствовании методов и средств технической защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах.

Задачами научного исследования являются:

анализ актуальных угроз безопасности информации, циркулирующей в АСУ ТП КВО;

совершенствование способов противодействия угрозам безопасности информации и обеспечения информационной безопасности АСУ ТП КВО;

разработка и совершенствование методов оценки эффективности системы технической защиты АСУ ТП КВО.

Исследования в области оценки рисков информационной безопасности отражены в работах С.А. Агеева [6], И.М. Ажмухамедова [7], И.В. Аникина [8], Е.К. Барановой [9], Т.И. Булдаковой [10], А.П. Глухова [11], А.А. Кононова [12] , А.Г. Кравец [13], С.С. Козунова [14], Н.Г. Милославской [15].

Анализ отмеченных исследований показал, что при оценке рисков недостаточно учитывается специфика АСУ ТП КВО, к примеру, упускается наносимый потенциальный ущерб от непроизводительных потерь, заключающийся в уменьшении объема добываемой или производимой продукции в определенный отрезок времени, или увеличении общего времени выпуска продукции (простоя, ремонта, восстановления работоспособности АСУ ТП КВО).

В целях практического внедрения разрабатывается типовая модель нарушителя и угроз безопасности информации АСУ ТП КВО, с привязкой к базовой модели для конкретной отрасли субъектов критической информационной инфраструктуры, являющихся КВО. Данные модели учитывают реальные критические процессы организаций с учетом особенностей субъектов КИИ и включают критерии (метрики) для проведения комплексной оценки защищенности АСУ ТП КВО.

Исследованиям в области анализа защищенности информационной инфраструктуры, а также применение различных методов выявления уязвимостей посвящены работы А.В. Барабанова [16], М.В. Буйневича [17,18], М.А. Еремеева [19], А.К. Новохрестова [20], В.В. Платонова [21]. Однако проблемы распознавания уязвимостей в современных АСУ ТП КВО остаются актуальными, из-за специфики коммуникации сетей АСУ ТП и информационной инфраструктурой предприятий.

Большой вклад в решение задач по обеспечению управления ИБ компьютерных, информационных и автоматизированных систем управления КИИ, в т.ч. АСУ ТП, внесли работы ученых: Д.П. Зегжда, П.Д. Зегжда, А.А. Кононов, И.В. Котенко, И.И. Лившиц, И.Б. Паращук, Д.С. Черешкин, В.Д. Чертовской. Актуальным остается совершенствование способов противодействия угрозам безопасности информации и обеспечения информационной безопасности АСУ ТП КВО

Начиная с 24 февраля 2022 г. по настоящее время в ходе рабочих поездок на предприятия, являющимися субъектами критической информационной инфраструктуры автором проводится контроль реализации мероприятий по повышению защищенности объектов информационной инфраструктуры Российской Федерации. В ходе контроля проведен анализ информационной инфраструктуры больше 250 предприятий по результатам которого отмечаются разные подходы в организации функционирования информационной инфраструктуры, в том числе на уровне сетевого взаимодействия (физического и логического), а также применяемых организационных и технических мер. В зависимости от сферы или области функционирования АСУ ТП различаются границы оценки угроз безопасности информации, категории нарушителей и интерфейсы воздействия.

В рамках исследования проведены:

анализ рисков нарушения безопасности информации и уязвимости процессов обрработки информации, циркулирующей в АСУ ТП КВО (**определены и конкретизированы** применительно к особенностям деятельности АСУ ТП КВО типовые компьютерные инциденты и категории актуальных нарушителей);

разработка модели и способов противодействия угрозам нарушения безопасности информации в АСУ ТП КВО и оценки ее защищенности (**в отличие от известных методик** конкретизированы критерии оценки защищенности АСУ ТП КВО);

разработка методики оценки эффективности системы технической защиты информации АСУ ТП КВО (определить базовый набор мер по обеспечению безопасности АСУ ТП КВО и **повысить уровень их защищенности**).

Данные научные и научно-технические результаты должны способствовать противодействию компьютерным атакам и иным источникам опасности для общества, экономики и государства в соответствии с подпунктом Д пункта 20 Стратегии научно-технологического развития Российской Федерации.

В настоящий момент основные публикации по теме исследования:

Организация концептуальной модели критической информационной инфраструктуры / А. М. Гельфанд, Н. Н. Лансере, А. А. Ложкина, И. И. Фадеев // Методы и технические средства обеспечения безопасности информации. – 2020. – № 29. – С. 39-40. – EDN PYPOHZ;

Внедрение методологии быстрой оценки объектов критической инфраструктуры для учреждений образования // Управление образованием: теория и практика / Education Management Review Том 12 (2022). No2 / Volume 12 (2022). Issue 2. С. 10-16.

Пермякова, М. А. Анализ риска вывода значимого объекта КИИ из строя в условиях реализации угрозы перехвата управления АСУ ТП / М. А. Пермякова // Сборник трудов X Конгресса молодых ученых : Материалы Конгресса, Санкт-Петербург, 14–17 апреля 2021 года. Том 1. – Санкт-Петербург: федеральное государственное автономное образовательное учреждение высшего образования "Национальный исследовательский университет ИТМО", 2021. – С. 175-179. – EDN KXBPCN.

Актуальные угрозы безопасности информации в сфере здравоохранения и офтальмологии / А. В. Красов, Д. Н. Шакин, Н. Н. Лансере [и др.] // Офтальмохирургия. – 2022. – № S4. – С. 92-101. – DOI 10.25276/0235-4160-2022-4S-92-101. – EDN IYQQXV.

Организация концептуальной модели критической информационной инфраструктуры / А. М. Гельфанд, Н. Н. Лансере, А. А. Ложкина, И. И. Фадеев // Методы и технические средства обеспечения безопасности информации. – 2020. – № 29. – С. 39-40. – EDN PYPOHZ.

Типовые офтальмологические информационные системы, являющиеся объектами критической информационной инфраструктуры / А. В. Красов, Н. Н. Лансере, И. И. Фадеев [и др.] // Офтальмохирургия. – 2022. – № S4. – С. 85-91. – DOI 10.25276/0235-4160-2022-4S-85-91. – EDN CBKURN.

Методы исследования базируются на положениях теории системного анализа, математического моделирования, теории вероятности и методологии теории рисков.

На многих предприятиях для систематического выполнения работ по повышению качества продукции широкое распространение получили системы бездефектной работы и управления качеством.

Реальная полезность таких мероприятий бесспорна. Однако и теоретический анализ, и практическое опробование подобных мероприятий свидетельствуют, что в большинстве случаев не полностью достигается потенциально возможный эффект, который с точки зрения теории могли бы дать системы управления качеством продукции. Дело в том, что при разработке этих мероприятий нередко не учитываются некоторые важные положения, обоснованные в квалиметрии, в теории систем и в теории управления.

Актуальной остается задача повышения успешности функционирования мероприятий по улучшению качества в любой из сфер применения. С точки зрения теории организации управления для обеспечения успешности функционирования любой работы, необходимо, чтобы все силы и средства систем безопасности реализовывали необходимые требования по защите систем. С целью повышения защищенности АСУ ТП, и их устойчивого функционирования необходима оценка следующих факторов:

что должно являться критериями для проведения мероприятий по защите по улучшению защищенности систем;

цели и задачи организационных и технических мероприятий по защите информации;

когда (на каких этапах жизненного цикла АСУ ТП) должны проводиться эти мероприятия;

оценка эффективности проведенных мероприятий и качество их выполнения.

Положения, выносимые на защиту.

1. Разработка типовой модели нарушителя безопасности информации на АСУ ТП КВО.

На основе анализа рисков нарушения безопасности информации и уязвимости процессов обработки информации, циркулирующей в АСУ ТП КВО разработана типовая модель нарушителя безопасности информации. Определены особенности и возможности нарушителей по категориям. Учтена специфика АСУ ТП КВО в масштабе федерального

округа. Уменьшено кол-во актуальных категорий нарушителя. Определены и конкретизированы применительно к особенностям функционирования АСУ ТП КВО типовые компьютерные инциденты относительно источников угроз безопасности информации. Разработанная модель нарушителя, позволяет уменьшить временные затраты на актуализацию категорий нарушителя на АСУ ТП КВО.

Автором проведен анализ подсистем безопасности АСУ ТП КВО на основе исследования рисков безопасности информации и слабых мест в системе обработки данных АСУ ТП КВО была создана модель типового нарушителя. Эта модель позволяет классифицировать нарушителей по различным категориям, учитывая их возможности и методы. При этом учитывается уникальная специфика работы различных АСУ ТП КВО рассматриваемых в объеме федерального округа. Разработанная модель позволит сократить количество релевантных категорий нарушителей. Также были выявлены типовые инциденты, связанные с компьютерной безопасностью, и их источники применительно к АСУ ТП КВО. В результате внедрения модели прогнозируется снижение времени, необходимое для анализа и классификации нарушителей в системе. Обобщены достоверные данные в масштабе федерального округа, автором проведен анализ информационных систем более 200 организаций.

Научно-исследовательская работа позволила разработать типовую модель угроз для АСУ ТП КВО, функционирующих в различных областях и сферах. В целях выполнения задач, решаемых в ходе оценки угроз, исходя из сферы деятельности субъекта были определены объекты критической информационной инфраструктуры, реализующие критические процессы. Разработанная типовая модель угроз объекта КИИ, являющегося АСУ ТП (пункт 3 паспорта специальности 2.3.6.) систематизирует виды и категории актуальных нарушителей и последовательности тактик и техник, применение которых может привести к реализации угроз безопасности информации и позволяет совершенствовать процесс моделирования актуальных угроз безопасности информации в АСУ ТП КВО, выработать рекомендации по парированию угроз безопасности и содержит информацию о мерах защиты информации, направленных на нейтрализацию угроз.

Достоверность результатов обеспечивается корректным применением общенаучных методов исследования, подтверждается апробацией полученных результатов на практике и хорошей корреляцией с известными исследованиями.

2. Разработка моделей и способов противодействия угрозам нарушения безопасности информации в АСУ ТП КВО

Автором разработана модель и способы противодействия для каждой сферы и области функционирования субъектов критический информационной инфраструктуры типовые модели угроз для АСУ ТП (пункт 5 паспорта специальности 2.3.6.), а также определены угрозы безопасности информации, для актуальных нарушителей и выработаны способы противодействия по каждой из угроз.

Способы противодействия ориентируются на источники угроз, являющиеся актуальными нарушителями для АСУ ТП КВО.

Ожидается сокращение времени на разработку и внедрение организационных и технических мер и повышение их эффективности

Определены угрозы безопасности информации и способы противодействия им по отношению к конкретным категориям актуальных нарушителей на АСУ ТП КВО

По результатам апробации дополнены и актуализированы способы противодействия актуальным угрозам безопасности информации, циркулирующей на АСУ ТП КВО

Создаются стандартные модели угроз для АСУ ТП для каждой области критической информационной инфраструктуры.

Идентифицированы ключевые угрозы безопасности информации, соответствующие актуальным нарушителям.

Выработаны конкретные методы противодействия на основе исходных данных об угрозах.

Основной фокус направлен на актуальные источники угроз для АСУ ТП КВО. Ожидается, что новые методы уменьшат время на разработку и внедрение мер безопасности и повысят их эффективность. Угрозы и методы противодействия категорированы в зависимости от конкретных актуальных нарушителей. Дополнены и обновлены способы для соответствия текущим угрозам безопасности в АСУ ТП КВО. Достоверность результатов обеспечивается надежными исходными данными.

3. Разработка Методики оценки защищенности информации в автоматизированных системах управления производственными и критериев оценки качества функционирования подсистемы защиты информации на АСУ ТП КВО.

Сокращение временных и трудовых затрат для проведения внутреннего контроля

Применение подходов теории квалиметрии в области защиты информации, циркулирующей на АСУ ТП КВО

Обеспечение повышения качества проведения внутреннего контроля.

(**пункт 10 паспорта специальности 2.3.6.**)

Защита диссертации пройдет в рамках диссертационного совета по защите диссертаций, как на соискание ученой степени кандидата наук, так и на соискание ученой степени доктора наук 99.2.038.03, созданного на базе университетов: "Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича (СПбГУТ)", "Санкт-Петербургский государственный университет аэрокосмического приборостроения (ГУАП)" и "Балтийский государственный технический университет «ВОЕНМЕХ» им. Д.Ф. Устинова".

Заключение.

В работе использованы результаты, в которых автору принадлежит определяющая роль. Часть опубликованных (публикуемых) работ и написана в соавторстве с сотрудниками СПбГУТ и Управления ФСТЭК России по Северо-Западному федеральному округу. В настоящее время полученные научные результаты проходят экспертизу в целях возможности открытого опубликования в рецензируемых изданиях из перечня ВАК при Минобрнауки России (3 публикации). В соответствии с планом выполнения проекта подготовлены материалы регистрации программы для ЭВМ (2 программы). Представление диссертации на НТС СПбГУТ спланировано на октябрь-ноябрь 2022 г.

СПИСОК ЛИТЕРАТУРЫ

1 Азамов О. В. Информационная безопасность / Будылин К. Ю., Бунев Е. Г., Сакун С. А., Шакин Д. Н. // Наука XXI – 2009. – Том 9, № 3. – С. 35–44.

2 Постановление Правительства Российской Федерации от 08 февраля 2018 г. «Об утверждении Правил категорирования объектов критической информационной

инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений».

3 Организация концептуальной модели критической информационной инфраструктуры / А. М. Гельфанд, Н. Н. Лансере, А. А. Ложкина, И. И. Фадеев // Методы и технические средства обеспечения безопасности информации. – 2020. – № 29. – С. 39-40. – EDN PYPOHZ.

4 Защита информации. INSIDE, 2023, №2, с.3

5 В «Лаборатории Касперского» сообщили о росте числа кибератак на АСУ ТП в России [электронный ресурс]. – Режим доступа : https://cisoclub.ru/v-laboratorii-kasperskogo-soobshhili-o-roste-chisla-kiberatak-na-asu-tp-v-rossii/?ysclid=lmkkynwake623739544 https://cisoclub.ru/v laboratorii-kasperskogo-soobshhili-o-roste-chisla-kiberatak-na-asu-tp-vrossii/?ysclid=lmkkynwake623739544/)

6 Конференция АО "ОСК" 29 марта 2022 г., г. Санкт-Петербург [электронный ресурс]. – Режим доступа : https://fstec.ru/territorialnye-organy-szfo/severo-zapadnyj-federalnyj-okrug/deyatelnost-szfo/vzaimodejstvie-szfo/2364-konferentsiya-ao-osk-29-marta-2022-g-g-sankt-peterburg/

7 Агеев, С.А. Оценка рисков сетевой компьютерной безопасности на основе нечеткого логического вывода / С.А. Агеев, И.Б. Саенко // ИБРР-2017: X Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России». – Санкт-Петербург: СПб.: СПОИСУ, 1-3 ноября, 2017. – Том 3. – С. 28–30.

8 Ажмухамедов, И.М. Анализ рисков информационной безопасности / И.М. Ажмухамедов, О.Н. Выборнова, О.М. Князева: Учебное пособие. – Астрахань: Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Астраханский государственный технический университет», 2015. – 104 с.

9 Аникин, И.В. Метод управления рисками информационной безопасности в корпоративных информационных сетях / И.В. Аникин // Инфокоммуникационные технологии. – 2015. – Том 13, № 2. – С. 215–221.

10 Баранова, Е.К. Методики анализа и оценки рисков информационной безопасности / Е.К. Баранова // Образовательные ресурсы и технологии. – 2015. – № 1(9). – С. 73–79.

11 Булдакова, Т.И. Оценка информационных рисков в автоматизированных системах с помощью нейро-нечёткой модели / Т.И. Булдакова, Д.А. Миков // Наука и образование: научное издание МГТУ им. Н.Э. Баумана. – 2013. – № 11. – С. 295–310.

12 Глухов, А.П. Оценка чувствительности ресурсов и рисков применения систем критических приложений к влияющим факторам / А.П. Глухов, Н.Н. Котяшев, А.В. Купцов // Стратегическая стабильность. – 2007. – № 1(38). – С. 39–44.

13 Черныш, К.В. Индикативная оценка рисков на критериальных моделях критически важных объектов и критических инфраструктур / К.В. Черныш, А.А. Кононов // XI Всероссийской конференции «Методологические проблемы управления макросистемами». – Апатиты: КНЦ РАН, 26 марта-3 апреля, 2016. – С. 86–89.

14 Козунова, С.С. Формализованное описание процедуры управления рисками информационной системы / С.С. Козунова, А.Г. Кравец // Вестник Астраханского государственного технического университета. Серия: управление, вычислительная техника и информатика. – 2018. – № 2. – С. 61–70.

15 Милославская, Н.Г. Управление рисками информационной безопасности / Н.Г. Милославская, М.Ю Сенаторов, А.И. Толстой: Учебное пособие для вузов. 2-е изд., испр. – М.: Горячая линия-Телеком, 2014. – 130 с.
16 Барабанов, А.В. Актуальные вопросы выявления уязвимостей и недекларированных возможностей в программном обеспечении / А.В. Барабанов, А.С. Марков, В.Л. Цирлов // Системы высокой доступности. – 2018. – Том 14, № 3. – С. 12–17.
17 Буйневич, М.В. Модель угроз информационно-технического взаимодействия в интегрированной системе защиты информации / М.В. Буйневич, В.В. Покусов, К.Е. Израилов // Информатизация и связь. – 2021. – № 4. – С. 66–73.
18 Буйневич, М.В. Аналитическое моделирование работы программного кода с уязвимостями / М.В. Буйневич, К.Е. Израилов // Вопросы кибербезопасности. – 2020. – № 3(37). – С. 2–12.
19 Еремеев, М.А. Продукционное представление знаний для моделирования источников атак в сети / М.А. Еремеев, А.Г. Ломако, В.М. Моргунов, Н.В. Свергун // CDE'17: The 2017 Symposium on Cybersecurity of the Digital Economy. – Иннополис: Издательский Дом "Афина" (Санкт-Петербург), 19-20 сентября, 2017. – С. 167–180.
20 Новохрестов, А.К. Модель угроз безопасности автоматизированной системы коммерческого учета энергоресурсов / А.К. Новохрестов, Д.С. Никифоров, А.А. Конев, А.А. Шелупанов // Доклады ТУСУРа. – 2016. – Том 19, № 3. – С. 111–114.
21 Платонов, В.В. Методы выбора свойств для систем обнаружения сетевых атак / В.В. Платонов // Методы и технические средства обеспечения безопасности информации. – 2016. – № 25. – С. 24–25

Лушников Н.Д.
ФГБОУ ВО «Уфимский университет науки и технологий»,
Институт информатики, математики и робототехники
ассистент кафедры управления информационной безопасностью
luschnikovnikita@yandex.ru

МУЛЬТИМОДАЛЬНАЯ СИСТЕМА БИОМЕТРИЧЕСКОЙ АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ НА ОСНОВЕ НЕЙРОННЫХ СЕТЕЙ.

Аннотация: Разработан и предложен алгоритм верификации пользователей на основе составленной базы биометрических данных. С применением разработанной структуры нейронной сети проведено обучение и получены показатели с помощью функции потерь. Нейронная сеть реализована с вычислением сигмоидальной функции и реализацией метода использования вероятностного линейного дискриминантного анализа (PLDA). Результатом исследования является разработанное программное обеспечение, предназначенное для распознавания пользователей информационной системы. База биометрических данных содержит как изображения лиц, так и аудиозаписи голоса пользователей информационной системы. В рамках данного исследования в режиме онлайн разработан модуль, позволяющий предотвратить реализацию злоумышленниками методику синтеза изображения (дипфейк).

Ключевые слова: аутентификация, пользователь, нейронная сеть, математические методы, программное обеспечение.

Процедуры аутентификации и авторизации субъектов являются важнейшим механизмом защиты, от качества которого зависит безопасность информационной системы. Средства аутентификации, авторизации и администрирования являются одними из классических средств по управлению информационной безопасностью компьютерными системами предприятия, и включают в себя такие процессы, как определение, создание, изменение, удаление и аудит пользовательских учетных записей [1]. Современные биометрические системы являются очень удобными для пользователей. В отличие от паролей и носителей информации, которые могут быть потеряны, украдены, скопированы, биометрические системы основаны на человеческих параметрах, которые всегда находятся вместе с ними, и проблема их сохранности не возникает. Потеря данных параметров маловероятна [2].

Мультимодальная (комбинированная) биометрическая система аутентификации применяет различные дополнения для использования нескольких типов биометрических характеристик, что позволяет соединить несколько типов биометрических технологий в системах аутентификации в одной. Это позволяет удовлетворить самые строгие требования к эффективности системы аутентификации. Такая структура может использовать все виды биометрических данных человека и может применяться там, где приходится форсировать ограничения одной биометрической характеристики. Комбинированные системы являются более надежными с точки зрения возможности фальсификации биометрических данных человека, так как труднее подделать целый ряд характеристик, чем фальсифицировать один биометрический признак [3].

Таким образом, целью исследования является повышение эффективности процесса аутентификации пользователей информационной системы по извлеченным биометрическим характеристикам.

Для достижения данной цели были поставлены и решены следующие задачи:

1. Разработка метода распознавания пользователей информационной системы с помощью мультимодальной биометрической аутентификации.
2. Разработка алгоритма мультимодальной биометрической аутентификации пользователей информационной системы.
3. Разработка подсистем биометрической аутентификации на основе искусственных нейронных сетей с разными наборами биометрических данных.
4. Разработка программного комплекса, реализующего метод мультимодальной биометрической аутентификации пользователей информационной системы.

В рамках исследования, с учетом поставленных задач, этапы реализации программного комплекса выглядят следующим образом (Рис. 1):

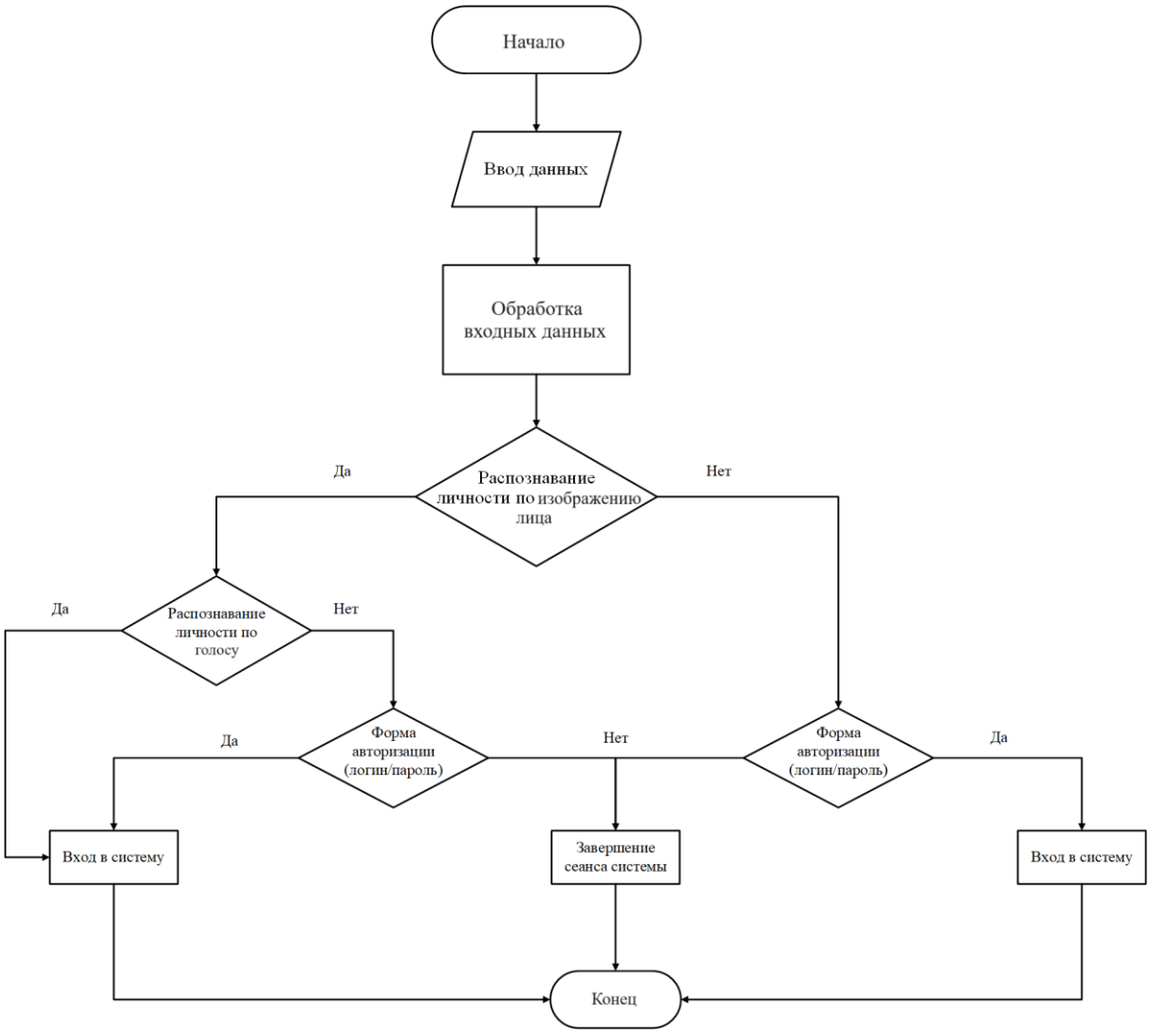


Рис. 1 – Блок–схема программного комплекса

Помимо рассмотренных моделей мультимодальной биометрической системы аутентификации пользователей информационной системы распознавания по изображению лица и голосу была также разработана форма авторизации пользователей информационной системы. В связи с сокращением времени процесса аутентификации форма авторизации не

является частью реализации программного комплекса, но представлена в виде отдельного фрейма (Рис. 2).

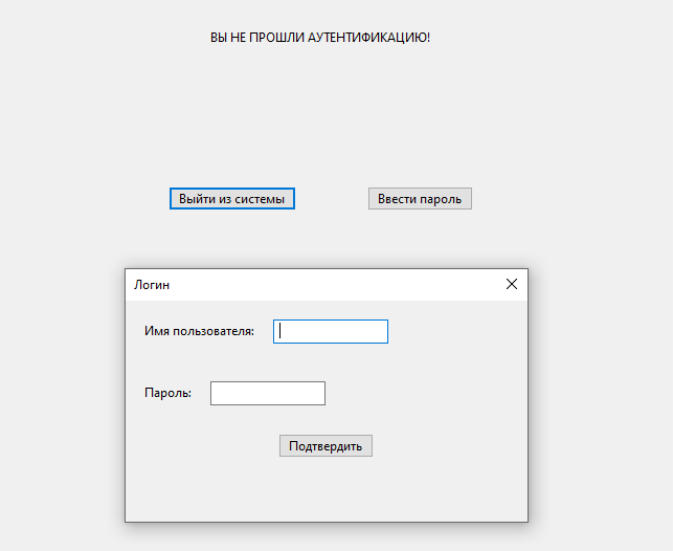


Рис. 2 – Форма авторизации пользователей информационной системы

В рамках данного исследования исходный программный код системы распознавания личности по фото сохранен в виде исполняемого файла в формате *.exe. Для удобства пользования программным комплексом в информационных системах был установлен инсталлятор программы с лицензионным соглашением.

Процессы обучения искусственной нейронной сети были рассмотрены ранее. Стоит обратить внимание на графический дизайн программного комплекса. Несмотря на используемую библиотеку PyQt5, возможности графического дизайна языка программирования Python очень ограничены. Начальный экран программного комплекса минималистичен: состоит из логотипа организации, индикации загрузки и кнопок «Пройти», «Выйти» (Рис. 3).

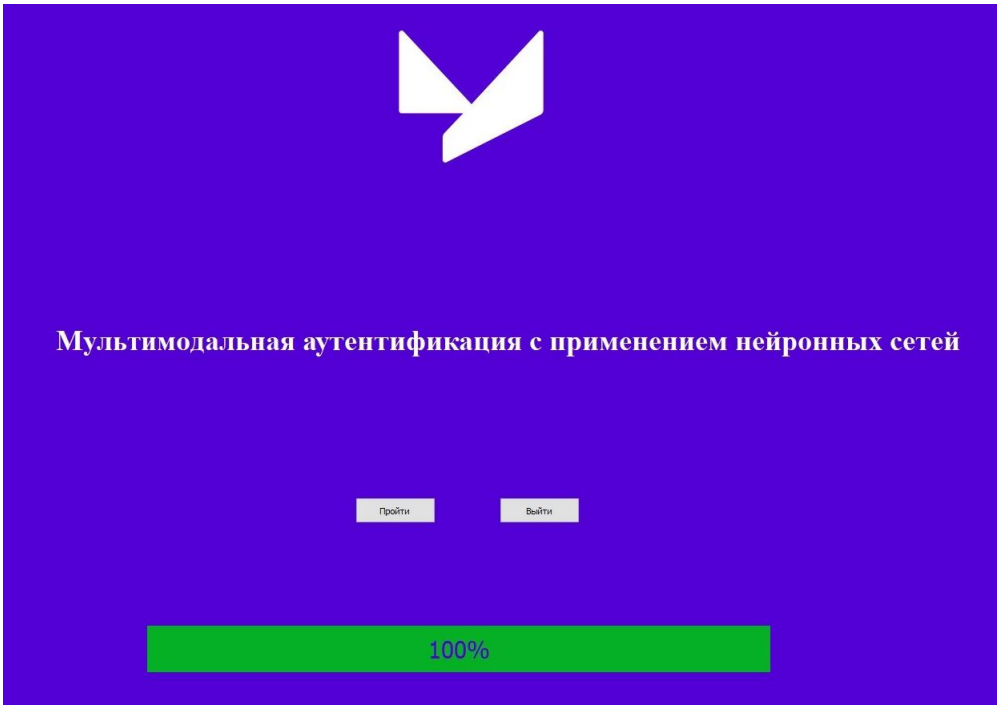


Рис. 3 – Интерфейс программного комплекса

После запуска процесса аутентификации необходимо пройти этап распознавания личности по лицу. По извлекаемым дескрипторам и ключевым точкам лица осуществляется

сравнение по видео изображения лица в режиме реального времени и изображения лица из базы биометрических персональных данных пользователей информационной системы (Рис. 4).

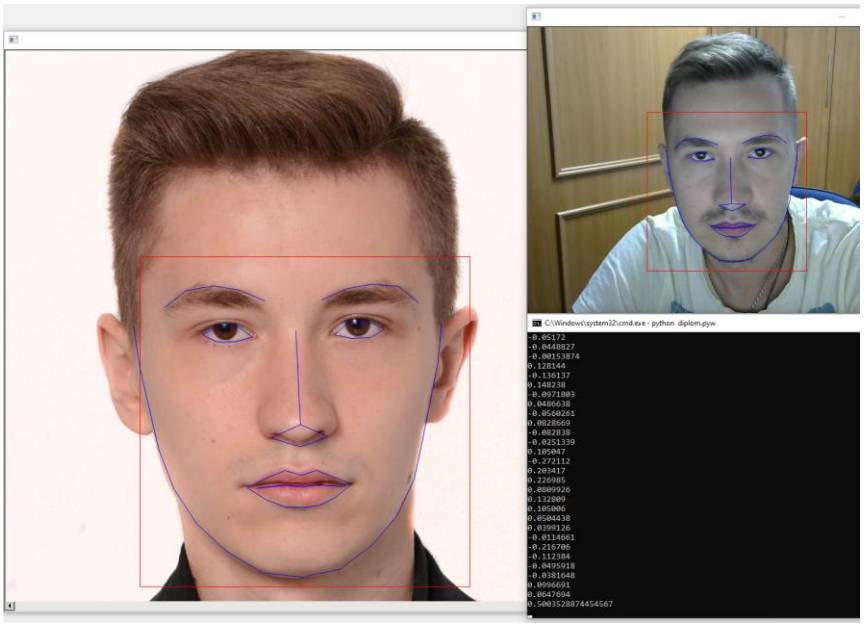


Рис. 4 – Процесс распознавания пользователей информационной системы по изображению лица

Следующим этапом является распознавание пользователей информационной системы по голосу. Его суть заключается в извлечении акустических признаков речевого сигнала входного аудиофрагмента с тем аудиофрагментом, который уже находился ранее в базе данных. В результате сравнения акустических признаков программный комплекс выводит результат пройденной процедуры [4].

Помимо поставленной задачи следует изучить не менее актуальную проблему распознавания искомого пользователя информационной системы. Для осуществления несанкционированного доступа (НСД) используется обширный арсенал разрабатываемых программных решений [5]. В том числе данные решения применяются в процессах аутентификации пользователей и олицетворяют собой методику синтеза изображения (дипфейк). Данная методика используется для соединения и наложения существующих изображений и видео на исходные изображения или видеоролики (например, FakeApp) [6]. Несмотря на то, что данные инструменты используются в других сферах деятельности (в том числе в качестве развлекательного контента), количество киберинцидентов продолжает расти. Не каждое современное программное решение, предназначенное для защиты биометрических персональных данных на устройстве, может справиться с действиями злоумышленников. В связи с этим в рамках данного исследования была разработана модель, предназначенная для противодействия методике синтеза изображения и для противодействия распознавания пользователей информационной системы по изображениям, распечатанным на бумажном носителе и сохраненных на других устройствах [7].

Для корректного распознавания пользователей информационной системы была сформирована база данных изображений, состоящая из следующих папок:

— Анфас.
— Профиль слева.
— Профиль справа.
— Глаза открыты.

— Глаза закрыты.

Во время записи в режиме реального времени видеосигнал обладает следующими характеристиками:

— Частота кадров – 25 FPS.

— Разрешающая способность – 800 × 600 пикселей.

— Битрейт – 8–10 Мбит/сек.

В результате прохождения ранее рассмотренных этапов, разработанная модель распознает искомых пользователей информационной системы [8].

Помимо этого, выводится результат противодействия методике синтеза изображения и противодействия распознавания пользователей информационной системы по изображениям, распечатанным на бумажном носителе и сохраненных на других устройствах (Рис. 5) [9].

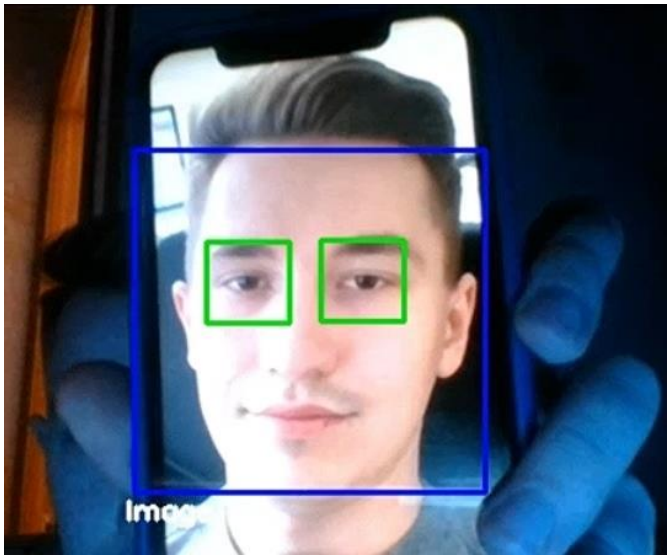


Рис. 5 – Распознавание изображения лица, сохраненного на другом устройстве

Научная значимость результатов заключается в создании новой мультимодальной биометрической системы аутентификации пользователей информационных систем, которая наиболее эффективно распознает пользователей информационных систем и оптимизирует обработку больших объемов биометрических данных.

Практическая значимость результатов заключается в том, что разработанный алгоритм и реализованный программный комплекс осуществляет процесс аутентификации пользователей информационных систем в режиме многопоточности.

При программной реализации мультимодальной биометрической системы аутентификации пользователей информационных систем были разработаны две архитектуры искусственных нейронных сетей с базой данных в 100, 200 и 600 биометрических образов. В ходе исследования была выявлена следующая положительная динамика: при пополнении базы данных биометрических образов значения ошибок первого и второго рода после прохождения аутентификации уменьшались.

На данный момент в рамках исследования проводится апробация нейронной сети wav2vec с международными базами данных VoxCeleb (10000 аудиозаписей) и TIMIT (1500 аудиозаписей) [10]. В дальнейшем, после укрупнения базы биометрических данных, будет проведено сравнение разработанных авторами архитектур искусственных нейронных сетей с представленными международными архитектурами нейронных сетей.

СПИСОК ЛИТЕРАТУРЫ

1. Лушников, Н. Д. Организация идентификации личности при помощи нейросетевых технологий / Н. Д. Лушников, А. С. Исмагилова // Актуальные проблемы прикладной математики, информатики и механики: сборник трудов Международной научной конференции, Воронеж, 07–09 декабря 2020 года / ФГБОУ ВО «Воронежский государственный университет». – Воронеж: Научно–исследовательские публикации, 2021. – С. 575–581.
2. Мамаев В. Многофакторная биометрическая идентификация // Системы безопасности. 2017, №5. С. 78–79.
3. Сабанов А. Г. Аутентификация и системы разграничения логического доступа: концепция оценки доверия к результатам / Сабанов А. Г. // Защита информации. Инсайд. – 2021. – № 2. – С. 10–17.
4. Лушников, Н. Д. Особенности голосовой идентификации в многофункциональном программном обеспечении с использованием нейронных сетей / Н. Д. Лушников, А. С. Исмагилова // Теория и практика обеспечения информационной безопасности: Сборник научных трудов по материалам всероссийской научно-теоретической конференции, Москва, 03 декабря 2021 года. – Москва: Московский технический университет связи и информатики, 2021. – С. 98-102.
5. Купка, И. П. Дипфейк как информационное оружие современности / И. П. Купка, С. С. Щербаков // Динамика медиасистем. – 2023. – Т. 3, № 1. – С. 375-381.
6. Свирщ, А. О. Развитие технологии deepfake / А. О. Свирщ, П. А. Олейникова // Modern Science. – 2021. – № 12-4. – С. 309-320.
7. Свидетельство о государственной регистрации программы для ЭВМ № 2021614672 Российская Федерация. Аутентификация учетных записей пользователей с помощью биометрических технологий: № 2021613387: заявл. 15.03.2021: опубл. 29.03.2021 / Н. Д. Лушников, А. С. Исмагилова; заявитель федеральное государственное бюджетное образовательное учреждение высшего образования «Башкирский государственный университет».
8. Лушников, Н. Д. Евклидово расстояние как основа программного комплекса по многофакторной биометрической аутентификации / Н. Д. Лушников, А. С. Исмагилова // Математическое моделирование процессов и систем: Материалы XI Международной молодежной научно–практической конференции, Стерлитамак, 10 – 12 ноября 2021 года / Отв. редактор С.В. Викторов. Том Часть 2. – Стерлитамак: Стерлитамакский филиал федерального государственного бюджетного образовательного учреждения высшего профессионального образования «Башкирский государственный университет», 2021. – С. 53–55.
9. Свидетельство о государственной регистрации программы для ЭВМ № 2020660303 Российская Федерация. Управление доступом при помощи нейронных сетей: № 2020618972: заявл. 12.08.2020: опубл. 01.09.2020 / Н. Д. Лушников, А. С. Исмагилова; заявитель федеральное государственное бюджетное образовательное учреждение высшего образования «Башкирский государственный университет».
10. Рахманенко, И. А. Автоматическая верификация диктора по произвольной фразе с применением свёрточных глубоких сетей доверия / И. А. Рахманенко, А. А. Шелупанов, Е. Ю. Костюченко // Компьютерная оптика. – 2020. – Т. 44, № 4. – С. 596-605. – DOI 10.18287/2412-6179-CO-621.

Маслова М.А.
ФГАОУ ВО Ростовский государственный
экономический университет (РИНХ),
аспирант, м.н.с.,
mashechka-81@mail.ru

ОСОБЕННОСТИ ФОРМИРОВАНИЯ ВХОДНЫХ И ВЫХОДНЫХ ДАННЫХ ПРИ АНАЛИЗЕ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация: Одним из важнейших задач управления какой-либо организацией является анализ и оценка рисков, так как они каждый день сталкиваются с ними все в большем объеме. Для эффективного управления рисками необходима методика их определения, постоянное отслеживание и предотвращение.

В работе были рассмотрены различные методы, применяемые для анализа и оценки рисков информационной безопасности, их основные плюсы и минусы, входные и выходные параметры. На основе данных стандартов и методов был создан новый унифицированный метод анализа и оценки рисков информационной безопасности, содержащий большую базу данных, которая имеет возможность постоянно модернизироваться в зависимости от появления новых угроз, должна быть проста в управлении, финансово выгодной, автоматизированной и дистанционной.

Ключевые слова: информационная безопасность, риски, метод, анализ и оценка, рекомендации, база данных.

С развитием цифрового общества одним из трендов в сфере информационной безопасности продолжают оставаться всевозможные риски, которые все больше набирают обороты и разновидности, такие как: киберугрозы, утечки данных, мошенничество с похищением учетных записей, человеческий фактор, фишинг, программы-вымогатели, вредоносные программы, взломы серверов и т.д. Организациям необходимо бороться с ними и постоянно держать «руку на пульсе» [1]. Очень часто организации не имеют определенных отделов и персонала для данной работы, прибегают к сторонней помощи или покупают какие-либо программы для анализа, оценки, предотвращения возможных рисков. С развитием санкций стало все более проблематично контролировать все рисковые ситуации в Российской Федерации и появилась нехватка программ для контроля за рисками. Поэтому разработка метода оценки рисков является актуальной [2, 3].

В данной работе проводится обзор:

– возможных методов определения и расчета рисков: количественным, качественным, комплексным методом, направления интеллектуального анализа для определения рисков [4, 5];

– основных методик, стандартов и методов, наиболее часто применяемых при оценке рисков информационной безопасности, направленных на дальнейший их анализ, уменьшение, предупреждение и ликвидацию;

– приводится общая и разрабатываемая модель анализа и оценки рисков информационной безопасности [6]

Для дальнейшего анализа в работе были выбраны следующие методики: ФСТЭК, CRAMM, BS 7799, ГОСТ ИСО/МЭК ТО 7, RiskWatch, FRAP, MOF, CORAS, MSAT, RISK IT, OCTAVE, Microsoft, ISO/IEC 27001, ГРИФ, СТО БР ИББС[7 - 10].

Они проанализированы и на основании этого описаны основные шаги, составляющие, активы, входные и выходные параметры, из которых выделены основные характеристики, сравнение сходящихся и расходящихся параметров, разделены на группы по определению: качественному, количественному и комбинированному (с определением плюсов и минусов каждой из них).

Далее была составлена база данных по:

– входным параметрам, которая составила 184 пункта, затрагивающая разные виды активов для возможного дальнейшего тщательного изучения и рассмотрения рисковых ситуаций в организациях;

– выходным параметрам, которая составила 101 пункт;

– сделано соответствие входных и выходных параметров;

– были разработаны рекомендации по анализу, предупреждению и устранению возможных рисков, которые формировались на основе нормативных актов, законов Российской Федерации, ФСТЭК и других документов по информационной безопасности по выходным параметрам метода [11, 12].

Все данные занесены в базу разработанного программного метода, где:

– управление происходит одним человеком – модератором, который приглашает клиентов и экспертов для поведения экспертизы;

– клиент регистрируется, получает свой личный кабинет, подает заявку на экспертизу с описанием организации, входных данных и уязвимых мест организации;

– эксперт регистрируется и получает личный кабинет, в котором он видит более подробную информацию об организации и может проводить экспертизу;

– модератор в свою очередь видит всю информацию по клиентам и экспертам, отвечает за управление, модернизацию, видоизменение программного вида, добавление и удаление какой-либо информации;

– для расчета сходимости параметров в методе был применен Дельфийский метод, где с помощью экспертной оценки оцениваются параметры по их важности, рассчитываются сходимость данных и, благодаря расчетам, выдаются рекомендации по анализу, предотвращению и устранению рисковых событий [13 - 15];

– на выходе разработанного метода выдается файл Excel с разработанными рекомендациями, относящимися непосредственно к той организации, которая подала заявку;

– все полученные данные отправляются на e-mail клиенту и отображаются в его личном кабинете [16 - 17].

Вывод. Благодаря анализу и тщательной проработке каждого выбранного метода была получена большая база данных входных и выходных параметров для работы экспертов, автоматических расчетов сходимости оцененных параметров и получению конкретных рекомендаций по каждому рисковому событию, что позволит организациям своевременно проанализировать, оценить, уменьшить, предотвратить, избежать какого-либо рискового события, что сэкономит им не только время, репутацию, но и немалые деньги.

СПИСОК ЛИТЕРАТУРЫ

1. Много ИБ-статистики. Как перевернулся мир ИБ за три года? [Электронный ресурс]. Режим доступа: https://habr.com/ru/companies/searchinform/articles/700500/;
2. Родина, Ю. В. Информационная безопасность и риски информационной безопасности. Интерпретация понятий / Ю. В. Родина // Экономика и менеджмент: от теории к практике: Сборник научных трудов по итогам международной научно-практической конференции, Ростов-на-Дону, 04 августа 2014 года / ИННОВАЦИОННЫЙ ЦЕНТР РАЗВИТИЯ ОБРАЗОВАНИЯ И НАУКИ. – Ростов-на-Дону: ИННОВАЦИОННЫЙ ЦЕНТР РАЗВИТИЯ ОБРАЗОВАНИЯ И НАУКИ, 2014. – С. 122-124;
3. Риски информационной безопасности // Управление рисками информационной безопасности - [Электронный ресурс]. – Режим доступа: https://www.dialognauka.ru/press-center/article/5990/?Ysclid=laxz579slh74947120;
4. Методы и средства анализа рисков информационной безопасности предприятия – [Электронный ресурс]. Режим доступа: Https://technet.microsoft.com/ru-ru/security/cc185712.aspx;
5. Фатхи, Д. М. Применение методов интеллектуального анализа данных для тестирования баз данных систем информационной безопасности / Д.М. Фатхи // Информационная безопасность регионов. 2014. № 1 (14). С 48-50;
6. Маслова, М. А. Инструментальный подход к оценке рисков информационной безопасности / М. А. Маслова // Информация и безопасность. – 2022. – Т. 25, № 2. – С. 209 - 216;
7. Разумников С. В. Анализ возможности применения методов Octave, riskwatch, Cramm для оценки рисков ИТ для облачных сервисов //Современные проблемы науки и образования. – 2014. – №. 1. – С. 247-247;
8. Пугин В.В., Губарева О.Ю. Обзор методик анализа рисков информационной безопасности информационной системы предприятия. T-Comm# 6-2012. С 54-57. [Электронный ресурс]. Режим доступа: Https://cyberleninka.ru/article/v/obzor-metodik-analiza-riskov-informatsionnoy-bezopasnosti-informatsionnoy-sistemy-predpriyatiya;
9. Пакет методологии Coras [Электронный ресурс]. – Режим доступа: Https://studref.com/325291/informatika/paket_metodologii_coras//;
10. Угрозы безопасности информации [Электронный ресурс] // Банк данных угроз безопасности ФСТЭК. URL: https://bdu.fstec.ru/threat/ubi.006/;
11. Маслова, М. А. Программные методы выработки рекомендаций при экспертном аудите информационных систем / М. А. Маслова // Вестник УрФО. Безопасность в информационной сфере. – 2022. – № 4(46). – С. 26-31.
12. Маслова, М. А. Научно-методические рекомендации по регулированию рисков нарушения информационной безопасности / М. А. Маслова // Информация и безопасность. – 2022. – Т. 25, № 4. – С. 513-520.
13. Стончюте, К. Э. Методы экспертных оценок: Метод Дельфи / К. Э. Стончюте, А. А. Гурбо, А. А. Пузыревская // . – 2021. – № 5(53). – С. 16-19.
14. Маслова, М. А. Анализ, применение и модификация метода Дельфи / М. А. Маслова // Вестник УрФО. Безопасность в информационной сфере. – 2022. – № 2(44). – С. 25-29.

15. Свидетельство о государственной регистрации программы для ЭВМ № 2022668264 Российская Федерация. Разработка модуля оценки входных данных для программы анализа рисков нарушения информационной безопасности: № 2022662069: заявл. 27.06.2022: опубл. 05.10.2022 / М. А. Маслова; заявитель федеральное государственное бюджетное образовательное учреждение высшего образования «Ростовский государственный экономический университет».

16. Свидетельство о государственной регистрации программы для ЭВМ № 2020662695 Российская Федерация. Программный модуль расчета рисков информационной безопасности методом экспертных оценок: № 2020661878: заявл. 07.10.2020: опубл. 16.10.2020 / М. А. Маслова, Д. В. Какаев; заявитель Федеральное государственное автономное образовательное учреждение высшего образования «Севастопольский государственный университет».

17. Свидетельство о государственной регистрации программы для ЭВМ № 2023666158 Российская Федерация. Программный модуль анализа и оценки исков нарушения информационной безопасности: № 2023664786: заявл. 12.07.2023: опубл. 26.07.2023 / М. А. Маслова; заявитель федеральное государственное бюджетное образовательное учреждение высшего образования «Ростовский государственный экономический университет».

Орел Е.М.
СПбПУ Петра Великого, аспирант,
orel@ibks.spbstu.ru

ОЦЕНКА УСТОЙЧИВОСТИ АРХИТЕКТУРЫ ДЕЦЕНТРАЛИЗОВАННЫХ СИСТЕМ ОБМЕНА СООБЩЕНИЯМИ ОТ ВРЕДОНОСНЫХ ВОЗДЕЙСТВИЙ НА ОСНОВЕ ТЕОРИИ ГРАФОВ

Аннотация: В данной работе представлены промежуточные результаты реализации научного проекта «Автоматизация управления безопасностью сетей с децентрализованной структурой на основе теории графов», направленного на обеспечение безопасности сетей с децентрализованной узловой структурой. Проведен анализ устойчивости архитектуры типовых систем обмена сообщениями с децентрализованной узловой структурой. Разработаны математические модели целевых систем, выделены ключевые особенности и недостатки их архитектуры. Представлены типовые угрозы подобных систем и модель графа атак для обработки результатов анализа защищенности подобных систем.

Ключевые слова: децентрализация, mesh-мессенджеры, самоорганизующиеся сети, Briar, Bridgefy, киберугрозы, граф атак, модель угроз.

Актуальность темы исследования. На сегодняшний день все больше компаний внедряет в свои системы возможность работы без наличия выхода в сеть Интернет: создаются новые пиринговые мессенджеры, системы экстренного оповещения и многие другие, имеющие децентрализованную структуру. При этом количество инцидентов в таких системах непрерывно растет. Основными причинами данных инцидентов являются архитектурные недостатки разработанных решений. Особенно остро данная проблема стоит в системах, осуществляющих управление производственным процессом, обеспечивающих децентрализованную коммуникацию (mesh-мессенджеры), хранение конфиденциальных данных пользователей, больничных комплексах.

Децентрализованные системы могут быть использованы для обеспечения коммуникации в таких обстоятельствах, когда использование стандартных централизованных систем невозможно в связи с определенными факторами. Такими факторами могут выступать как чрезвычайные обстоятельства, природные катаклизмы, так и намеренная перегрузка или глушение связи с сетью Интернет [1].

Степень разработанности темы исследования. Большинство публикаций, связанных с кибербезопасностью киберфизических систем с децентрализованной архитектурой, направлены на обозначение проблематики и задач защиты от новых угроз [2][3][4]. В работе [5] представлен применимый в рамках работы метод оценки защищенности киберфизических систем, в котором кибербезопасность является процессом, а не статическим состоянием. В работе [6] авторы предлагают подход к реализации архитектуры умного города на основе графового взаимодействия, однако подход уязвим к большинству кибератак. В данных архитектурах не учитывается специфика киберфизических систем, функционирующих в условиях постоянно происходящих кибератак.

Ряд методов по выявлению киберугроз в крупномасштабных самоорганизующихся сетях, разработанных в СПбПУ Петра Великого, интегрирован в запатентованные программы

Калинина М.О [7], Зегжды П.Д., Крундышева В.М. [8], что подтверждает актуальность проблем информационной безопасности подобных систем.

Цель исследования – анализ устойчивости архитектуры децентрализованных систем обмена сообщениями.

Задачи исследования:

1. Разработка математических моделей систем децентрализованного обмена сообщениями Briar и Bridgefy.
2. Оценка устойчивости архитектуры децентрализованных систем обмена сообщениями на примере Briar и Bridgefy.
3. Разработка модели угроз типовых децентрализованных систем обмена сообщениями.

Научная новизна исследования заключается в разработанных моделях децентрализованных систем обмена сообщениями Briar и Bridgefy, представленных в виде графов, модели угроз исследованных систем и графа атак для представления результатов анализа их защищенности. Анализ особенностей данных моделей позволил установить ряд недостатков, присущих подобного рода системам.

Теоретическую значимость работы представляют выявленные недостатки типовых систем децентрализованного обмена сообщениями Briar и Bridgefy, а именно: примитивность алгоритмов динамической маршрутизации, принятая за аксиому враждебность среды и возможность проведения атак типа wormhole при удачном расположении злоумышленника в сети, имперсонация устройств системы, возможность деградации сети, позволивших говорить о их низкой отказоустойчивости. Практическая значимость результатов работы заключается в возможности разработки методов по регулированию доступа пользователей к децентрализованным системам Briar и Bridgefy, возможности применения разработанных моделей для проведения оценки защищенности схожих систем.

Методология и методы исследования. Для решения поставленных задач использовалась теория графов, теория множеств и алгоритмический подход.

Степень достоверности и апробация результатов. Достоверность и обоснованность результатов подтверждается анализом аналогичных научных работ в данной области и результатами экспериментов.

Промежуточные результаты проекта были представлены на 32-й научно-технической конференции «Методы и технические средства обеспечения безопасности информации» (МиТСОБИ) имени Петра Дмитриевича Зегжды (Санкт-Петербург, 2023гг.), а также отражены в публикации в издании, индексируемом в РИНЦ.

Положения выносимые на защиту:

1. Результаты оценки устойчивости архитектуры систем с децентрализованной узловой структурой от вредоносных воздействий.
2. Модель угроз типовых систем обмена сообщениями с децентрализованной узловой структурой.
3. Математическое описание графа атак, сгенерированного на основе текущих сведений о системе и известных сценариев атак.

Структура сети Bridgefy представляет собой граф следующего вида (1.1):

$$G(V, B, P) =< V, B, P >, V \neq \emptyset, \{v, v\} \notin B, \{v, v\} \notin P, v \in V \quad (1.1)$$

V – непустое множество узлов графа, *B (P)* – множества ребер, представляющих собой каналы передачи широковещательных, в контексте mesh-сети, (личных) сообщений. На рис. 1 представлена визуализация заданного графа.

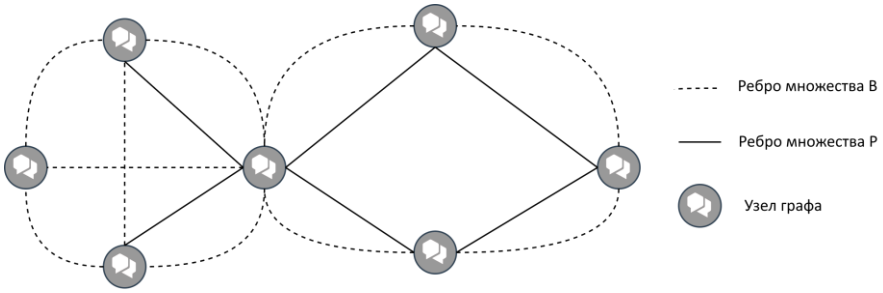


Рис. 1. Структура сети Bridgefy

Функция *private* определяет, используется ли данное ребро для передачи личных сообщений.

$$\forall x, y \in V, \{x, y\} \in B: private(x, y) = 0$$
$$\forall x, y \in V, \{x, y\} \in P: private(x, y) = 1 \quad (1.2)$$
$$B \cap P = \emptyset$$

Узел графа сети Bridgefy представляет собой структуру, содержащую следующие характеристики: имя пользователя, mac-адрес bluetooth-адаптера устройства, идентификатор пользователя, используемый протокол на сетевом уровне (bluetooth classic или bluetooth low energy), набор открытых ключей ассиметричного шифрования.

Ребро $\{v, u\} \in P$ графа представляет собой связь между двумя доверенными устройствами. Для организации обмена личными сообщениями Bridgefy использует протокол согласования ключей X3DH [9] на основе эллиптической кривой Ed25519 для установки общего секрета и алгоритм Double Ratchet [10] для обмена зашифрованными сообщениями. В результате между устройствами устанавливается сессия протокола Signal.

Ребро $\{v, u\} \in B$ представляет собой установленную между двумя устройствами сессию протокола Signal. Для существования подобного ребра необходимо, чтобы устройства v и u ранее прошли процедуру взаимной верификации.

Briar представляет собой децентрализованную систему обмена файлами и сообщениями, позиционирующуюся разработчиками как инструмент обеспечения конфиденциальности общения вне зависимости от среды передачи данных [11].

На уровне приложения Briar использует 5 основных протоколов [12] для организации всего процесса сетевого взаимодействия (BQP, BSP, BTP, BHP и BRP).

Сеть Briar строится на основе уровней доверия между устройствами: верифицированный, не верифицированный, не доверенный. Верификация контактов осуществляется по протоколу BQP [13].

Структура сети Briar представляет собой граф следующего вида:

$$G(V, C, S, T) =< V, C, S, T >, \{v, v\} \notin C, \{v, v\} \notin S, v \in V \quad (1.3)$$

Множество *V* – непустое множество вершин. Множества *C (S)* – множества ребер, инцидентные узлы которых являются верифицированными (не верифицированными) контактами. Функция *verify* определяет, является ли пара узлов верифицированными контактами:

$$\forall x, y \in V, \{x, y\} \in C: verify(x, y) = 1$$
$$\forall x, y \in V, \{x, y\} \in S: verify(x, y) = 0 \quad (1.4)$$
$$C \cap S = \emptyset$$

На рис. 2 представлена визуализация заданного графа.

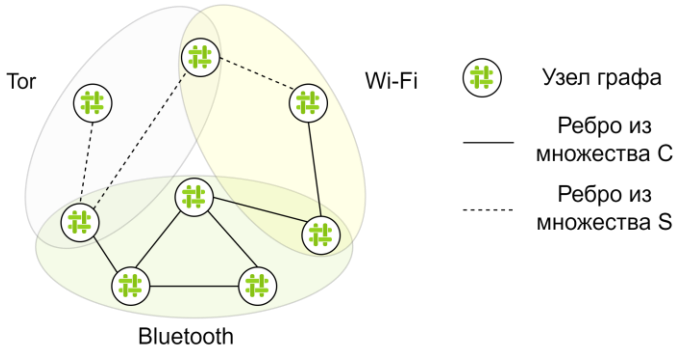


Рис. 2. Структура сети Briar

$T = \{0, 1, 2\}$ – множество типов связи на сетевом уровне (Bluetooth Classic, Wi-Fi, Tor)

Обозначим объединение множеств ребер: $E = C \cup S$. Тогда $transport -$ отображение вида:

$$transport: V \times V \times T \to E \quad (1.5)$$

Для определения числа инцидентных ребер из E для $v \in V$, имеющих тип связи t на сетевом уровне, используется следующая формула:

$$\varphi(v, t) = \sum_{i=0}^{\deg(v)} \mathrm{I}\{t_i = t\}, \quad (1.6)$$

где $I -$индикаторная функция, $t_i -$ тип связи на сетевом уровне для ребра из E.

Значение $\varphi(v, t) \leq 7$ для $t = 0$ (для соединений с типом связи Bluetooth).

Узел графа представляет собой структуру, содержащую следующие характеристики:

— идентификатор для связи через Bluetooth: MAC-адрес Bluetooth и UUID;

— идентификатор для связи через 802.11: IP-адрес и TCP-порт на устройстве;

— специальный сгенерированный идентификатор для связи через Tor;

— набор открытых ключей ассиметричного шифрования.

Для каждого узла графа в любой момент времени задан хотя бы один из трех типов идентификаторов для каждого инцидентного с ним узла.

Конфиденциальность и целостность данных сообщения на уровне приложения обеспечивается использованием алгоритмов $Salsa20Poly1305$ и $EcDSA$.

Архитектурные особенности рассмотренных мессенджеров:

1. Рассмотренные системы используют максимально простые алгоритмы поиска маршрута. В Bridgefy сообщение транслируется всем узлам в радиусе действия Bluetooth-адаптера отправителя или отправляется напрямую целевому устройству, в Briar – всем верифицированным контактам, входящим в ту же группу или форум, что и отправитель сообщения.

2. Оба решения используют понятие доверенного (верифицированного) узла, вводя процедуру верификации. Данная процедура заключается в обмене открытыми ключами для последующей генерации общего секрета, на основе которого создаются все последующие сессии.

3. Ввиду потенциальной вредоносности среды верифицированными могут считаться только те устройства, которые хотя бы раз оказались в непосредственной близости от отправителя.

4. В подобных системах отсутствует механизм контроля подлинности сообщений, отправленных не верифицированным для целевого узла устройством.

5. Наличие нескольких протоколов и режимов передачи данных между устройствами сети обуславливает высокую гетерогенность её структуры и положительно влияют на отказоустойчивость.

Описанные выше особенности архитектуры децентрализованных систем обмена сообщениями позволили выделить ряд недостатков, присущих подобного рода системам:

— Наличие системы уровней доверия приводит к тому, что сеть становится менее отказоустойчивой: в случае выхода из строя части устройств, сеть не сможет автоматически перестроиться, так как для построения новых маршрутов необходимо прохождение взаимной верификации устройств.

— Граф сети Briar по своей структуре имеет множество мостов – ребер графа, удаление которых приведет к появлению новой компоненты связности графа. При этом появление новых ребер между компонентами связности возможно только при активном взаимодействии устройств сети.

— Нагрузка на узлы подобных систем распределяется неравномерно, а в виду их использования на мобильных платформах, производительность узлов сильно ограничена.

— Системы децентрализованного обмена сообщениями подвержены атакам вида Wormhole на узлах сети, являющихся шарнирами – узлами графа, удаление которых приведет к появлению новой компоненты связности. При появлении злоумышленника на одном из шарниров, он может контролировать весь траффик сети, маршрутизируемый между инцидентными ему компонентами связности.

— С ростом сети Bridgefy растет сложность регулирования ситуации лавинного распространения вредоносных пакетов.

— В рассмотренных системах возможна имперсонация под любой из узлов системы в рамках обмена сообщениями между устройствами, не прошедшими взаимную верификацию.

Разработка методов оценки защищенности и противодействия кибератакам систем с децентрализованной узловой структурой требует разработки модели угроз и средств представления результатов анализа защищенности для их последующей обработки.

Можно выделить следующие группы нарушителей систем децентрализованного обмена сообщениями:

— находящиеся в локальной сети;

— удаленные, воздействующие через сеть Интернет;

— имеющие физический доступ к устройству.

Основные угрозы конфиденциальности децентрализованных систем обмена сообщениями приведены в Табл. 1.

Табл. 1. Угрозы методов сетевого взаимодействия mesh-мессенджеров

Описание метода	УБИ по ФСТЭК
КОНФИДЕНЦИАЛЬНОСТЬ	
Раскрытие содержания сообщения с одним адресатом	133, 088
Раскрытие содержания сообщения с несколькими адресатами	088, 133
Установление факта использования ПО на конкретном устройстве	104, 133
Раскрытие метаинформации о сообщении (времени передачи сообщения, адресат, адресант)	104
Раскрытие ключа шифрования локальной базы данных приложения	088
Раскрытие кода доступа к пользовательским данным приложения	133, 104, 088, 006
Раскрытие факта взаимодействия двух конкретных устройств в рамках личного общения	104, 099
Раскрытие факта взаимодействия конкретных устройств в рамках группы	104, 099

ЦЕЛОСТНОСТЬ	
Обход процедур идентификации при отправке сообщения в режиме широковещательных сообщений	006, 128
Обход процедур идентификации при отправке сообщения в режиме сообщений с одним адресатом	006, 128, 088
Обход процедур идентификации при отправке сообщения в режиме общения с несколькими адресатами	006, 128, 088
Модификация информации о содержимом сообщений в локальной копии (атака на синхронизацию)	140, 006
Подмена содержимого сообщения (или его метаданных) легитимного пользователя на сетевом уровне	069, 006, 104, 140
Подмена содержимого сообщения (или его метаданных) от легитимного пользователя на программном уровне	006, 140
Удаление существующего сообщения	140
ДОСТУПНОСТЬ	
Отказ в обслуживании конкретного устройства	140
Отказ в обслуживании центральных узлов графа сети	140
Централизация графа атакующего устройства	140, 104

В рамках исследования были определены угрозы воздействия на организованную сетевую инфраструктуру систем децентрализованного обмена сообщений, имеющие фундаментальный характер. Помимо этого были определены угрозы, объектами воздействия которых является используемое программное обеспечение узлов децентрализованный систем. Для проведения полноценного анализа защищенности подобных систем необходима разработка методологии проведения исследования, которая в свою очередь требует разработки метода представления данных, подлежащих анализу.

Представление результатов анализа защищенности осуществляется на основе ориентированного двудольного графа (граф атаки), представляющего собой действие нарушителя (атаку) и полученные в результате его выполнения сведения (результат атаки).

Граф атаки имеет следующую структуру:

$$G(D, C, A, T) = < D, C, A, T >, T \neq \emptyset \quad (1.7)$$

D – множество вершин графа, представляющих результат атаки, A – множество вершин, представляющих собой готовую к проведению атаку, C – параметров системы, применимых для проведения атаки на любом узле графа, T – множество возможных сценариев атак (профилей).

Отображение AG определяет набор атак, которые могут быть реализованы с текущей совокупностью результатов атак на систему (R), с учетом заданного множества сценариев атак (T) и общих параметров системы (C)

$$AG: R \times T \times C \to A \quad (1.8)$$

Отображение AR сопоставляет каждому набору атак результат данной атаки:

$$AR: A \to D \quad (1.9)$$

Значение совокупности результатов атак вычисляется следующим образом:

$$R(d_i) = d_i \cup R\big(P(d_i)\big), d_i \in D \quad (1.10)$$

$$P(d_i) = \begin{cases} \emptyset, d_i - \text{корень графа} \\ d_j: AG\big(R\big(d_j\big), t, c\big) = a, \;\; AR(a) = d_i, t \in T, c \in C, d_j \in D, a \in A \end{cases} \quad (1.11)$$

Таким образом, граф отображает все возможные действия нарушителя в системе. При этом покрытие графа ограничено только набором возможных профилей атак. Такой подход позволяет повысить эффективности проводимого анализа защищенности за счет

максимизации его покрытия. Дальнейшее направление исследования связано с разработкой методики оценки защищенности систем с децентрализованной узловой структурой, оптимизацией алгоритмов над разработанным графом атак.

СПИСОК ЛИТЕРАТУРЫ

1. Cortes, V.: Bridgefy sees massive spike in downloads during Hong Kong protests: [Электронный ресурс]. URL: https://contxto.com/en/mexico/mexican-bridgefy-sees-massive-spike-in-downloads-during-hong-kong-protests/. (Дата обращения: 16.11.2022).
2. Sajid A., Abbas H., Saleem K. Cloud-assisted IoT-based SCADA systems security: A review of the state of the art and future challenges //Ieee Access. – 2016. – Т. 4. – С. 1375-1384.
3. Sadeghi A. R., Wachsmann C., Waidner M. Security and privacy challenges in industrial internet of things //Proceedings of the 52nd annual design automation conference. – 2015. – С. 1-6.
4. Varga P. et al. Security threats and issues in automation IoT //2017 IEEE 13th International Workshop on Factory Communication Systems (WFCS). – IEEE, 2017. – С. 1-6.
5. Pavlenko E., Zegzhda D. Sustainability of cyber-physical systems in the context of targeted destructive influences //2018 IEEE Industrial Cyber-Physical Systems (ICPS). – IEEE, 2018. – С. 830-834.
6. Abreu D. P. et al. A resilient Internet of Things architecture for smart cities //Annals of Telecommunications. – 2017. – Т. 72. – С. 19-30.
7. Kalinin M. O. Programma vyavlenia polimorfnyh kiberugroz v odnorangovyh samoorganizuyutschyhsya setyax ustroysv po biokodiruemym prosledovatelnostyam pryznakov. – 2020.
8. Zegzhda P. D., Kalinin M. O., Krundyshev V.M. Programma bystrogo obnaruzhenija kiberugroz v krupnomasshtabnyh rekonfiguriruemyh setjah ustrojstv. – 2021.
9. The X3DH Key Agreement Protocol: [Электронный ресурс]. URL: https://signal.org/docs/specifications/x3dh/. (Дата обращения 01.12.2022)
10. The Double Ratchet Algorithm: [Электронный ресурс]. URL: https://signal.org/docs/specifications/doubleratchet/. (Дата обращения 02.12.2022)
11. Briar: [Электронный ресурс]. URL: https://briarproject.org/. (Дата обращения: 05.12.2022)
12. Blöchinger, Simon, Richard von Seck. Survey of Mesh Networking Messengers. // Network 1. – 2021. – pp. 2–4
13. Bramble QR Code Protocol: [Электронный ресурс]. URL: https://code.briarproject.org/briar/briar-spec/-/blob/master/protocols/BQP.md. (Дата обращения 20.12.2022)

Палютина Г.Н.
Институт развития технологий цифровой экономики
РГЭУ (РИНХ), младший научный сотрудник,
hello616@yandex.ru

РАЗРАБОТКА АЛГОРИТМОВ АДАПТИВНОЙ ОЦЕНКИ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ОСНОВЕ ТЕХНОЛОГИИ КОГНИТИВНОГО МОДЕЛИРОВАНИЯ

Аннотация: В работе рассмотрен подход к решению научной задачи повышения эффективности оценки рисков информационной безопасности (ИБ) за счет внедрения в этот процесс технологий когнитивного моделирования (КМ), а именно нечеткие когнитивные карты (НКК), что позволяет сделать процесс оценки более адаптивным. Также для качественной работы НКК в работе рассмотрено применение технологии нейронных сетей (НС) для выставления весов связи между концептами НКК.

Ключевые слова: адаптивная оценка рисков ИБ, когнитивное моделирование, нечеткие когнитивные карты, веса связей между концептами, нейронные сети, обучение нейронных сетей.

Актуальность темы исследования. С ростом зависимости от информационных систем и увеличением количества киберугроз, обеспечение информационной безопасности становится критически важным. Классические статические методы оценки рисков ИБ могут быть ограничены в своей способности адаптироваться к новым и меняющимся угрозам. В этом контексте, разработка алгоритмов адаптивной оценки рисков на основе КМ представляет собой важное направление исследования. КМ позволяет учитывать человеческие факторы, такие как память, восприятие и принятие решений, что может быть важным при оценке рисков ИБ. Алгоритмы адаптивной оценки рисков, основанные на КМ, могут улучшить способность системы обнаруживать и анализировать новые угрозы, предсказывать их вероятность и воздействие, а также принимать решения об эффективных контрмерах. Исследования в этой области могут привести к разработке новых методов и алгоритмов, которые позволят повысить эффективность и надежность систем ИБ.

Степень разработанности темы исследования. Значительный вклад в формирование теоретической и методологической основы исследований по вопросам оценки рисков и когнитивного моделирования внесли: Гузаиров М. Б., Вульфин А. М., Картак В. М., Кириллова А. Д., Миронов К. В., Петухова А. В., Коваленко А. В., Теунаев Д. М, Васильев В. И., Глушенко С. А. и другие исследователи.

В результате решены многие вопросы, в том числе предложено применение технологий нечетких когнитивных карт для придания процессу оценки рисков свойств адаптивности. Однако, все еще актуальным стоит вопрос устранения разрозненности мнений экспертов и сложность обработки большого объема данных.

Цели и задачи работы:

Основной целью исследования «Разработка алгоритмов адаптивной оценки рисков информационной безопасности на основе технологии когнитивного моделирования» является повышение эффективности управления рисками ИБ путем внедрения технологий КМ в

процесс оценки рисков ИБ. Для достижения цели, поставленной в рамках данной работы, необходимо решить следующие задачи:

1. Анализ нормативных документов, ГОСТов и международных стандартов, раскрывающих понятие и этапы оценки рисков ИБ.
2. Анализ современных методов оценки рисков ИБ.
3. Анализ свойств адаптивности оценки рисков ИБ.
4. Анализ особенностей применения технологии КМ, в частности НКК, для оценки информационных рисков.
5. Анализ нейронных сетей, их типов, архитектуры и методов обучения.
6. Анализ принципов построения математических моделей проблемных ситуаций и исследование математических методов анализа задач принятия решений на основе нечеткой логики.
7. Формирование алгоритмического метода, применимого для оценки рисков ИБ на основе КМ с использованием НКК.
8. Теоретическое обоснование эффективности применения результатов исследований.
9. Апробация и внедрение результатов в практику работы организаций различного профиля.

Научная новизна. В рамках работы были исследованы различные публикации, связанные с тематикой исследования. В каждой публикации были отмечены актуальные на сегодняшний день недостатки как самого процесса оценки рисков, так и отдельно технологий КМ и НС. Среди основных проблемных моментов:

– Необходимость обработки большого количества данных;

– Необходимость правильного формирования источников этих данных: недостаток данных или неправильная представительность обучающей выборки может повлиять на качество модели и ее способность к обобщению на новые данные;

– Недостаточный объем статистической информации об угрозах и уязвимостях;

– Сложности формального определения функции итогового показателя оценки;

– Важную роль играет опыт эксперта, необходима высокая квалификация специалистов по ИБ;

– Возможная разрозненность и несогласованность мнений нескольких экспертов;

– Невозможность комплексно оценивать влияние нескольких факторов на один узел нечеткой когнитивной карты, сложность интерпретации ее топологии;

– Неясность, как обучать алгоритмы рассчитывать наборы ВС. Сложность оценки силы связей концептов НКК;

– Проблема динамического изменения структуры НКК, при включении и выключении концептов в структуре НКК;

– Необходимость правильного выбора функции активации и обновления НКК.

В работе предложены способы устранения вышеперечисленных проблем за счет внедрения технологий КМ. Предложено применение гибридного модуля на одном из этапов оценки рисков ИБ. Модуль представляет собой комбинацию НКК с НС, которая обучается выставлять веса связи между концептами НКК. Это должно способствовать снижению рассогласованности и разрозненности мнений экспертов, и устранения необходимости работать с большими объемами данных, и тем самым ускорения процесса оценки. Что может повлиять на эффективность и точность процесса идентификации угроз, а также сделать этот

процесс адаптивным за счет гибкости, способности к обучению и обновлению с каждой новой итерацией.

Теоретическая и практическая значимость работы. Наработанный в результате исследования фактический материал и теоретические выводы могут быть использованы при изучении вопросов риск-менеджмента, адаптивной оценки рисков ИБ, КМ, НС. Практическая значимость исследования заключается в том, что полученные результаты могут использоваться в формировании алгоритмов и методов, способствующих улучшению процесса оценки рисков ИБ. За счет внедрения комбинированных технологий НКК и НС.

Методология и методы исследования. В ходе работы были использованы методы анализа для исследования различных типов нейронных сетей, их процесса обучения, архитектуры; когнитивных моделей; методы классификации для исследования алгоритмов обучения нейронной сети, типов нечетких когнитивных карт. Для построения функциональной модели оценки рисков ИБ, создания нечеткой когнитивной карты, алгоритма обучения нейронной сети оценивать веса связи между концептами карты были применены методы моделирования.

Положения, выносимые на защиту:

1. Функциональная модель оценки рисков ИБ с предложенными этапами, в которые можно вне.
2. Модели нечетких когнитивных карт для этапов оценки рисков ИБ.
3. Методика адаптивной оценки рисков на основе гибридного модуля из КМ и НС.
4. Алгоритм обучения НС выставлять веса связи для НКК.

Степень достоверности и апробация результатов. Полученные результаты диссертационного исследования подтверждены на научных конференциях и семинарах, публикациях в журналах ВАК.

Краткое содержание диссертации с упором на результаты, полученные за период реализации научного проекта в рамках гранта

За время реализации проекта для первой главы диссертации был проведен анализ ГОСТов, международных стандартов и других документов по оценке рисков ИБ [1-5]. На основе чего была сформирована функциональная модель оценки рисков ИБ, данная модель представлена на рис. 1.

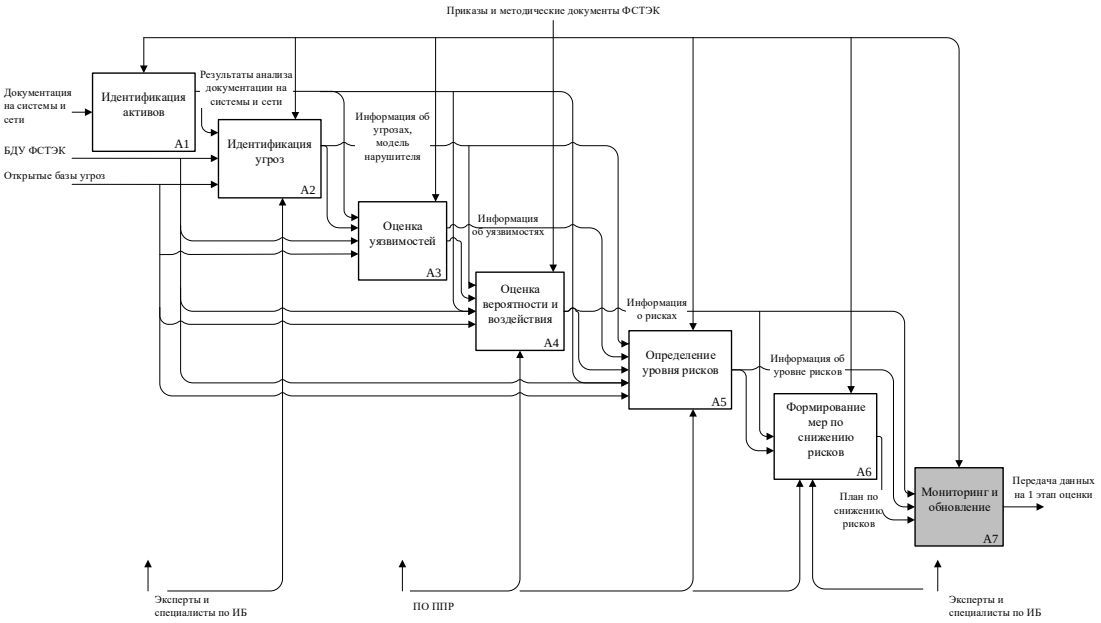


Рис. 1. Функциональная модель оценки рисков ИБ

Данная функциональная модель необходима для определения, в какой из ее этапов внедрить свойства адаптивности, чтобы повысить эффективность процесса оценки рисков ИБ. Также были проанализированы научные публикации по методам оценки рисков ИБ, технологиям когнитивного моделирования. Были исследованы особенности формирования НКК, ансамбля серых НКК [6-10]. Были проанализированы источники для формирования входных данных, на основе этого анализа был сформирован перечень этих источников (БДУ ФСТЭК, базы уязвимостей, открытые данные компаний, занимающихся вопросами ИБ).

Во второй главе в рамках проекта усовершенствована функциональная модель оценки рисков ИБ за счет внедрения гибридного модуля с НКК. Модуль позволяет формировать НКК, состоящую из различных концептов, данная карта способствует выбору именно тех факторов, которые могут влиять на оценку рисков. Данная карта представлена на рис. 2.

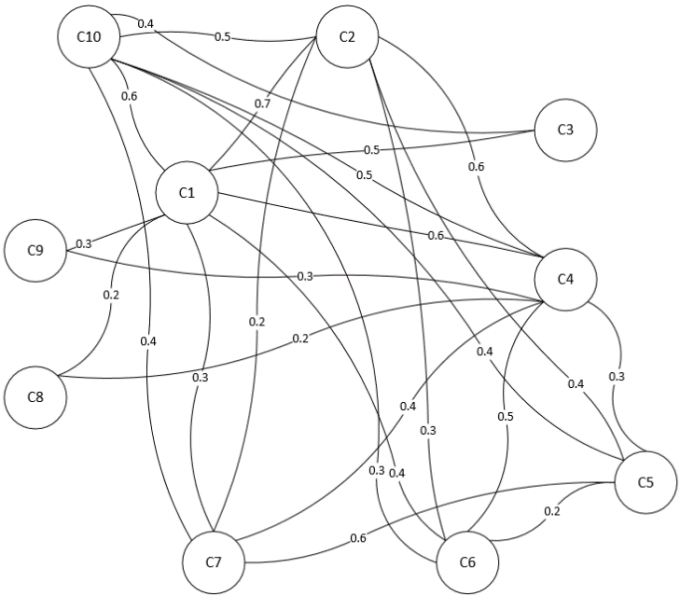


Рис. 2. НКК модели пространства рисков

Были исследованы подробно технологии КМ, обнаружены недостатки во время экспертной оценки в виде рассогласованности и разрозненности мнений экспертов, большого объема входных данных ввиду чего долгой скорости проведения самой оценки, что препятствует ей быть адаптивной. Для устранения этого предложено обучать НС самостоятельно выставлять веса связи НКК. В связи с чем были изучены более детально особенности технологий НС, их типы, элементы архитектуры, а также методы обучения [11-16]. Были протестированы разные архитектуры НС, разные методы обучения. В рамках проекта для данной задачи был выбран тип НС – многослойный персептрон, метод обучения - алгоритм обратного распространения ошибки и градиентного спуска. Алгоритм обучения НС проводить оценку весов связи НКК представлен на рис. 3.

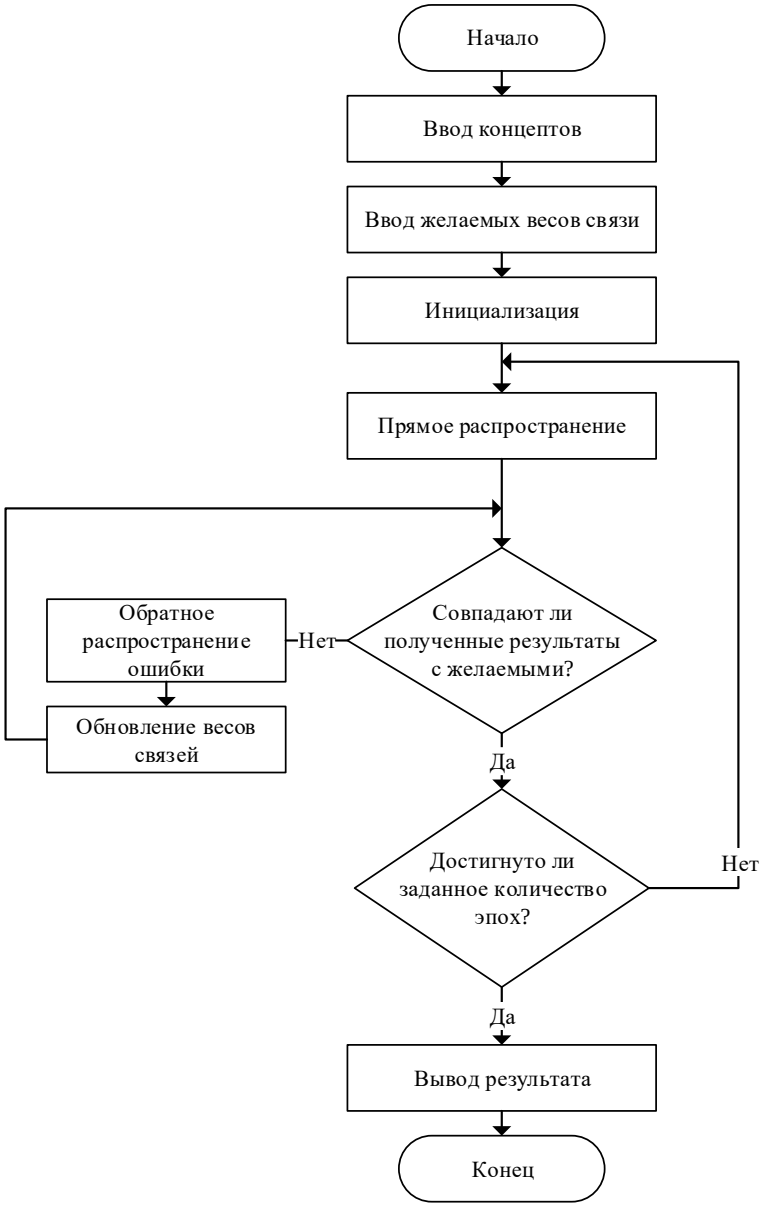


Рис. 3. Алгоритм обучения НС проводить оценку весов связи НКК

Чтобы оценить работоспособность предложенной модели, тем самым доказать применимость технологий КМ и НС в оценке рисков ИБ и повышении эффективности данного процесса за счет внедрения свойств адаптивности, важно учитывать то, на сколько быстро и хорошо НС обучается оценивать ВС НКК модуля «Идентификация угроз». Для этого было предложено использовать показатель средней абсолютной ошибки (MAE, Mean Absolute Error) [How to interpret MAE. [17]. MAE представляет собой разность между спрогнозированным и фактическим значениями. Чем ближе MAE к нулю, тем точнее модель. MAE рассчитывается по формуле:

$$MAE = (1/n) * \Sigma|y - \hat{y}|$$

Где y – действительные значения,

$\hat{y}$ – предсказанные значения,

n – количество примеров данных.

Рекомендации и перспективы дальнейшей разработки темы

Результаты научной работы могут быть использованы в системах оценки рисков ИБ. Дальнейшее развитие данного исследования заключается в проведении экспериментов по совершенствованию НС, корректировки ее архитектуры, размерности слоев с целью подбора наиболее оптимальной версии, а также поиск других блоков из предложенной функциональной модели, в которых можно использовать такую комбинацию технологий как НС и КМ.

СПИСОК ЛИТЕРАТУРЫ

1. ISO/IEC 31010:2019 Менеджмент риска. ПРИНЦИПЫ И РУКОВОДСТВО. 2019.
2. ГОСТ Р ИСО/МЭК 31010-2011. Менеджмент риска. Методы оценки риска. 2011. – 4 с.
3. ГОСТ Р № ИСО/МЭК 27001-2021 от 01.01.2022. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. 2022.
4. ISO 27001 Системы менеджмента информационной безопасности. 2021.
5. ISO/IEC 27005:2018 «Информационные технологии. Методы обеспечения безопасности. Менеджмент рисков информационной безопасности». 2018.
6. Гузаиров М. Б., Вульфин А. М., Картак В. М., Кириллова А. Д., Миронов К. В. Сравнительный анализ алгоритмов когнитивного моделирования при оценке рисков информационной безопасности/ Труды ИСА РАН, 2019. № 4. Том 69. DOI: 10.14357/20790279190408 URL: http://www.isa.ru/proceedings/images/documents/2019-69-4/62-69.pdf
7. Петухова А. В., Коваленко А. В., Теунаев Д. М. Обзор динамических свойств и алгоритмов обучения нечетких когнитивных карт/ Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета, 2021. № 163. Том 3. URL: https://cyberleninka.ru/article/n/obzor-dinamicheskih-svoystv-i-algoritmov-obucheniya-nechetkih-kognitivnyh-kart
8. Васильев В. И., Вульфин А. М., Герасимова И. Б., Картак В. М. Анализ рисков кибербезопасности с помощью нечетких когнитивных карт/DOI:10.21681/2311-3456-2020-2-11-21. URL: https://cyberrus.com/wp-content/uploads/2020/06/11-21-236-20_2.-Vasilyev.pdf
9. Васильев В. И., Вульфин А. М., Кириллова А. Д., Кучкарова Н. В. Методика оценки актуальных угроз и уязвимостей на основе технологий когнитивного моделирования и Text Mining/ Системы управления, связи и безопасности, 2021. № 3. URL: https://cyberleninka.ru/article/n/metodika-otsenki-aktualnyh-ugroz-i-uyazvimostey-na-osnove-tehnologiy-kognitivnogo-modelirovaniya-i-text-mining
10. Ефремова Н. А., Аверкян А. Н., Ярушев С. А. Гибридные нечеткие когнитивные карты в задачах поддержки принятия решений и прогнозирования/ Software journal theory and applications, 2017. № 4. DOI: 10.15827/2311-6749.25.291 URL: http://swsys-web.ru/hybrid-fuzzy-cognitive-maps-in-decision-support-tasks.html
11. Чупакова А. О., Гудин С. В., Хабибулин Р. Ш. Разработка и обучение модели искусственной нейронной сети для создания систем поддержки принятия решений/ Вестник Астраханского государственного технического университета. Серия: Управление, вычислительная техника и информатика, 2020. № 3. URL: https://cyberleninka.ru/article/n/razrabotka-i-obuchenie-modeli-iskusstvennoy-neyronnoy-seti-dlya-sozdaniya-sistem-podderzhki-prinyatiya-resheniy

12. Пивкин Е.Н., Белов В.М., Белкин С.А. К вопросу об анализе защищенности объектов информатизации с использованием нейронных сетей/ Доклады Томского государственного университета систем управления и радиоэлектроники, 2014. № 2 URL: https://journal.tusur.ru/storage/44773/30.pdf?1465976630

13. Миняев А. А. Моделирование угроз безопасности информации в территориально-распределенных информационных системах/ Наукоемкие технологии в космических исследованиях Земли, 2021. № 2. Том 13. URL: https://cyberleninka.ru/article/n/modelirovanie-ugroz-bezopasnosti-informatsii-v-territorialno-raspredelennyh-informatsionnyh-sistemah

14. Черкасов А. Н., Сивенко А. В. Разработка модели обеспечения безопасности аккаунта социальной сети на основе нейросетевого алгоритма/ Вестник Адыгейского государственного университета. Серия 4: Естественно-математические и технические науки, 2021. № 4. URL: https://cyberleninka.ru/article/n/razrabotka-modeli-obespecheniya-bezopasnosti-akkaunta-sotsialnoy-seti-na-osnove-neyrosetevogo-algoritma

15. Корнев Л. В. Нечеткая модель оценки рисков информационной безопасности и поддержки уровня защищенности ERP-систем / Молодой ученый. 2021. № 27. URL: https://moluch.ru/archive/369/83061\

16. Созыкин А. В. Обзор методов обучения глубоких нейронных сетей/ Вестник Южно-Уральского государственного университета. Серия: Вычислительная математика и информатика, 2017. № 3. Том 6. URL: https://cyberleninka.ru/article/n/obzor-metodov-obucheniya-glubokih-neyronnyh-setey

17. How to interpret MAE (simply explained). URL: https://stephenallwright.com/interpret-mae/?ref=helenkapatsa.ru

Русаков А.М.
РТУ МИРЭА, старший преподаватель
rusakov_a@mirea.ru

РЕЗУЛЬТАТЫ ПРОЕКТА «ОЦЕНКА ДИНАМИКИ РИСКОВ ДЕСТРУКТИВНОГО ВОЗДЕЙСТВИЯ ИНФРАСТРУКТУРНОГО ГЕНЕЗА»

Аннотация: Во время перехода к цифровой экономике особенно актуальны вопросы информационной безопасности субъектов критической информационной инфраструктуры (КИИ). С ростом информационных технологий наряду с быстрым моральным «старением» средств защиты информации остаются нерешенные вопросы оценки рисков инфраструктурного характера субъектов КИИ. В данном проекте предлагаются модели и алгоритмы оценки рисков субъектов КИИ с учетом возникающих межобъектных и межсубъетных системных связей инфраструктурного характера, обоснованных тем, что сама система при определенных условиях может генерировать деструктивизм инфраструктурного характера, приводящий к катастрофическим последствиям. В рамках проекта разработана антропоморфическая модель взаимодействия деструктивных воздействий инфраструктурного генеза, которая основывает процесс взаимодействия элементов КИИ с позиции мира живых микроорганизмов. Разработана эпидемиологическая модель оценки рисков динамики межобьектного влияния в условиях инфраструктурного деструктивизма, которая позволяет оценивать динамические риски информационной безопасности для КИИ с позиции инфраструктурного деструктивизма. Предложен метод оценки деструктивных воздействий инфраструктурного генеза для различных типов информационных инфраструктур позволяющий выполнять их классификацию и оценивать «стрессоустойчивость» КИИ.

Ключевые слова: инфраструктурный деструктивизм, деструктивные воздействия инфраструктурного генеза, критическая информационная инфраструктура

В последние десятилетия роль КИИ в обеспечении устойчивого развития различных отраслей цифровой экономики стала неоспоримой. Однако, недостаточное внимание к оценке рисков деструктивных воздействий на информационные инфраструктуры приводит к серьезным последствиям, которые могут негативно повлиять на функционирование и развитие социально-экономических систем в целом.

Оценка рисков деструктивных воздействий инфраструктурного генеза является сложной задачей, которая требует использования современных методов и инструментов. Под инфраструктурным деструктивизмом будем понимать накопление различных эффектов деструктивных воздействий (кибератак, вирусов и т.д.) которое приводит к невозможности функционирования информационной инфраструктуры в штатном режиме [1-2].

Специфичные для КИИ признаки и свойства определяют динамизм рисков деструктивного воздействия инфраструктурного генеза, порождаемых самой инфраструктурой [3, 4], что требует их исследования в контексте ИБ.

Тема проекта связана с разработкой модели динамики рисков деструктивного воздействия инфраструктурного генеза. Диссертационное исследование выполнено на тему: «Методы и алгоритмы оценки рисков деструктивных воздействий инфраструктурного генеза».

Цель исследования: повышение уровня информационной безопасности объектов критической информационной инфраструктуры за счет оценки рисков деструктивных воздействий инфраструктурного генеза.

Среди работ в области защиты КИИ от деструктивных воздействий следует выделить работы М.В. Буйневича, К.Е. Израилова, М.А. Еремеева, А.К. Новохрестова, С.И. Макаренко, Г.В. Бабенко, Н.А. Гайдамакина, П.Н. Девянина, Д.П. Зегжды, П.Д. Зегжды, Е.А. Максимовой и других ученых. Перспективными являются работы Г. А. Остапенко, А. Н. Шершень[5, 6]; С. И. Макаренко [7]; П. Д. Зегжда, В. Г. Анисимов, А. Ф. Супрун [8]; Е. А. Басыни [9]; Д. В. Афанасьевой [10].

В рамках проекта разработана **антропоморфическая модель взаимодействия деструктивных воздействий инфраструктурного генеза**, которая основывается на описание процесса взаимодействия элементов КИИ с позиции «живых» микроорганизмов. Опишем данную модель использую теоретико-множественное представление. Пусть: $O_1, O_2 \dots O_n$ – взаимодействующие элементы КИИ; $S_1, S_2 \dots S_m$ – взаимосвязанные моногенные подсистемы инфраструктур КИИ; D_1 и D_2 – источники деструктивных воздействий; R_1 и R_2 – результаты воздействий D_1 и D_2 соответственно;. Информационное взаимодействие между элементами инфраструктур является важным процессом, прямо отражающимся на процессе функционирования инфраструктуры в целом. Охарактеризуем виды имеющихся взаимодействий и воздействий между элементами КИИ.

Под **негативным воздействием** на КИИ будем понимать различные уязвимости, вирусы, кибератаки, и другие негативные воздействия, которые могут вывести информационную инфраструктуру из строя, обозначим данные воздействия через источники деструктивных воздействий D_1 и D_2, в количественном отношения будем обозначать как $-1d_1 \dots 0$ и $-1d_2 \dots 0$.

Под **позитивным воздействием** на КИИ будем понимать различные эффекты от деструктивных воздействий D_1 и D_2, которые приводят к положительным эффектам на информационную инфраструктуру в целях информационной безопасности при этом данные воздействия в количественном отношения будем обозначать как $+1d_1 \dots 0$ и $+1d_2 \dots 0$ соответственно.

Модель основывается на допущении о том, что взаимодействие деструктивных воздействий инфраструктурного генеза принципиально схоже со взаимодействием биологических микроорганизмов. Согласно широко распространенному в науке делению отношений организмов известны следующие типы их взаимодействий: симбиоз (облигатный и факультативный симбиоз, комменсализм, паразитизм, хищничество) – когда хотя бы один из организмов получает выгоду, антибиоз (аменсализм, аллелопатия, конкуренция) – когда один из организмов ограничивает возможности другого, и нейтрализм – сосуществования организмов без взаимного влияния. В этой работе приведем два крайних случая, когда деструктивные воздействия образуют факультативный симбиоз и аллелопатию, которые дают максимальный и минимальный антропоморфический эффект.

Рассмотрим факультативный симбиоз деструктивных воздействий, который в природе характеризуется взаимной выгодой от совместного сосуществования организмов, но без необходимости как таковой. То есть деструктивные воздействия влияют на информационную

инфраструктуру, но при этом деструктивный эффект от их совместного взаимодействия возрастает.

Положим, что эффект возрастает со знаком минус $-2d_1$ при условии наличия деструктивных воздействий $-1d_2$ и $-2d_2$ при условии $-1d_1$ соответственно. Таким образом общий эффект от факультативного симбиоза составит $-2d_1 - 2d_2$, что соответствует следующей формуле: $-2(d_1 + d_2)$, которая подтверждается механизмами существования микроорганизмов в живой природы. Схематически отобразим данное явление на рисунке 1.

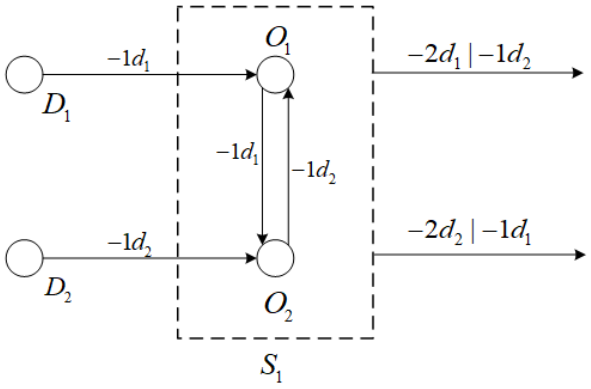


Рис. 1. Схема факультативный симбиоз деструктивных воздействий

Рассмотрим аллелопатию деструктивных воздействий. С позиции живой природы данный тип взаимодействия биологических организмов характеризуется их взаимно-вредным влиянием друг на друга. То есть деструктивные воздействия влияют на информационную инфраструктуру, но при этом они сами себя уничтожают.

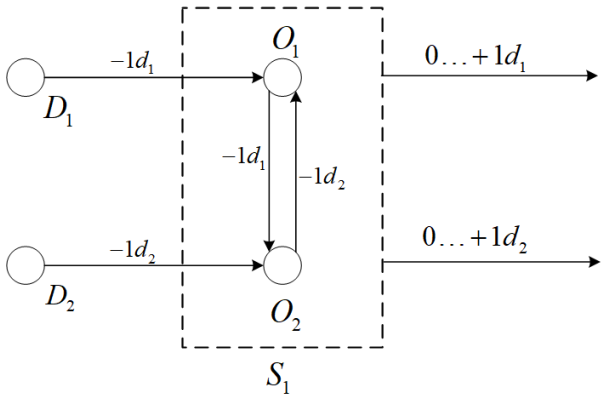


Рис. 2. Схема аллелопатия деструктивных воздействий.

Таким образом общий эффект от аллелопатии деструктивных воздействий составит в худшем случае 0 и в лучшем случае составит $1d_1 + 1d_2$, что также подтверждается механизмами существования живой природы. Описав данные процессы для всех антропоморфических механизмов взаимодействия деструктивных воздействий стало возможным качественно и количественно оценить каждый из них как по отдельности, так и в совокупности.

В рамках проекта разработана **эпидемиологическая модель оценки рисков динамики межобъектного влияния в условиях инфраструктурного деструктивизма**. Рассмотрены следующие эпидемиологические модели: SI-модель, SIR-модель, SEIR модель, PSIDR-модель. Наиболее адекватной моделью для данной задачи показала себя SEIR модель.

В SEIR-модели учитывается возможность того, что деструктивное воздействие инфраструктурного генеза может иметь некий "латентный период", во время которого оно не наносит какого-либо вреда КИИ [11]. Обычно деструктивное воздействие поражает уязвимую инфраструктуру (S) до входа в свою латентную стадию, в течение латентного периода (Ex, Exposed) элемент инфраструктуры считается заражённым, но не распространяет деструктивные воздействия, через некоторое время он становиться способным к заражению других (I) и далее становиться "вылеченным" (R) [11]. Предложенная модель реализована на основе многоагентной системы моделирования NetLogo [12] и позволяет оценивать динамику рисков инфраструктурного генеза деструктивных воздействий с учетом антропоморфической модели взаимодействия активных элементов.

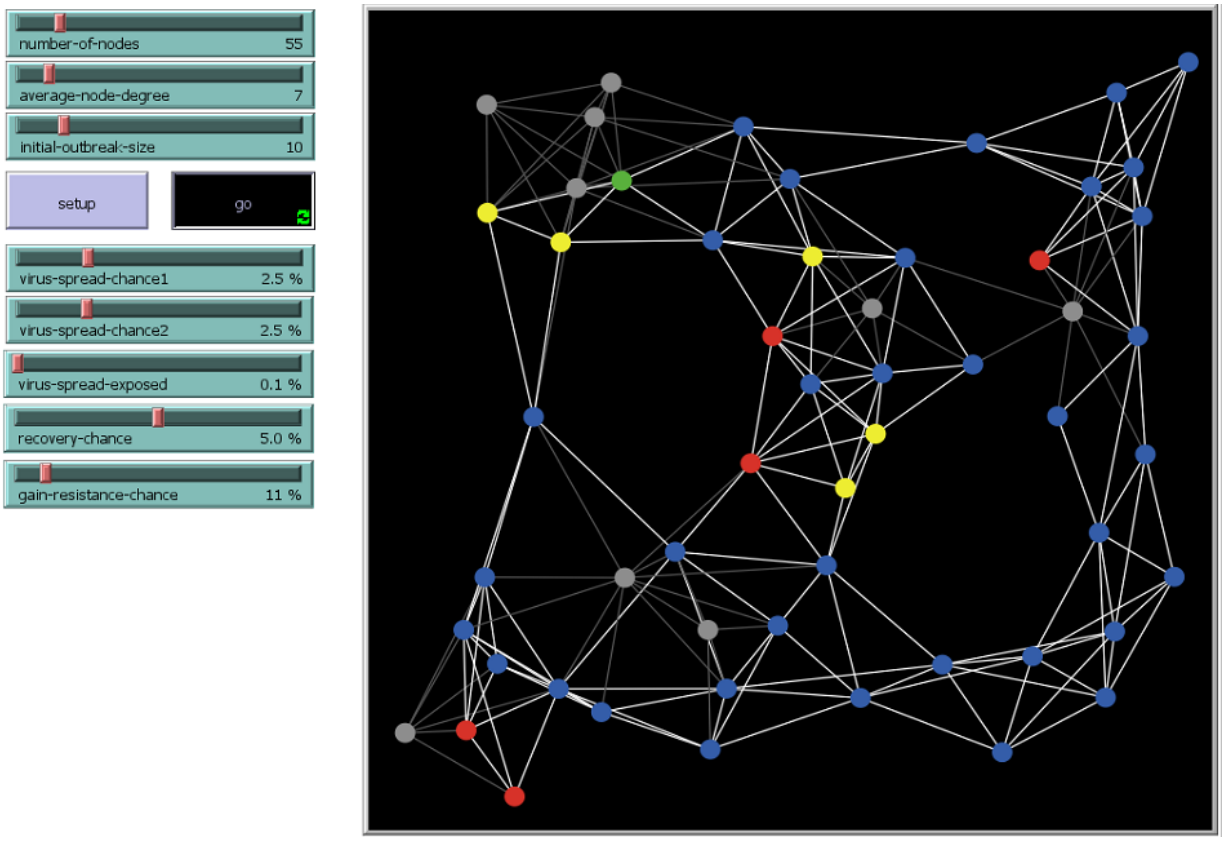


Рис. 3. Программное обеспечение для оценки динамики рисков инфраструктурного генеза деструктивных воздействий

На рисунке 3 представленно основное окно программного средства динамики рисков инфраструктурного генеза деструктивных воздействий. На рисунке 4, приведены графики оценки динамики рисков КИИ. Благодаря данному программному средству стало возможным оценить риски как на этапе проектирования, так и на этапе эксплуатации КИИ.

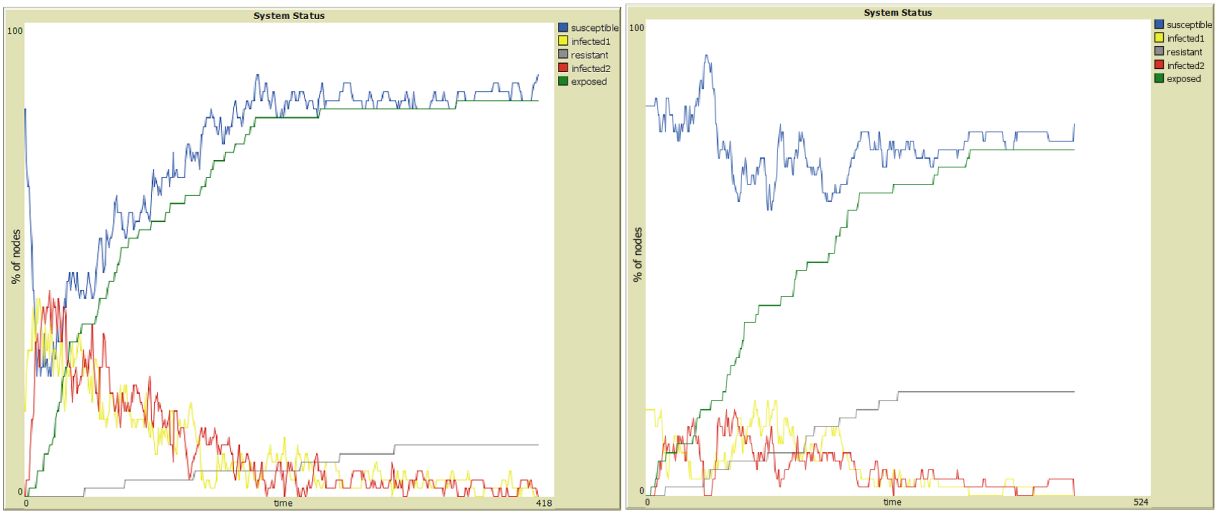


Рис. 4. Графики состояния КИИ при деструктивных воздействиях

В проекте предложен **метод оценки деструктивных воздействий инфраструктурного генеза для различных типов инфраструктур**. Предлагается использовать специальную спектральную теорию графов для анализа структурной сложности КИИ с целью определения ее энергетической составляющей [13, 14]. Спектральная теория графов позволяет судить о свойствах графа по свойствам матриц, связанных с ним (смежности, лапласиана, инцидентности) [15]. Спектр представляет собой мультимножество собственных значений. Применение спектральной теории графов к анализу информационных инфраструктур позволяет повысить информационную безопасность информационных инфраструктур на стадии их проектирования за счет прогнозирования эффекта инфраструктурного деструктивизма.

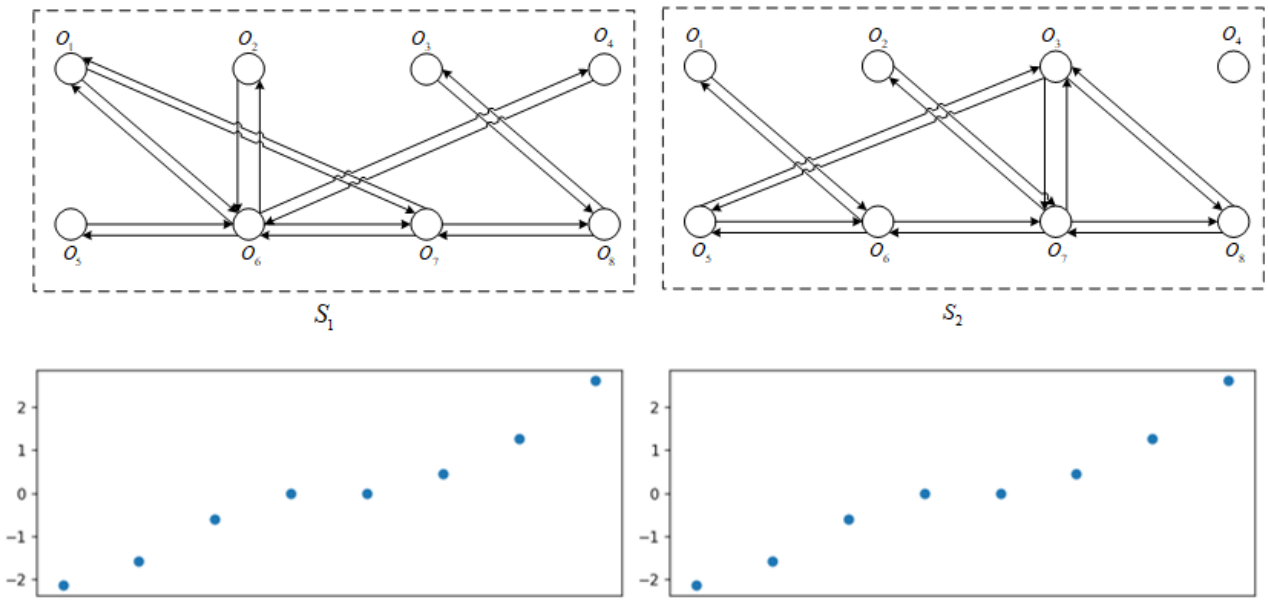


Рис. 5. Схемы информационных инраструктур и их спектр.

В проекте показано, что спектр графа является решающим фактором для классификации информационных инфраструктур с позиции деструктивных воздействий инфраструктурного генеза. На рисунке 5 показаны две схемы информационных

инфраструктур для которых спектральная энергетическая составляющая одинаковая. Применяя данный подход, стало возможным оценить схожесть графов информационных инфраструктур и тем самым выделять различные категории рисков инфраструктурного деструктивизма. В проекте введена классификация информационных инфраструктур, а также понятие стрессоустойчивость КИИ к деструктивным воздействиям инфраструктурного генеза.

Задача повышения уровня информационной безопасности КИИ за счёт разработки методов и алгоритмов оценки рисков деструктивных воздействий инфраструктурного генеза благодаря поддержки гранта частично решена в данном проекте.

СПИСОК ЛИТЕРАТУРЫ

1. Максимова, Е. А. Модель состояний субъектов критической информационной инфраструктуры при деструктивных воздействиях в статичном режиме / Е. А. Максимова // Труды учебных заведений связи. – 2021. – Т. 7. – № 3. – С. 65-72. – DOI 10.31854/1813-324X-2021-7-3-65-72.
2. Максимова, Е. А. Оценка информационной безопасности субъекта критической информационной инфраструктуры при деструктивных воздействиях / Е. А. Максимова; Волгоградский государственный университет. – Волгоград: Волгоградский государственный университет, 2020. – 95 с. – ISBN 978-5-9669-1975-7.
3. Anthropomorphic Model of States of Subjects of Critical Information Infrastructure Under Destructive Influences / E. A. Maksimova, A. M. Rusakov, M. A. Lapina, V. G. Lapin // Lecture Notes in Networks and Systems. – 2022. – Vol. 424. – P. 569-580. – DOI 10.1007/978-3-030-97020-8_51.
4. Максимова, Е. А. Метод оценки инфраструктурной устойчивости субъектов критической информационной инфраструктуры / Е. А. Максимова, М. В. Буйневич // Вестник УрФО. Безопасность в информационной сфере. – 2022. – № 1(43). – С. 50-63. – DOI 10.14529/secur220107.
5. Предупреждение и минимизация последствий компьютерных атак на элементы критической информационной инфраструктуры и автоматизированные информационные системы критически важных объектов: риск-анализ и оценка эффективности защиты / А. Г. Остапенко, Е. В. Ермилов, А. Н. Шершень [и др.] // Информация и безопасность. – 2013. – Т. 16. – № 2. – С. 167-178.
6. Остапенко, Г. А. Концептуальный подход к расчету и регулированию рисков нарушения актуальности информации в элементах критической информационной инфраструктуры / Г. А. Остапенко, А. Н. Шершень, А. О. Калашников // Информация и безопасность. – 2013. – Т. 16. – № 2. – С. 239-242.
7. Макаренко, С. И. Динамическая модель двунаправленного информационного конфликта с учетом возможностей сторон по наблюдению, захвату и блокировке ресурса / С. И. Макаренко // Системы управления, связи и безопасности. – 2017. – № 1. – С. 60-97. – DOI 10.24411/2410-9916-2017-10106.
8. Зегжда П. Д., Анисимов В. Г., Супрун А. Ф. и др. Модели и метод поддержки принятия решений по обеспечению информационной безопасности информационно-управляющих систем //Проблемы информационной безопасности. Компьютерные системы. – 2018. – №. 1. – С. 43-47.

9. Басыня, Е. А. Распределенная система сбора, обработки и анализа событий информационной безопасности сетевой инфраструктуры предприятия / Е. А. Басыня // Безопасность информационных технологий. – 2018. – Т. 25. – № 4. – С. 42-51.
10. Афанасьева, Д. В. Применение искусственного интеллекта в обеспечении безопасности данных / Д. В. Афанасьева // Известия Тульского государственного университета. Технические науки. – 2020. – № 2. – С. 151-154.
11. Зегжда П. Д. и др. Эффективность функционирования компьютерной сети в условиях вредоносных информационных воздействий //Проблемы информационной безопасности. Компьютерные системы. – 2021. – №. 1. – С. 96-101.
12. Wilensky, U. (1999). NetLogo. http://ccl.northwestern.edu/netlogo/. Center for Connected Learning and Computer-Based Modeling, Northwestern University, Evanston, IL.
13. Русаков, А. М. Исследование структурных свойств информационных систем на основе спектральной теории графов / А. М. Русаков, Н. А. Юшкова // Наукосфера. – 2023. – № 6-1. – С. 192-199. – DOI 10.5281/zenodo.8055586.
14. Козлов С. В. Интерпретация инвариантов теории графов в контексте применения соответствия Галуа при создании и сопровождении информационных систем // International Journal of Open Information Technologies. 2016. Т. 4. №. 7. С. 38-44.
15. Qiu L., Ji Y., Wang W. On a theorem of Godsil and McKay concerning the construction of cospectral graphs // Linear Algebra and its Applications. 2020. Т. 603. С. 265-274.

Сипович Д.Е.
РГГМУ ст. преподаватель каф. ИТ и СБ,
d.sipovich@rshu.ru

РАЗРАБОТКА МОДЕЛИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ТЕЛЕКОММУНИКАЦИОННОЙ СИСТЕМЫ В КОНТУРЕ УПРАВЛЕНИЯ МУНИЦИПАЛЬНЫМ ОБРАЗОВАНИЕМ

Аннотация: существующие модели обеспечения информационной безопасности базируются на угрозах которые были применены в одной из систем и эта система не смогла эту угрозу распознать. На основании полученного опыта была разработана методика, на основании которой получили опыт и этим опытом пользуются. Как противостоять новой угрозе о которой никто не знает написано в этом документе.

Ключевые слова: Информационная безопасность, синтез модели информационной безопасности, телекоммуникационная система.

В современных условиях развития общества особое значение приобретают информационные процессы. Особо актуальным является рынок информационных услуг. Насколько государство успешно управляет этим рынком, на столько успешно осуществляется социально-экономическое, промышленное развитие региона.

Анализ показал, что особую важность на информационном пространстве России имеет телекоммуникационные системы. Данная совокупность факторов и определяет актуальность настоящей работы, а целью настоящей работы является:

выбрать, обосновать, и реализовать условия обеспечения информационной безопасности на базе разработки аналитической динамической модели систем интеграции базовых процессов**.**

Дано: Муниципальное образование, система управления на базе элементов телекоммуникации.

Требуется: Разработать аналитическую динамическую модель информационной безопасности на базе телекоммуникационной

системы основанную на интеграции трёх базовых и целевого процессов:

- процесса целевого функционирования телекоммуникационной системы;

- процесс образования угрозы;

- процесс идентификации угрозы;

- процесс нейтрализации угрозы.

Объект: телекоммуникационная система.

Задача: разработка модели управления информационной безопасности: (декомпозиция на 4 подзадачи)

1.Проанализировать известные методы, модели, технологии и особенности обеспечения информационной безопасности в условиях деструктивных воздействий на основе использования закона сохранения целостности объекта.

2.Разработать модель системной интеграции процессов обеспечения информационной безопасности в условиях деструктивных воздействий на основе применения ЗСЦО.

3.Разработать технологию управления процессами обеспечения информационной безопасности телекоммуникационной системы в условиях деструктивных воздействий на основе применения закона сохранения целостности объекта.

4.Разработать предложения по совершенствованию системы обеспечения информационной безопасности ТКС в условиях деструктивных воздействий на основе применения ЗСЦО.

Выбор, обоснование и реализация условий обеспечения информационной безопасности телекоммуникационной системы в контуре управления муниципальным образованием на базе разработки аналитической динамической модели системной интеграции базовых процессов**.**

Для достижения данной цели, поставлена и решена задача, определен предмет и объект. Решение поставленной задачи потребовало решения четырёх основных подзадач.

Сервисы, предоставляемые телекоммуникационной системой, представлены на рисунке 1.

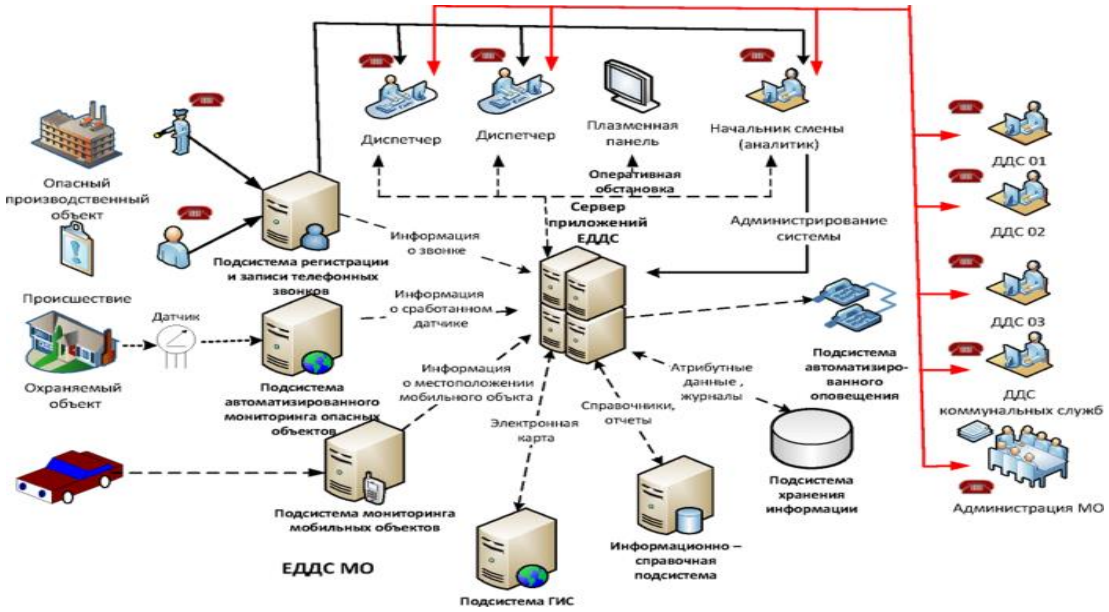


Рис. 1 Сервисы предоставляемые телекоммуникационной системой.

Из теории функциональных систем Анохина следует – все объекты окружающего мира, созданные человеком, **есть реализация модели решения человека, главного конструктора**.

Отсюда следует, что если мы имеем адекватную модель решения человека, то и модель построения и функционирования объекта, с которым работает человек, будет адекватна. А сам объект при функционировании будет давать требуемый результат! **Отсюда можно сделать вывод :**

Проблема информационной безопасности – деятельность не соответствующая ожиданиям.

1.Неудовлетворительный результат управления обоснован противоречивыми выводами.

2.Для исключения противоречивых выводов следует использовать аксиоматический метод

3.Аксиоматический метод предполагает существование следующих элементов

3.1.Основные допущения и предположения, обычно выражающихся базовых принципах.

3.2. Базовых понятий, ключевых слов, Аксиом; Правил вывода; Теорем

4.В процессе деятельности участвуют

1.Человек, его сознание.

2.Окружающий МИР(объект).

3.Нечто, что дано природой и позволяет осуществлять познание. (Всеобщая связь)

5.Трёхкомпонентность отражается в трёх принципах.

Для построения адекватной модели необходимо, чтобы решение человека, лица принимающего решение было основано на системной интеграции свойств мышления человека, свойств объектов окружающего мира и всеобщей связи явлений. **В изученных публикациях по выработке управленческого решения построить математическую модель не представляется возможным.** Согласно трудов Анохина - **нет системообразующего фактора.**

Поэтому нам не остаётся как только воспользоваться для формирования условий гарантирующих достижения цели деятельности естественно-научным подходом**.** В данном подходе мы будем использовать Аксиоматический метод для исключения противоречивых выводов, которые являются следствием неудовлетворительного результата управления.

3.Аксиоматический метод предполагает существование следующих элементов

3.1.Основные допущения и предположения, обычно выражающихся базовых принципах.

3.2. Базовых понятий, ключевых слов, Аксиом; Правил вывода; Теорем

4.В процессе деятельности участвуют

1.Человек, его сознание.

2.Окружающий МИР(объект).

3.Нечто, что дано природой и позволяет осуществлять познание. (Всеобщая связь)

5.Трёхкомпонентность отражается в трёх принципах.

Существует 2 подхода построения систем обеспечения информационной безопасности на основе анализа и на основе синтеза.

Подход на основе анализа:

+ прост в применении,

- не в полной мере позволяет достигать цели обеспечения информационной безопасности в сложных системах.

Подход на основе синтеза:

- формирование процесса с наперёд заданными свойствами,

- формирования условий, гарантирующих достижения цели деятельности используя естественно - научный подход (ЕНП).

Недостатки: трудности в реализации.(отсутствует закон функционирования и построения систем). (Гуд . Макол 1957г.)

Для решения указанных трудностей необходимо:

- условие существования процесса. Решение основано на системной интеграции свойств мышления человека, свойств объектов окружающего мира и всеобщей связи явлений. Человек осуществляет свою деятельность на основе модели. (Анохин 1979, Бурлов 2007) **Без математической модели не возможно получить гарантированный результат.**

Метод «Трансформации вербальной модели решения в формальную модель на основе регламентации пространственно-временных состояний 3-мя базовыми принципами»

Базовые принципы естественно-научного подхода.

1.**Принцип** трёхкомпонентности познания.

Компонент А. Абстрактное представление (Условие существования). (Методология.))

Компонент В. Абстрактно-конкретное. (Причинно-следственные связи.) (Методы).

Компонент С. Конкретное представление (Технологии. Алгоритмы.)

2.Принцип целостности Мира. Реализуется ЗСЦО (Burlov, V. G. (2007). Burlov, V. G. (2015)). *ЗСЦО* **-** устойчивая повторяющаяся связь свойств объекта и свойств действия при фиксированном предназначении.

В соответствии с ЕНП каждый процесс должен быть представлен тремя компонентами, соответствующим свойствам «объективность», «целостность» и «изменчивость» (или понятиям «объект», «предназначение» и «действие» соответственно рис. 3).

3.Принцип познаваемости Мира. Реализуется методами

Декомпозиция.

Абстрагирование.

Агрегирование.

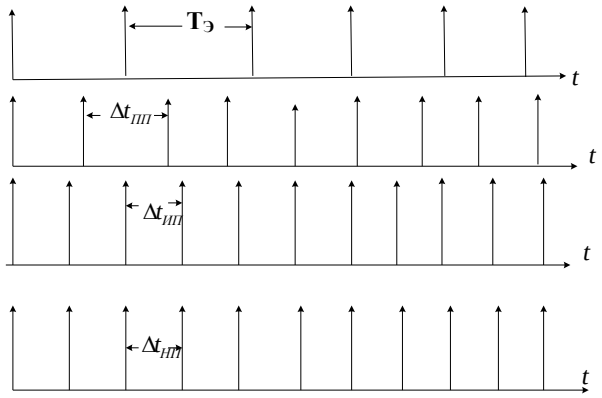


Рис. 2 Диаграмма проявления базовых элементов формирования модели решения.

Представленная структурная схема модели “Решения” на рис. 3 после применения декомпозиции содержит 3 взаимосвязанных компонента.

Обстановка,

информационно-аналитическая работа,

решение.

Применяя абстрагирование обстановка представлена 2 процессами (**Целевой процесс, процесс проявления проблемы**). Решение представлено – **процессом нейтрализацией**, **информационно-аналитическая работа – процессом идентификации**. Для синтеза математической модели применим методы декомпозиции, абстрагирования и агрегирования. Показатель безопасности представлен как функция от базовых процессов.

Применяя метод агрегирования, получим условие существования решения в виде следующего соотношения **(1)**

P = F (*T*э, Δ*t*пп Δ*t*нп Δ*t*нп). (1)

P – характеризует степень достижения цели в деструктивных условиях. Это вероятность того что проблема идентифицируется и нейтрализуется.

Рис. 3 Структурная схема модели “Решения”

Таким образом представим управленческое решение в виде схемы рис. 4

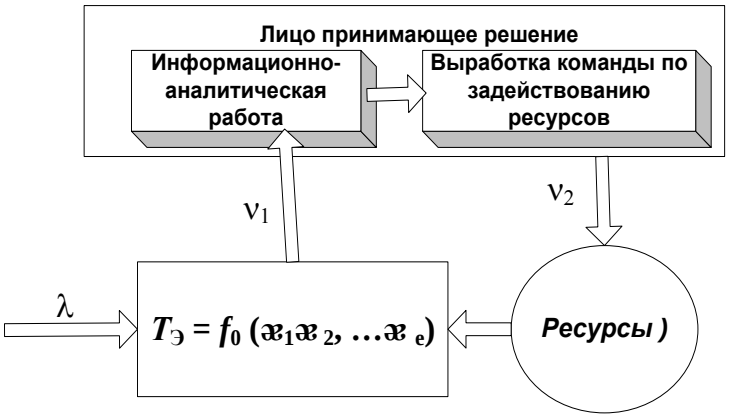


Рис. 4 Схема управленческого решения.

Процесс формирования решения согласно трудов АН СССР Анохина представлен в виде графа Рис. 5**.**

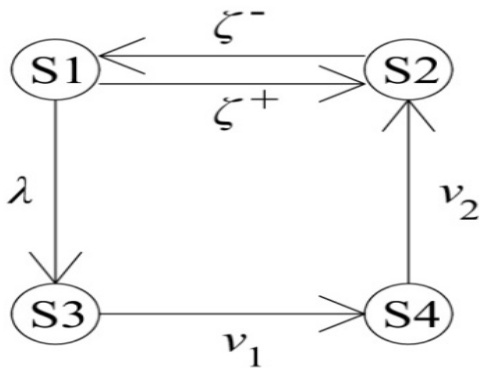


Рис. 5 Граф процесса формирования решения.

В виде условия существования процесса простроена телекоммуникационная система, настроено оборудование и .т.д. Для описания процесса изменений состояния состояний на графе необходимо сделать следующие допущения:

1.Рассматривается схема формирования решения человека в форме информационно-управляющей системы. На основе решения формируется процесс обеспечения безопасности.

2. Промежуток времени между началом и концом целевого процесса (этапа целевой деятельности) является величиной случайной.

3. Промежутки времени между моментами обнаружения фактов проявления проблем являются величинами случайными.

4. Обнаруженные факты во времени образуют поток, близкий к потоку Пуассона.

5. Время обработки данных о требуемом признаке является величиной случайной.

6. Данные о признаках распределяются далее между выделенными ресурсами, решающими соответствующие целевые задачи по обеспечению безопасности.

7. Рассматривается случай, когда время пребывания требуемых признаков (фактов) в области действия системы (человека) весьма ограниченно и соизмеримо со временем, которое необходимо для их идентификации, а также обработки данных и принятия адекватных действий по этим признакам.

8. Система подготовлена к решению задач распознания и нейтрализации проблем.

9. Разрабатываемая система (решение человека) предназначена для оценивания потенциальных возможностей системы обеспечения безопасности в зависимости от обстановки.

Согласно сделанных допущений и предположений позволяют использовать систему ДУ Колмагорова –Чепмена **(2)**.

$$\begin{cases} \dfrac{dP_1(t)}{dt} = -(\zeta^+ + \lambda)\cdot P_1(t) + \zeta^- \cdot P_2(t), \\ \dfrac{dP_2(t)}{dt} = \zeta^+ \cdot P_1(t) - \zeta^- \cdot P_2(t) + \nu_2 \cdot P_4(t), \\ \dfrac{dP_3(t)}{dt} = \lambda \cdot P_1(t) - \nu_1 \cdot P_3(t), \\ \dfrac{dP_4(t)}{dt} = \nu_1 \cdot P_3(t) - \nu_2 \cdot P_4(t). \end{cases} \quad (2)$$

Показателем эффективности управления безопасности функционирования телекоммуникационной системы является передача требуемого кол-ва пакетов в единицу времени**.** Это определяется соотношением P2 **(3)**.

$$P_2 = \frac{\lambda\cdot\nu_1\cdot\nu_2 + \zeta^+\cdot\nu_1\cdot\nu_2}{\lambda\cdot\zeta^-\cdot\nu_1 + \lambda\cdot\zeta^-\cdot\nu_2 + \lambda\cdot\nu_1\cdot\nu_2 + \zeta^+\cdot\nu_1\cdot\nu_2 + \zeta^-\cdot\nu_1\cdot\nu_2} \quad (3)$$

Результаты решения четырёх подзадач позволило получить решение основной задачи, а именно удалось разработать технологию управления моделью безопасности. И тем самым достичь поставленной цели:

Выбрать и обосновать и реализовать условия обеспечения информационной безопасности пути развития телекоммуникационной системы в интересах обеспечения экономического развития региона.

Реализация условия обеспечения информационной безопасности в телекоммуникационной системе реализованной в муниципальном образовании г. Сланцы Ленинградской области с показателем эффективности 0,8 основано на частоте поступающих событий возникающих аварий на сети и скорости их нейтрализации с доступностью функционирования каждого узла не менее 95%. Проблемой в реализации данного показателя эффективности является дифицит или отсутствие требуемых ресурсов. Для решения этой проблемы интегрированы и использованы программно-аппаратные средства обеспечения функционирования оборудования. Для обеспечения электропитания используется 1 категория электроснабжения. На магистральных линиях используется различные среды дублирования передачи данных.

СПИСОК ЛИТЕРАТУРЫ

1. Постановление Правительства Российской Федерации от 31 марта 2020 г. № 386-20
2. П. Д. Зегжда, В. Г. Анисимов, П. В. Семьянов Е. Г. Анисимов, Т. Н. Сауренко “Подход к оцениванию эффективности защиты информации в управляющих системах” Журнал: Теоретические основы информационной безопасности №1 2020г. на с.9.
3. Сауренко Т. Н. Прогнозирование инцидентов информационной безопасности /Т. Н. Сауренко и др. // Проблемы информационной безопасности. Компьютерные системы. — 2019. — № 3. — С. 24–28.
4. Павленко Е. Ю. Зегжда Д. П. Устойчивость киберфизических систем в контексте целенаправленных деструктивных воздействий. 2018 IEEE Industrial Cyber-Physical Systems (ICPS), St. Petersburg, Russia, 2018. — IEEE, 2018. — P. 830–834
5. Показатели эффективности защиты информации в системе информационного взаимодействия при управлении сложными распределенными организационными объектами. Анисимов В.Г., Анисимов Е.Г. , Зегжда П.Д., Сауренко Т.Н., Присяжнюк С.П., Прохорова А.М. **Страницы 140-145**
6. Ожегов С.И. Словарь русского языка. 20-е издание. Под редакцией чл.-корр. АН СССР. Н.Ю. Шведовой. «Русский язык». Москва – 1988. – 751с
7. П. Д. Зегжда, В. Г. Анисимов, П. В. Семьянов Е. Г. Анисимов, Т. Н. Сауренко “Подход к оцениванию эффективности защиты информации в управляющих системах” Журнал: Теоретические основы информационной безопасности №1 2020г. на с.9.
8. Характеристики мониторинга безопасности киберфизических систем. М. А. Полтавцева Журнал: Теоретические основы информационной безопасности №1 2020г. на с.73.
9. Горбачев И. Е. Моделирование процессов нарушения информационной безопасности критической инфраструктуры / И. Е. Горбачев,А. П. Глухов // Труды СПИИРАН. — 2015. — Том. 38 (2015). — С. 112–135.

10. Humayed A. et al. Cyber-Physical Systems Security — A Survey // IEEE Internet of Things Journal. 2017. — Vol. 4. — № 6. — P. 1802–1831. — Doi: 10.1109/JIOT.2017.2703172

11. Giraldo J. et al. A Survey of Physics-Based Attack Detection in Cyber-Physical Systems. // ACM Comput. Surv. 2018. — Vol. 51. — № 4. — P. 1–36. — Doi: 10.1145/3203245

12. Моисеев Н.Н. Математические задачи системного анализа. Наука. Москва. 1981 г. 468с.

13. Анохин П.К. Принципиальные вопросы общей теории функциональных систем. М.: Директ-Медиа, 2008. 131 с.

14. П. Д. Зегжда, В. Г. Анисимов, П. В. Семьянов Е. Г. Анисимов, Т. Н. Сауренко “Подход к оцениванию эффективности защиты информации в управляющих системах” Журнал: Теоретические основы информационной безопасности №1 2020г. на с.9.

15. Д. С. Лаврова, Р. С. Соловей обеспечение информационной безопасности беспроводных динамических сетей на основе теоретико-игрового подхода. Журнал проблемы информационной безопасности компьютерные системы № 2 2020г. с.16

16. Бурлов В.Г. Основы моделирования социально-экономических и политических процес-сов (Методология. Методы) СПб: Факультет Комплексной Безопасности, СПБГПУ.2007г.-265 с.

17. Организационная защита информации В.И. Аверченков, М.Ю. Рытов Издательство БГТУ Брянск 2005 180с ISBN 5-89838-141-4.

18. Бурлов В.Г. Логико-алгебраическая концепция построения модели системы и её приложение для синтеза системы защиты информации (в кн. «Безопасность информации регионов России») НТК 13-15. 10. 1999 г.- СПб.; СПИИРЛН, 1999.

19. Бурлов В.Г. Методы построения систем поддержки принятия решения, основанные на логико алгебраической системной концепции математики. (Тезисы доклада) НТК 28-29 10, - С-Пб; ВИКУ им. А.Ф., 1999.

20. Андреев А.В., Бурлов В.Г., Гомазов Ф.А. Технология управления процессами обеспечения безопасности трудовой деятельности. XXI век: итоги прошлого и проблемы настоящего плюс, № 4(44), 276-281.

21. Бурлов В.Г., Андреев А.В., Гомазов Ф.А. Управление безопасностью объекта техносферы на основе закона сохранения целостности объекта Технико-технологические проблемы сервиса. 2018. № 1 (43). С. 56–60.

22. Бурлов В. Г., Гробицкий А.М., Гробицкая А.М. (2016). Управление строительным производством с учетом показателя успешного выполнения производственного задания Инженерно-Строительный журнал № 3. С. 77–91. doi: 10.5862/MCE.63.5.

Сушкин Н. А.
ИКТИБ ЮФУ, аспирант, техник
sushkin@sfedu.ru

ТЕХНОЛОГИЯ ОБНАРУЖЕНИЯ ВРЕДОНОСНОГО ВОЗДЕЙСТВИЯ НА СИСТЕМУ НАВИГАЦИИ И СВЯЗИ БПЛА

Аннотация проекта:

В последнее время заметно увеличилось число инцидентов, связанных с беспилотными летательными аппаратами (БПЛА), что акцентирует внимание на неотложной необходимости повышения уровня их защищенности. Диссертационная работа направлена на решение этой актуальной проблемы через разработку метода для обнаружения вредоносного воздействия на систему навигации и связи БПЛА.

С учетом большого количества разнородных моделей БПЛА на рынке возникает острая необходимость унификации подходов к сбору и анализу данных для обеспечения эффективного обнаружения атак. Предложена новая модель построения вектора атаки на систему. Данная модель на основе онтологического подхода отражает связь между кибер-физическими параметрами БПЛА, атакующим воздействием и последствием. Модель позволила выявить уникальные наборы групп параметров, которые связаны с конкретными атаками и другими типами деструктивного воздействия. Таким образом, можно выявить группы параметров и оценить степень воздействия на них со стороны. Это позволяет идентифицировать аномалии и предотвратить возможные атаки на ранней стадии.

Разработанный алгоритм представляет собой универсальный инструмент, который способен анализировать большой объем разнородных данных в реальном времени, выделяя аномальные паттерны поведения системы и тем самым значительно снижая риски воздействия вредоносных факторов.

Экспериментальная часть демонстрирует эффективность предложенного подхода на практике, подтверждая его высокую работоспособность в условиях различных моделей эксплуатации БПЛА.

В заключении подчеркивается теоретическая и практическая ценность работы, которая может стать фундаментом для дальнейшего развития технологий в сфере безопасности киберфизических систем и обеспечения защиты от кибератак, внеся весомый вклад в повышение уровня безопасности эксплуатации БПЛА в условиях увеличивающегося числа инцидентов

Ключевые слова: безопасность, атака, навигационная система, беспилотный летательный аппарат, угроза, вероятность, глобальная навигационная спутниковая система, технология защиты.

Научная задача

1. Разработка технологии обнаружения вредоносного воздействия на систему навигации и связи БПЛА.
2. Реализация программного обеспечения для полетного контроллера или платы управления БПЛА, которое позволит в автономном режиме обнаруживать атаку и уведомлять об этом оператора, либо соседние БПЛА.

3. Разработка метода автономного обнаружения вредоносного воздействия для БПЛА, основанного на анализе изменений кибер-физических параметров БПЛА.

4. Разработка методики категорирования и оценки типов вредоносного воздействия на БПЛА.

Предметом исследования являются математические модели, методы и алгоритмы обнаружения вредоносного воздействия на систему навигации и связи.

Методы исследования. Метод самотестирования БПЛА на основе принципа рефлексии, для определения состояния БПЛА и возможного инцидента информационной безопасности основывается на методах анализа больших данных, математической статистики и теории информации. Методы натурного моделирования использовались для создания БПЛА и его тестирования. Методы теории вероятней и теории информации были использованы для разработки метода детектирования аномалий.

Теоретическая ценность диссертационной работы заключается в системном анализе и классификации существующих угроз и методов атак на системы навигации и связи БПЛА, построения новой модели кибератак на БПЛА на основе онтологического подхода. В процессе исследования будет предложен новый метод для анализа и обнаружения аномалий, основанный на принципах теории информационной энтропии и дивергенции Кульбака-Лейблера. Работа способствует расширению теоретических знаний в области безопасности киберфизических систем и может стать основой для дальнейших научных исследований в данной области.

Практическая ценность работы определяется возможностью создания эффективного инструмента для обнаружения и предотвращения вредоносного воздействия на системы навигации и связи БПЛА, что значительно повысит уровень безопасности их эксплуатации. Разработанный алгоритм внедрен в существующие системы управления БПЛА для автоматического обнаружения аномалий и предотвращения возможных атак в реальном времени. Кроме того, данная технология может найти применение не только в области БПЛА, но и в других кибер-физических системах, требующих повышенного уровня защиты от вредоносных воздействий.

Научная новизна исследования:

1. Новый метод автономного обнаружения деструктивного воздействия, основанного на анализе изменений киберфизических параметров БПЛА, который позволяет БПЛА автономно оценивать наличие изменений в его подсистемах, и выявлять признаки кибератаки. Представленный метод позволяет обеспечить энергетическую эффективность, низкую задержку при обнаружении, а также простоту развертывания и возможность масштабирования за счет унификации и нормализации наборов параметров, а также применения методов на основе теории информации.

2. Технология обнаружения деструктивного воздействия на систему навигации и связи БПЛА, обеспечивающая классификацию типа вредоносного воздействия в автономном режиме. Преимущества данной технологии заключаются в том, что как правило, большинство исследований в данной области направлено только на определение типа атаки, при этом, за счет того, что БПЛА находится вне контролируемой зоны, на него может быть оказано деструктивное воздействие не только со стороны злоумышленника, но и со стороны окружающей среды, либо людьми не злонамеренно.

3. Модель деструктивного воздействия на систему навигации и связи БПЛА. На сегодняшний день, ученые при оценке собственных методов обнаружения атак зачастую

пользуются системами моделирования. При этом каждый исследователь использует собственные параметры симуляции атаки. Разработана модель атаки на основе анализа реальных экспериментальных данных, формализовано представление атаки и других типов вредоносного воздействия на БПЛА, а также создана база вредоносных воздействий на БПЛА. Впервые представлены и систематизированы знания о воздействии техногенного и природного характера, а также определена степень влияния различных типов воздействия на БПЛА.

Основные положения, выносимые на защиту:

1. Технология обнаружения активных атак на систему навигации и связи БПЛА, реализованная в виде программного обеспечения для полетного контроллера и платы управления БПЛА. Технология позволяет БПЛА в автономном режиме обнаруживать атаку и уведомлять об этом оператора, либо соседние БПЛА.

2. Метод автономного обнаружения деструктивного воздействия для БПЛА, основанный на анализе изменений кибер-физических параметров БПЛА, который внедрен в технологию обнаружения вредоносного воздействия на систему навигации и связи БПЛА.

3. Методика оценки качества обнаружения вредоносного воздействия на БПЛА, включающая базу данных наборов параметров БПЛА для сценариев воздействия для оценки качества обнаружения.

4. Модель деструктивного воздействия на БПЛА со стороны злоумышленника и со стороны факторов окружающей среды, на основе оценки состояния подсистем БПЛА, а также изменений кибер-физические параметров.

Использование результатов. Материалы данной диссертационной работы были использованы в следующих грантах и НИР:

1. Грант РНФ 22-11-00184 Технология обеспечения кибербезопасности от деструктивного воздействия на объекты критической информационной инфраструктуры;

2. НИР «Исследования по созданию интеллектуальных систем группового управления для БПЛА ближнего действия и малой дальности» («Защитник-19». (Министерство обороны РФ)).

3. Грант Информационной Безопасности МТУСИ 2022

Степень достоверности полученных результатов подтверждается разработкой действующих алгоритмов и программной реализацией средств обнаружения и идентификации, результатами экспериментов.

Краткое содержание диссертации:

В последние годы мир стал свидетелем значительного роста применения беспилотных летательных аппаратов (БПЛА) в различных сферах: от мониторинга и обследования территорий до выполнения специализированных задач в области безопасности. Однако с ростом популярности БПЛА увеличивается и риск вредоносных воздействий на системы навигации и связи этих аппаратов. Перед научным сообществом и индустрией стоит задача создания надежных методов обнаружения и предотвращения таких атак.

В рамках настоящей диссертационной работы предлагается разработка технологии обнаружения вредоносного воздействия на систему навигации и связи БПЛА, опирающейся на детальный анализ изменений энтропии в динамике киберфизических параметров системы. Предполагается, что подобный подход позволит создать универсальный инструмент для мониторинга состояния системы на основе анализа энтропийных характеристик, варьирующихся в зависимости от воздействия внешних факторов на систему.

Основной целью исследования является создание методологических и технологических основ для создания системы обнаружения вредоносных воздействий, обладающей высокой степенью надежности и способной функционировать в условиях различных внешних воздействий. Для достижения поставленной разработан алгоритм, опирающийся на теоретически обоснованные методы анализа изменений энтропии системы.

Работа метода основывается на детализированном анализе временных рядов киберфизических параметров системы навигации и связи БПЛА с использованием понятия информационной энтропии и дивергенции Кульбака-Лейблера.

На первом этапе производится сбор и нормализация входных данных. Следует отметить, что корректная нормализация данных является критически важной для обеспечения точности последующего анализа.

Далее, после обработки исходных данных, происходит расчет энтропии каждого киберфизического параметра. Энтропия тут служит мерой неопределенности и помогает выявлять необычные изменения в динамике системы. Следующим этапом является анализ полученных значений энтропии с применением дивергенции Кульбака-Лейблера, что позволяет оценить расхождение между текущим и нормальным (или базовым) распределениями вероятностей. Величина дивергенции служит индикатором аномалий, позволяя оперативно обнаруживать возможные угрозы.

Важным моментом в работе алгоритма является динамическая установка пороговых значений для обнаружения аномалий, что позволяет адаптироваться к изменяющимся условиям эксплуатации и различным моделям БПЛА. По результатам анализа строится конечный вывод об аномалии, основываясь на котором, система может предпринять ряд действий по обеспечению безопасности, включая переход в режим автономной работы или активацию других защитных механизмов.

В ходе исследования был проведен ряд экспериментов, направленных на верификацию разработанного алгоритма обнаружения вредоносных воздействий на системы навигации и связи БПЛА. Исследование предусматривало создание симуляционной среды, в которой имитировались различные сценарии атак на указанные системы.

Первым этапом экспериментальной работы стало сбор и нормализация данных. Исходные данные представляли собой набор киберфизических параметров системы, включая показания датчиков и информацию о состоянии различных подсистем БПЛА. Эти данные были нормализованы с использованием различных математических методов, включая преобразования для обеспечения однородности масштабов и распределений параметров.

После этого, было проведено вычисление энтропии системы с использованием дивергенции Кульбака-Лейблера. Этот метод позволяет оценить степень отклонения текущего распределения параметров от некоторого базового, или «нормального», состояния, исходя из статистических характеристик каждого параметра.

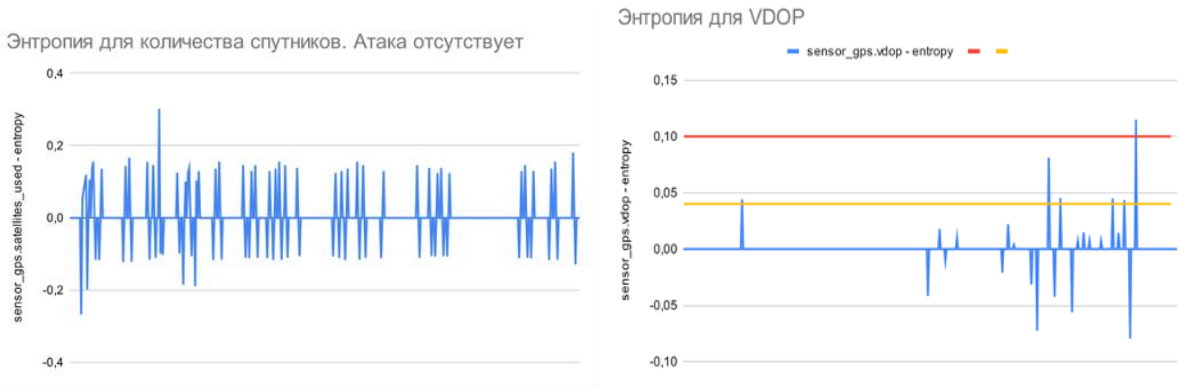
Следующим шагом была визуализация результатов, что облегчило интерпретацию полученных данных. Графическое представление демонстрировало динамику изменения энтропии во времени, что позволяло увидеть моменты превышения пороговых значений энтропии, что свидетельствовало о возможных аномалиях или атаках.

Результаты тестовых испытаний, которые проводились в полевых условиях представлены в таблице 1. Всего было проведено более 150 полетов, во время которых наблюдались различные погодные условия, а также проводились атаки на БПЛА.

Таблица 1 – Суммарные результаты полётных испытаний.

Воздействие	Средняя вероятность обнаружения	Среднее время обнаружения
1 Подмена навигационного сигнала	98%	0.25 сек.
2 Глушение сигнала	100%	0.38 сек.
3 Погодная аномалия (сильный ветер)	95%	0.25 сек.
4 Погодная аномалия (облачность)	95%	0.5сек.
5 Атака наводнения пакетами	94% сек.	0.5 сек.

Результаты эксперимента подтвердили теоретические предположения о работоспособности предложенного метода. На графиках (рис. 1) явно прослеживались моменты, в которых значения энтропии выходили за установленные пороговые значения, указывая на аномальные изменения в системе и потенциально вредоносные воздействия.



а) б)

Рис. 1. Изменение значения энтропии без атаки (а) и с атакой (б).

Таким образом, экспериментальная часть исследования показала эффективность применения методов анализа энтропии для обнаружения аномалий в системах навигации и связи БПЛА. Результаты экспериментов дали основание считать, что предложенный метод может стать основой для создания надёжных систем обеспечения безопасности БПЛА.

Итак, предложенный метод позволяет не только эффективно обнаруживать попытки вредоносного воздействия на систему навигации и связи БПЛА, но и своевременно реагировать на них, обеспечивая тем самым высокий уровень защиты. Этот подход обладает значительным потенциалом для интеграции в существующие системы безопасности, обеспечивая надежную и устойчивую эксплуатацию беспилотных аппаратов в сложных и динамично изменяющихся условиях современного мира.

Заключение

Поскольку метод позволяет анализировать любые параметры и может работать с любыми доступными данными, то не имеет значения, какими датчиками оснащен БПЛА. С помощью разработанного метода можно не только обнаруживать аномалии, но и определять

изменение закономерностей поведения БПЛА, изменение его состояний. Если значения определяемой энтропии не слишком высоки, и имеет место однократное увеличение, то это может указывать на изменение режима полета. Соотношение анализируемых параметров позволяет выявить атаку и определить ее тип. Каждая атака затрагивает определенный набор подсистем, поэтому тип атаки можно охарактеризовать по результирующим параметрам, на которые она влияет. Данные, собранные в виде временных рядов, могут быть использованы для обучения нейронных сетей принимать решения о проведении атаки. Метод может использоваться для анализа других наборов параметров и применяться не только к БПЛА, но и к любой кибер-физической системе.

Список литературы:

1. J. Warner and R. Johnston, "A simple demonstration that the global positioning system (gps) is vulnerable to spoofing", In: Journal of Security Administration, 2003
2. E. T. Lester, "Military position source challenges for worldwide ads-b out compliance", In: Integrated Communications Navigation and Surveillance Conference, 2013.
3. Clifton A. Ericson, Software safety in a nutshell.
4. "Global positioning system directorate", In: Systems engineering and integration Interface Specification IS-GPS-200G Technical Report, 2012.
5. E. P. Blasch, J. J. Salerno and G. P. Tadda, "Measuring the worthiness of situation assessment", Proceedings of the 2011 IEEE National Aerospace and Electronics Conference (NAECON), pp. 87-94, 2011.
6. Y. M. Zhang, "Fault Detection and Diagnosis for NASA GTMUAV with Dual Unscented Kalman Filter", Handbook of Unmanned Aerial Vehicles, pp.1157-1181, 2015.
7. Z. Birnbaum, A. Dolgikh, V. Skormin, E. O'Brien, D. Muller and C. Stracquodaine, "Unmanned Aerial Vehicle Security Using Recursive Parameter Estimation", Journal of Intelligent & Robotic Systems, vol. 84, pp.107-120, 2016.
8. J. Pang, D. Liu, H. Liao, Y. Peng and X. Peng, "Anomaly detection based on data stream monitoring and prediction with improved Gaussian process regression algorithm",2014 International Conference on Prognostics and Health Management, pp. 1-7, 2014
9. Y. Qiao, Y. Zhang and X. Du, "A Vision-Based GPS-Spoofing Detection Method for Small UAVs," 2017 13th International Conference on Computational Intelligence and Security (CIS), Hong Kong, 2017, pp. 312-316, doi: 10.1109/CIS.2017.00074.

Фадеев И.И.
Санкт-Петербургский государственный университет телекоммуникаций
им. проф. М.А.Бонч-Бруевича, старший преподаватель кафедры
fadeev.collapse@yandex.ru

АНАЛИЗ ПОДХОДОВ К МОДЕЛИРОВАНИЮ АКТУАЛЬНЫХ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

Аннотация: В ходе анализа подходов к моделированию актуальных угроз необходимо определить научные подходы к разработке базовой модели угроз, методик оценки рисков и анализа масштабов возможных последствий, а также методики принятия решений при задании и разработке требований к подсистеме безопасности объектов критической информационной инфраструктуры, функционирующих в области оборонной промышленности. Итоговым результатом работы будет являться методика оценки эффективности принятых организационных и технических мер объекта КИИ, функционирующего в области оборонной промышленности.

Ключевые слова: критическая информационная инфраструктура, оборонная промышленность, угрозы информационной безопасности, деструктивные воздействия, целевые компьютерные атаки, модель нарушителя информационной безопасности, модель угроз, компьютерные инциденты, подсистема безопасности.

Введение. В XXI веке окружающая среда с каждым днем все стремительней развивается и меняется благодаря новым информационным технологиям и интернету [1].

В период с 2005 по 2008 год ФСТЭК России, были разработаны и утверждены методические документы по обеспечению безопасности информации в ключевых системах информационной инфраструктуры Российской Федерации.

В связи с применением вновь утвержденной Методики оценки угроз безопасности информации [2] Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных и Методика определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры более не применяются. При этом Базовые модели угроз безопасности информации могут применяться для моделирования угроз безопасности информации на значимых объектах критической информационной инфраструктуры Российской Федерации до утверждения ФСТЭК России соответствующих методических документов [3].

При этом действующие методики предполагают анализ всех угроз безопасности информации, а уточняющие методические документы, такие как Типовые модели угроз безопасности информации для конкретных видов объектов КИИ или Базовые модели угроз безопасности объекта КИИ в конкретных сферах деятельности субъектов КИИ частично находятся в стадии разработки.

Актуальность темы исследования. Развитие подходов в области обеспечения безопасности критической информационной инфраструктуры, развитие требований, предъявляемых к их защите, выделение отдельных понятий в информационной безопасности таких систем и практика применения изданных ранее нормативных и методических

документов обусловлены различными направлениями информатизации и развитием информационных технологий. Цифровая трансформация затрагивает всё больше повседневных процессов, затрагивающих экономику, потенциал и безопасность государства, а также здоровье и безопасность граждан, в том числе за счет экологической и социальной безопасности. При этом, защита от угроз, обусловленных техногенными источниками, регулируется различными отраслями ещё с конца XX века.

В настоящее время особое внимание уделяется антропогенным источникам угроз: с развитием информационных (автоматизированных) систем и сетей компьютерные инциденты и возможные последствия их возникновения должны быть рассмотрены как результаты целевых компьютерных атак, с учетом подготовки потенциальных нарушителей к реализации сценариев, использующих все последовательности возможных тактик и соответствующих им техник.

Одним из проблемных вопросов, возникающим при моделировании угроз является определение актуальности применяемых нормативных и методических документов в области защиты информации. Многогранность подходов к обеспечению безопасности существующих и создаваемых объектов критической информационной инфраструктуры обусловлена широкой сферой использования информационных (автоматизированных) систем и сетей и разнообразием их типов.

Так, в соответствии с законодательством Российской Федерации [4] определено 13 сфер и областей функционирования объектов критической информационной инфраструктуры. В зависимости от критических процессов субъекта, реализуемых в информационных (автоматизированных) системах и сетях, а также типов таких систем могут быть определены базовые подходы к их категорированию и моделированию актуальных угроз, путём экспертной оценки и статистических данных.

Степень разработанности темы. Изученные научные подходы и практические решения в области информационной безопасности объектов критической информационной инфраструктуры зачастую связаны с автоматизированными решениями. Созданию интеллектуальных сервисов защиты информации в критических инфраструктурах посвящены работы таких ученых, как Д.П. Зегжда, И.В. Котенко, И.Б. Саенко, С.А. Петренко, А.Е. Кучерявый, А.И. Толстой. Также в научных исследованиях отражены подходы к анализу и оценке рисков в области информационной безопасности, в том числе с использованием нейро-нечёткой модели, данные исследования включены в работы С.А. Агеева [5], И.М. Ажмухамедова [6,7], И.В. Аникина [8,9], Е.К. Барановой [10,11], Т.И. Булдаковой [12], Н.Г. Милославской [13] и других.

Проведенный анализ работ по научной деятельности в области информационной безопасности показал, что научно-техническая задача оценки рисков и прогнозирования угроз информационной безопасности не охватывает область оборонно-промышленного комплекса (ОПК). В частности не рассмотрена специфика предприятий и организаций, работающих в сфере ОПК и объектов критической информационной инфраструктуры, принадлежащих им. Существующие методики не охватывают информационных систем реальных производств в указанной сфере, новые информационные угрозы и сопутствующие им риски и возможные негативные сценарии.

Цели и задачи работы. Цели исследования заключаются в повышении защищенности объектов критической информационной инфраструктуры (КИИ) и состоят из следующих задач: анализ текущего состояния защищенности объектов КИИ, разработка варианта базовой

модели угроз и типовой модели нарушителя объекта КИИ, функционирующего в области оборонной промышленности; разработка методики оценки рисков и анализа масштабов возможных последствий; разработка методики принятия решений при задании и разработке требований к системе защиты информации. Все задачи взаимосвязаны и результаты их выполнения позволят выработать рекомендации по принятию решений о целесообразности внесения изменений в существующие объекты КИИ, на предпроектной стадии или на стадии определения перечня объектов КИИ, подлежащих категорированию.

Научная новизна. Впервые проведен анализ подсистем безопасности объектов КИИ, функционирующих в области оборонной промышленности, обобщены достоверные сведения в масштабе федерального округа.

Теоретическая и практическая значимость работы. В ходе анализа современного состояния исследований в данной области было выявлено, что существующие методические подходы зачастую находятся в стадии разработки и требуют апробации. Отсутствие широкой правоприменительной практики, в том числе полноценных (в рамках охвата большого количества объектов) результатов государственного надзора (контроля) за обеспечением безопасности значимых объектов критической информационной инфраструктуры позволяет формировать новые подходы и оценивать применимость различных методов в ходе проведения научных исследований.

Разрабатываемые базовые модели угроз, которые будут содержать описание типовых объектов критической информационной инфраструктуры, номенклатуру и общее описание угроз безопасности и рекомендации по их нейтрализации (парированию), регулятором также планируется разработать Методики оценки показателей критериев значимости и Типовые модели угроз.

В Методиках оценки показателей критериев значимости помимо непосредственного описания (алгоритма) оценки показателей будут доступны основные логические и (или) расчетные соотношения, необходимые для оценки возможных ущербов, возникающих вследствие реализации компьютерных атак и нарушения функционирования объектов критической информационной инфраструктуры, а также соотношения, необходимые для определения показателей критериев значимости. Таким образом, среди подходов по категорированию необходимо выделить особенности сферы (области) функционирования объектов критической информационной инфраструктуры, принадлежащим субъектам и сфер деятельности субъектов в целом с привязкой к возможным негативным последствиям в данных сферах и непосредственно применимым показателям критериев значимости. Основой для осуществления моделирования будут являться в первую очередь анализ критических процессов, реализуемых в конкретной сфере (области) деятельности субъекта критической информационной инфраструктуры. На основании экспертной оценки и статистических данных для каждой сферы возможна разработка примерных базовых моделей угроз с учетом определения обобщенных групп возможных нарушителей и основных негативных последствий актуальных для определенной сферы деятельности.

Методы исследования базируются на положениях теории системного анализа, математического моделирования, теории вероятности и методологии теории рисков.

В рамках проводимого исследования проанализированы результаты мониторинга сведений о публикуемых критических уязвимостях программного обеспечения государственных информационных систем и объектов критической информационной инфраструктуры, а также связанных с ними компьютерных атаках. На основании сведений,

полученных из общедоступных источников информации в период с 28 февраля 2022 г. по настоящее время оценено влияние целевых компьютерных атак на состояние защищенности критической информационной инфраструктуры Российской Федерации.

По результатам анализа проведенного в рамках взаимодействия с организациями, функционирующими в области разработки и внедрения средств защиты информации, и информации Национального координационного центра по компьютерным инцидентам, установлено, что в указанный период:

повысилась интенсивность рутинного опроса внешних интерфейсов информационных систем и сетей;

основные компьютерные инциденты были вызваны использованием «открытых» инструментов, распространяемых в общедоступных источниках информации;

инциденты, повлекшие масштабные негативные последствия зачастую были реализованы за счет возможностей внутренних нарушителей или связаны со слабой парольной защитой.

Учитывая, что потенциал и мотивация нарушителей теперь не являются определяющими факторами в условиях открытого распространения и простоты использования инструментов для реализации атак, для разработки базовой модели угроз предлагается рассмотреть угрозы безопасности информации, реализуемые нарушителями, обладающими высокими возможностями по реализации угроз безопасности информации (Н4).

Таким образом, в случае отсутствия информации о времени и цели атаки на критическую информационную инфраструктуру, а также в условиях отсутствия масштабных негативных последствий возможно рассмотреть состояния объектов КИИ в рамках марковских процессов для решения задачи по разработке базовой модели угроз. Использование Методики [2], автором смоделировано функционирование объектов КИИ со следующими работоспособными состояниями (Табл. 1).

Табл. 1. Состояние объектов КИИ

Вариант состояния	**Описание состояния**
S0	нормальное состояние, в работе, без инцидентов
S1	нормальное состояние, отключен, без инцидентов
S2	нарушение конфиденциальности, в работе
S3	несанкционированный доступ к компонентам, защищаемой информации, системным, конфигурационным, иным служебным данным; в работе
S4	отказ в обслуживании компонентов (нарушение доступности), в работе
S5	нарушение целостности информации, в работе
S6	несанкционированное использование вычислительных ресурсов систем и сетей в интересах решения несвойственных им задач, в работе
S7	нарушение функционирования (работоспособности) отдельных программно-аппаратных средств обработки, передачи и хранения информации, в работе

Разработка варианта базовой модели угроз и типовой модели нарушителя ОКИИ для организаций ОПК необходима по причине отсутствия методических документов, предлагаемых (рекомендуемых) к применению при моделировании актуальных угроз безопасности информации. Также разработанная модель систематизирует виды и категории

актуальных нарушителей и последовательности тактик и техник, применение которых может привести к реализации угрозы безопасности информации.

Типовые модели угроз предполагают описание архитектуры систем (совокупность основных структурно-функциональных характеристик, свойств, компонентов систем и сетей, воплощенных в информационных ресурсах и компонентах, правилах их взаимодействия, режимах обработки информации), являющихся объектами критической информационной инфраструктуры, и их описание как объектов защиты от компьютерных атак. На основании типовой архитектуры описываются потенциальные уязвимости систем (с учетом основного программного и программно-аппаратного обеспечения, используемого в данных системах), типовая модель нарушителя в системе, типовые способы (сценарии) реализации угроз и типовые компьютерные инциденты, происходящие в результате реализации угроз безопасности. Таким образом в развитие Базовых моделей угроз, определив типовые объекты критической информационной инфраструктуры для каждой сферы, могут быть разработаны примерные Типовые модели угроз для актуальных типов информационных (автоматизированных) систем, где особенно важным будет являться определение интерфейсов объектов воздействия для конкретных видов систем.

Указанные подходы при формировании модели угроз и определения актуальных угроз безопасности информации также могут быть использованы до утверждения ФСТЭК России соответствующих методических документов.

Также в ходе оценки угроз безопасности информации для типовых объектов критической информационной инфраструктуры, актуальных для сферы деятельности субъекта должны быть определены возможные негативные последствия (социальные, политические, экономические, экологические, и последствия для обеспечения обороны страны, безопасности государства и правопорядка), которые могут наступить от реализации (возникновения) угроз безопасности информации [14]. При этом, решая задачу моделирования угроз необходимо помнить о взаимосвязи возможных негативных последствий с показателями критериев значимости.

Дополнительно возможно провести анализ источников угроз, определив общую характеристику нарушителей и (или) источники угроз для конкретных угроз безопасности информации. В рамках данного анализа рекомендуется определить взаимосвязь последствий реализации угрозы с видами воздействий (нарушение конфиденциальности, целостности, доступности), а также с целями и объектами защиты.

Таким образом исходя из актуальных возможных негативных последствий, актуальности источников угроз разрабатывается номенклатура угроз безопасности информации для конкретной сферы деятельности субъекта. На данном этапе при формировании Базовых моделей угроз из общего перечня угроз безопасности информации при наличии обоснования могут быть исключены угрозы невозможность реализации которых связана с отсутствием объектов воздействия (применяемых информационных технологий), отсутствием актуальных источников угроз и отсутствием актуальных негативных последствий (во взаимосвязи с показателями критериев значимости). Отдельные угрозы безопасности, реализация которых обусловлена эксплуатацией уязвимостей также могут быть исключены из общего перечня уязвимостей.

В соответствии с полученной номенклатурой угроз безопасности информации для объектов критической инфраструктуры, функционирующих в конкретных сферах деятельности должны быть выработаны рекомендации по их нейтрализации (парированию).

В зависимости от сферы деятельности субъекта в целом или объекта критической информационной инфраструктуры меры по защите могут определяться в соответствии с существующими требованиями в области защиты информации (например, при рассмотрении возможных категорий обрабатываемой информации), также могут применяться отдельные организационные и технические мероприятия, направленные на предотвращение определенных ранее актуальных негативных последствий. Должны быть разработаны отдельные рекомендации для парирования угроз, реализация которых обусловлена эксплуатацией уязвимостей.

Разработка Типовых моделей угроз сопряжена с анализом и классификацией существующих информационных (автоматизированных) систем и сетей. В соответствии с Методикой оценки угроз безопасности информации допускается разработка одной модели угроз безопасности информации для нескольких однотипных создаваемых систем и сетей обладателя информации или оператора. Типовые модели угроз предлагают конкретную классификацию объектов критической информационной инфраструктуры и направлены на их детальное описание как объектов защиты.

Первой задачей в разработке Типовой модели угроз является обобщенное описание архитектуры, свойственной описываемым системам. На основании типовой архитектуры должно быть выполнено логическое сегментирование компонентов систем и сетей с целью определения отдельных сегментов как объектов (интерфейсов) воздействия угроз безопасности информации.

Дополнительно для объектов (интерфейсов) воздействия могут быть определены типы программного (программно-аппаратного) обеспечения, применяемого для реализации критических процессов, могут быть рассмотрены конкретные продукты (продуктовые линейки).

На основании анализа типовой архитектуры оценивается наличие потенциальных угроз безопасности информации (и, при необходимости уязвимостей) в соответствии с используемыми информационными технологиями, возможными объектами воздействия. Дополнительно может быть определена критичность объектов воздействия с использованием описания векторов компьютерных атак, содержащиеся в базах данных и иных источниках, опубликованных в сети «Интернет» (CAPEC, ATT&CK, OWASP, STIX, WASC и др.) [2].

В развитие описываемой в Базовых моделях угроз общей характеристики модели нарушителя при разработке Типовой модели угроз определяются типовые нарушители, на основании возможностей которых должны быть определены способы реализации угроз безопасности информации. Обладая уточненной информацией о типовых архитектурах и объектах воздействия, полученных в ходе разработки модели угроз, данные способы должны учитывать сценарии реализации угроз с применением соответствующих основных тактик и типовых техник, основывающихся на применении свойственных типовому объекту информационных технологий и программных (программно-аппаратных) средств.

При этом, угроза безопасности информации является актуальной, только в том случае, если имеется сценарий реализации угрозы: имеется источник угрозы (нарушитель), имеются объекты и интерфейсы воздействия, а способы реализации угрозы безопасности информации и непосредственно реализация угрозы может привести к негативным последствиям [2]. Таким образом, описав типовые объекты воздействия, типовых нарушителей и способы реализации угроз следующим шагом в разработке Типовой модели угроз будет являться определение актуальных видов воздействий и возможных негативных последствий. В рамках данного шага

необходимо провести анализ в соответствии с новой Методикой, где помимо используемых в Банке данных угроз безопасности информации ФСТЭК России нарушений конфиденциальности, целостности и доступности актуальными также будут являться: несанкционированный доступ к компонентам, защищаемой информации, системным, конфигурационным, иным служебным данным; несанкционированное использование вычислительных ресурсов систем и сетей в интересах решения несвойственных им задач; нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передачи и хранения информации [2].

Положения, выносимые на защиту.

1. Разработка базовой модели угроз.

Проведен анализ подсистем безопасности ОКИИ, функционирующих в области оборонной промышленности, обобщены достоверные сведения в масштабе федерального округа, автором проведен анализ информационных систем более 40 значимых организаций оборонно-промышленного комплекса.

Научно-исследовательская работа позволила разработать базовую модель угроз объектов КИИ, функционирующих в области оборонной промышленности. В целях выполнения задач, решаемых в ходе оценки угроз, исходя из сферы деятельности субъекта были определены объекты критической информационной инфраструктуры, реализующие критические процессы. Разработанная базовая модель угроз объекта КИИ функционирующего в области оборонной промышленности (**пункт 3 паспорта специальности 2.3.6.**) **систематизирует** виды и категории актуальных нарушителей и последовательности тактик и техник, применение которых может привести к реализации угроз безопасности информации и **позволяет совершенствовать** процесс моделирования актуальных угроз безопасности информации в организациях ОПК, **выработать рекомендации по парированию** угроз безопасности и содержит информацию о мерах защиты информации, направленных на нейтрализацию угроз.

Достоверность результатов обеспечивается корректным применением общенаучных методов исследования, подтверждается апробацией полученных результатов на практике и хорошей корреляцией с известными исследованиями.

2. Разработка типовой модели угроз.

Автором также оценены и проанализированы статистические данные более 200 субъектов КИИ.

Анализ рисков нарушения информационной безопасности в информационных системах управления производством (**пункт 7 паспорта специальности 2.3.6.**) позволяет смоделировать актуальные угрозы безопасности для таких систем. Проведен обширный анализ подсистем безопасности объектов КИИ, являющихся информационными системами управления производством, обобщены достоверные сведения в масштабе федерального округа. **Определены и конкретизированы** применительно к особенностям деятельности организаций ОПК типовые компьютерные инциденты, их **взаимосвязь** с объектами и интерфейсами воздействия. Разработанная типовая модель ОКИИ, **позволит определить** границу оценки угроз безопасности информации и необходимые исходные данные, используемые в ходе выявления критических процессов организаций ОПК и объектов, подлежащих категорированию.

Достоверность результатов обеспечивается надежными исходными данными и подтверждается внедрением полученных результатов в практику организаций оборонно-промышленного комплекса.

3. Разработка методики оценки эффективности.

Итоговым результатом работы будет являться методика оценки эффективности принятых организационных и технических мер объекта КИИ, функционирующего в области оборонной промышленности (пункт 10 паспорта специальности **2.3.6.**) в которой**, в отличие от известных методик** конкретизированы критерии оценки эффективности защиты применительно к области оборонной промышленности. Дополнительно автором разработан метод принятия решений при задании и установлении требований к подсистемам защиты информации ОКИИ (**пункт 15 паспорта специальности 2.3.6.**).

Разработка метода принятия решений при задании и установлении требований к системе защиты информации в зависимости от типов систем и сетей **в отличие от известных**, учитывает требования к обеспечению безопасности различных систем и сетей, дополняет существующие базовые модели угроз Метод **основан на совершенствовании проведения экспертных оценок** за счёт определения весовых коэффициентов. устанавливает зависимость объектов и видов воздействия от негативных последствий, которые могут наступить от реализации (возникновения) угроз безопасности информации.

Апробация результатов будет осуществлена не позднее ноября текущего года в рамках работы Координационного совета по проблемам противодействия иностранным техническим разведкам в организациях ОПК Северо-Западного федерального округа (более 20 предприятий ОПК).

Защита диссертации пройдет в рамках диссертационного совета по защите диссертаций, как на соискание ученой степени кандидата наук, так и на соискание ученой степени доктора наук 99.2.038.03, созданного на базе университетов: "Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича (СПбГУТ)", "Санкт-Петербургский государственный университет аэрокосмического приборостроения (ГУАП)" и "Балтийский государственный технический университет «ВОЕНМЕХ» им. Д.Ф. Устинова".

Заключение.

В работе использованы результаты, в которых автору принадлежит определяющая роль. Часть опубликованных (публикуемых) работ и написана в соавторстве с сотрудниками СПбГУТ и Управления ФСТЭК России по Северо-Западному федеральному округу. В настоящее время полученные научные результаты проходят экспертизу в целях возможности открытого опубликования в рецензируемых изданиях из перечня ВАК при Минобрнауки России (3 публикации). В соответствии с планом выполнения проекта подготовлены материалы регистрации программы для ЭВМ (2 программы). Представление диссертации на НТС СПбГУТ спланировано на ноябрь 2023 г.

СПИСОК ЛИТЕРАТУРЫ

1. Организация концептуальной модели критической информационной инфраструктуры / А. М. Гельфанд, Н. Н. Лансере, А. А. Ложкина, И. И. Фадеев // Методы и технические средства обеспечения безопасности информации. – 2020. – № 29. – С. 39-40. – EDN PYPOHZ.

2. Методический документ «Методика оценки угроз безопасности информации» (утв. Федеральной службой по техническому и экспортному контролю 5 февраля 2021 г.);
3. Информационное сообщение ФСТЭК России «Об утверждении методики оценки угроз безопасности информации» от 15 февраля 2021 г. № 240/22/690.
4. Федеральный закон Российской Федерации от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».
5. Агеев, С.А. Оценка рисков сетевой компьютерной безопасности на основе нечеткого логического вывода / С.А. Агеев, И.Б. Саенко // ИБРР-2017: X Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России». – Санкт-Петербург: СПб.: СПОИСУ, 1-3 ноября, 2017. – Том 3. – С. 28–30.
6. Ажмухамедов, И.М. Управление рисками информационной безопасности в условиях неопределенности / И.М. Ажмухамедов, О.Н. Выборнова, Ю.М. Брумштейн // Проблемы информационной безопасности. Компьютерные системы. – 2016. – № 1. – С. 7–14.
7. Ажмухамедов, И.М. Анализ рисков информационной безопасности / И.М. Ажмухамедов, О.Н. Выборнова, О.М. Князева: Учебное пособие. – Астрахань: Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Астраханский государственный технический университет», 2015. – 104 с.
8. Аникин, И.В. Обеспечение информационной безопасности корпоративных информационных сетей через оценку и управление рисками / И.В. Аникин, Л.Ю. Емалетдинова, А.П. Кирпичников // Вестник технологического университета. – 2015. – Том 18, № 7. – С. 247–250.
9. Аникин, И.В. Метод управления рисками информационной безопасности в корпоративных информационных сетях / И.В. Аникин // Инфокоммуникационные технологии. – 2015. – Том 13, № 2. – С. 215–221.
10. Баранова, Е.К. Методики анализа и оценки рисков информационной безопасности / Е.К. Баранова // Образовательные ресурсы и технологии. – 2015. – № 1(9). – С. 73–79.
11. Баранова, Е.К. Процедура применения методологии анализа рисков OCTAVE в соответствии со стандартами серии ИСО/МЭК 27000-27005 / Е.К. Баранова, А.С. Забродоцкий // Образовательные ресурсы и технологии. – 2015. – № 3(11). – С. 73–80.
12. Булдакова, Т.И. Оценка информационных рисков в автоматизированных системах с помощью нейро-нечёткой модели / Т.И. Булдакова, Д.А. Миков // Наука и образование: научное издание МГТУ им. Н.Э. Баумана. – 2013. – № 11. – С. 295–310.
13. Милославская, Н.Г. Управление рисками информационной безопасности / Н.Г. Милославская, М.Ю Сенаторов, А.И. Толстой: Учебное пособие для вузов. 2-е изд., испр. – М.: Горячая линия-Телеком, 2014. – 130 с.
14. Постановление Правительства РФ от 8 февраля 2018 г. № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений».

Фельдман Е.В.
Челябинский государственный университет, старший преподаватель кафедры Компьютерной безопасности и прикладной алгебры
mila008.is@gmail.com

ПРОТИВОДЕЙСТВИЕ СОВЕРШЕНИЮ БЕСКОНТАКТНЫХ ПРЕСТУПЛЕНИЙ С ИСПОЛЬЗОВАНИЕМ ФИНАНСОВЫХ ОПЕРАЦИЙ

Аннотация: Цифровизация различных процессов создала площадку, позволяющую бесконтактно совершать общественно опасные деяния. Злоумышленники научились похищать информацию, обходить систему платежей налогов, создавать серые схемы расчетов, в том числе с использованием криптовалют. Отдельной проблемой специалисты выделяют тему узаконивания денег, добытых запрещенным путем, средства полученные при мошенничестве, наркоторговле, торговле людьми и так далее. Для восполнения экономической и информационной стабильности и безопасности в приоритете является разработка и внедрение новых информационных и финансовых технологий и специальные автоматизированные системы. Автоматизированная система контроля с (Anti-Money Laundering system, AML-системы) в настоящее время стала одним из главных подходов в борьбе с совершением бесконтактных преступлений с использованием цифровых технологий. Существующие методы искусственного интеллекта разработаны недостаточно для борьбы с бесконтактными преступлениями при использовании финансовых операций, также не существует универсальных систем анализа транзакций. Разработка методов борьбы с бесконтактными преступлениями при использовании финансовых операций в настоящее время актуальна. Цель работы – разработать организационные и технические способы противодействия, а также модели обнаружения аномальных банковских транзакций, применяемых при процессе отмывания денег и нелегальном обороте товаров и услуг.

Ключевые слова: компьютерная безопасность, машинное обучение, распознавание образов, нейронные сети, классификация, выявление аномальных транзакций, банковские транзакции.

На сегодняшний день отмечается рост преступности, совершаемой с использованием компьютерных технологий, в том числе включающей в себя бесконтактные преступления, а также бесконтактные финансовые операции. Существующие методы расследований таких преступлений, а также ограничения законодательной базы не позволяют в полной мере бороться с преступлениями, совершаемыми бесконтактными способами.

В рамках данной статьи рассматриваются два ключевых вектора противодействия бесконтактным преступлениям, а также два направления расследований таких преступлений. В качестве направлений расследований рассматриваются сетевой вектор и финансовый. А в качестве противодействия, рассматривается использование методов искусственного интеллекта в предиктивном управлении финансовыми транзакциями.

Существующие методы искусственного интеллекта разработаны недостаточно, что не позволяет обрабатывать поток операций, проходящих онлайн. Отметим, что во время интеллектуального анализа существующих решений транзакции фильтруются в соответствии с разработанными правилами и заданными ограничениями. Все отфильтрованные транзакции считаются «законными» и не проходят процедуру анализа, который может быть использован

в незаконных целях. Существующие решения учитывают только показатели, связанные непосредственно с операцией или ее участниками, и не учитывают косвенные показатели. В результате возникают ложные ошибки и срабатывания. Таким образом, важными проблемами в области автоматизации противодействия легализации (отмыванию) денег, полученных незаконным путем, и поддержке терроризма являются [1]: невозможность автоматизировать в режиме онлайн те факторы и признаки, которые уникальны для конкретных видов финансовой деятельности или финансовых агентств; отсутствие централизованного инструмента для анализа транзакций; обязательность в использовании сочетания программного обеспечения и ручного анализа; большое количество неверных срабатываний и ошибок; существенные затраты на содержание команды аналитиков для ручного анализа транзакций.

В настоящее время стоит вопрос о разработке и развитии системы, которая будет фиксировать подозрительные транзакции. С ее помощью можно облегчить и ускорить процесс обработки данных, снизить риски, хранить информацию и данные о злоумышленниках, рассчитать их скоринг, далее это помогает отслеживать пользователей, которые могут заниматься отмывкой денег. Но из-за высокой стоимости таких систем только позволить себе их могут только крупные финансовые организации [2].

Высокую надежность информации обусловлено решениями, поддерживающими искусственный интеллект. Они автоматизируют весомую часть операций и обеспечивают надежность информации за счет расширенных возможностей анализа структурированных и неструктурированных данных. Современные системы научились выполнять следующие операции [1]: исследование и анализ активности клиентов; мониторинг коммуникаций, анализ писем по ключевым словам; многоязычный мониторинг, по сравнению с существующими инструментами решения искусственного интеллекта предлагает лучший вариант для перевода или транслитерации имен клиентов, кодовых слов и других данных на языках и скриптах, отличных от тех, которые используются в языках с латинскими корнями; мониторинг списков наблюдения, длинные отраслевые списки, включающие имена на нелатинских языках. Это затрудняет постоянный анализ существующих инструментов.

Борьба с отмыванием денег важна для обеспечения безопасности финансовых систем, а также для обнаружения незаконного оборота услуг и товаров. Создание виртуальных денег (криптовалюты), казалось бы, вызвало в обществе противоречие: скрываться от правоохранительных органов и действия закона злоумышленникам помогает анонимность, но доступная операция базы криптовалют дает возможность вести криминалистическое исследование, либо аналитику денежных операций. Важная функция AML аналитики – это отслеживание и фиксация подозрительных транзакций. Анализ транзакции, проведенный вручную, может показывать ошибочные данные. В сравнении с ним прогресс в настоящее время стоит за автоматическим анализом криптографических транзакций [3,4,5,6,7,8].

Также следует отметить, что борьба с бесконтактным совершением преступлений при использовании цифровых технологий представляет собой сложный механизм, требующий детального и длительного документирования фактов преступления, значительного количества привлекаемых технических средств, организации тесного взаимодействия с сотрудниками оперативно- поисковых и оперативно-технических подразделений. А успешное противодействие совершению бесконтактных преступлений возможно в тех случаях, в которых будет применяться аналитическая система, позволяющая проводить оперативно-розыскные мероприятия с применением цифровых технологий, машинного обучения и технологии Больших данных.

Одной из проблем предметной области является незрелость законодательных актов и руководящих документов. Уголовное законодательство не успевает за высокотехнологичными и инновационными способами совершения преступлений и, как правило, не отражает всех особенностей преступных посягательств на электронные платежные системы и потребителей услуг кредитно-кассовых организаций. Поэтому правильный подход законодателя к формулированию норм об уголовной ответственности представляется более абстрактным, сочетающим общие нормы о преступлениях против собственности, связанных с использованием электронных систем, с формулировкой общих концепций, отражающих использование компьютерного оборудования и программного обеспечения для совершения таких действий.

В работе рассматривается модель для выявления аномальных транзакций биткоинов с использованием машинного обучения. Для обучения и оценки модели использовался набор данных Elliptic, состоящий из более чем 200 тысяч транзакций биткоинов: 4545 имеют класс «незаконные», 42019 имеют класс «законные» и 157205 имеют класс «неизвестные». Выполнена оценка предложенной модели на основе метрик: доля верных ответов, точность, полнота, F1 метрика и индекс сбалансированной точности. В предложенной модели выявления аномальных транзакций биткоинов использованы различные алгоритмы машинного обучения с подбором гиперпараметров, но надежность предложенной модели равная 0.9780 не приемлема для задачи эффективного детектирования аномальных транзакций. С помощью алгоритма ресэмплинга TomekLinks в условиях несбалансированности классов повышена надежность классификации аномальных транзакций биткоинов в сравнении с лучшим результатом на наборе данных Elliptic, равным 0.9780. В результате надежность предложенной модели выявления аномальных транзакций биткоинов на основе алгоритма градиентного бустинга XGBClassifier равняется 0.9921. Результаты эффективности предложенной модели выявления аномальных транзакций биткоинов на основе алгоритма градиентного бустинга XGBClassifier были подтверждены с помощью 10-кратной перекрестной проверки.

В работе рассматривается еще одна модель выявления аномальных банковских транзакций на основе машинного обучения. Для оценки и обучения модели используется набор данных CreditCardFraud. Он состоит из 284807 транзакций кредитных карт: 492 имеют класс «незаконные», 284315 — «законные». Оценка предложенной модели выполнена на основе таких метрик, как доля верных ответов, F1 метрика, полнота, точность и индекс сбалансированной точности. В предложенной модели выявления аномальных банковских транзакций были использованы различные алгоритмы машинного обучения с подбором гиперпараметров. В условиях несбалансированности классов с помощью алгоритма ресэмплинга TomekLinks повышена надежность классификации аномальных банковских транзакций в сравнении с лучшим результатом на наборе данных CreditCardFraud, равным 0.9780. В результате надежность предложенной модели обнаружениям аномальных банковских транзакций составляет 0.9999 на основе алгоритмов Tpot и RandomForest. Результаты эффективности предложенной модели выявления аномальных банковских транзакций биткоинов на основе алгоритмов Tpot и RandomForest подтверждены с помощью десятикратной перекрестной проверки.

Техническое сопровождение оперативных мероприятий и следственных действий является важным вопросом. Техническое сопровождение состоит из следующих этапов: обыски, выемки, наведение справок, получение компьютерной информации; правильное

написание запросов в организации; правильное назначение исследования, компьютерной экспертизы. При реализации по компьютерным преступлениям (и по тем преступлениям, которые совершаются с использованием компьютерных технологий) следователь и оперативные сотрудники должны не только обеспечивать соответствие мероприятия процессуальным нормам, но и обеспечивать соответствие электронных носителей или компьютерной информации на предмет наличия доказательной базы, а также целостности данной информации.

В работе был проведен комплексный анализ принципов и решений для борьбы с бесконтактным совершением преступлений при использовании цифровых технологий, были разработаны организационные и технические меры для борьбы с бесконтактным совершением преступлений при использовании цифровых технологий, а именно: разработаны организационные меры для борьбы с бесконтактным совершением преступлений при использовании цифровых технологий; Создана надежная модель для обнаружения аномальных транзакций биткоинов, которая будет применима в схемах отмывания денег и нелегальном обороте товаров и услуг; Выполнена оценка предложенной модели на основе таких метрик, как доля верных ответов, F1 метрика, полнота, точность и индекс сбалансированной точности; Проведен сравнительный анализ надежности предложенной модели обнаружения аномальных транзакций биткоинов, результаты которого показали, что наилучшим оказывается алгоритм градиентного бустинга XGBClassifier, точность составляет 0.9921. Результаты эффективности предложенной модели выявления аномальных транзакций биткоинов на основе алгоритма градиентного бустинга XGBClassifier были подтверждены с помощью 10-кратной перекрестной проверки; Создана надежная модель для обнаружения аномальных банковских транзакций, которая будет применима в схемах отмывания денег и нелегальном обороте товаров и услуг; Выполнена оценка предложенной модели на основе таких метрик, как доля верных ответов, F1 метрика, полнота, точность и индекс сбалансированной точности; Проведен сравнительный анализ надежности предложенной модели обнаружения аномальных банковских транзакций, результаты которого показали, что наилучшим оказывается алгоритм на основе Tpot и RandomForest, точность составляет 0.9999. Результаты эффективности предложенной модели выявления аномальных банковских транзакций биткоинов на основе алгоритмов Tpot и RandomForest подтверждены с помощью десятикратной перекрестной проверки.

Целью данной работы является научно обоснованная разработка организационного, технического, математического и алгоритмического обеспечения для борьбы с бесконтактными преступлениями при использовании финансовых операций, в частности для обнаружения аномальных транзакций, используемых в процессе отмывания денег и нелегальном обороте товаров и услуг.

Задачи научного исследования: анализ состояния предметной области и инструментов для борьбы с бесконтактными преступлениями при использовании финансовых операций; разработка организационных и технических мер для борьбы с бесконтактным совершением преступлений при использовании цифровых технологий; оценка возможности использования доступных наборов данных для разработки модели обнаружения аномальных банковских транзакций; разработка модели обнаружения аномальных банковских транзакций; сравнительный анализ точности разработанных моделей обнаружения аномальных банковских транзакций.

Новизна научного исследования состоит в решении следующих перспективных задач: проведение комплексного анализа принципов и решений для борьбы с бесконтактным совершением преступлений при использовании цифровых технологий, и разработка научно-обоснованной модели обнаружения аномальных банковских транзакций с помощью методов машинного обучения.

Перспективы дальнейшей разработки темы исследования заключаются в: разработке аналитической системы, позволяющая проводить оперативно-розыскные мероприятия с применением цифровых технологий, машинного обучения и технологии Больших данных; разработке автоматизированной системы, позволяющая проводить взаимодействие служб безопасности банков и компаний, организующих электронные платежные системы с Федеральной службой по финансовому мониторингу и ведомствами, специализирующимися на борьбе бесконтактными преступлениями; разработке автоматизированный системы с функцией детального и длительного документирования фактов преступления, организации тесного взаимодействия с сотрудниками оперативно-поисковых и оперативно- технических подразделений; разработке автоматизированной системы блокирования доступа к опасным сайтам, в полном их закрытии.

СПИСОК ЛИТЕРАТУРЫ

1. Khrestina M.P. Development of Algorithms for Searching, Analyzing and Detecting Fraudulent Activities in the Financial Sphere / Khrestina M.P., Dorofeev D.I., Kachurina P.A., Usubaliev T.R., Dobrotvorskiy A.S. // European Research Studies Journal. — 2017. —4B. — 484-498.
2. Анженко Т.А. Применение финансовых технологий для противодействия отмыванию денежных средств [Электронный ресурс]: Официальный сайт газеты «Экспертный союз». – Режим доступа: https://confes.fb.tusur.ru/sites/default/files/webform/Anzhenko T. Fintech.docx (дата обращения 09.07.21);
3. Weber M. Anti-Money Laundering in Bitcoin: Experimenting with Graph Convolutional Networks for Financial Forensics / Weber M., Domeniconi G., Chen J., Weidele D., Bellei C., Robinson T., Leiserson C. // Arxiv. — 2019.
4. Bistarelli S. A Suite of Tools for the Forensic Analysis of Bitcoin Transactions: Preliminary Report / Bistarelli S., Mercanti I., Santini F. // Euro-Par Workshops. — 2018.
5. Kedharewsari K. Integration of Big Data & Cloud Computing To Detect Black Money Rotation with Range – Aggregate Queries / Kedharewsari K., Anu M., Rajalakshmi V. // International Journal of Engineering and Technology. — 2016. — 8. — 768-773.
6. Maksutov A. Detection of Blockchain Transactions Used in Blockchain Mixer of Coin Join Type / Maksutov A., Alexeev M., Fedorova N., Andreev D. // 2019 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus) . — 2019. — 274-277.
7. Oakley J. Unmasking Criminal Enterprises: An Analysis of Bitcoin Transactions / Oakley J., Worley C., Yu L., Brooks R., Skjellum A.// 13th International Conference on Malicious and Unwanted Software (MALWARE) . — 2018.— 161-166.
8. Plaksiy K. Applying Big Data Technologies to Detect Cases of Money Laundering and Counter Financing of Terrorism / Plaksiy K., Nikiforov A., Miloslavskaya N. // 6th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW). — 2018. — 70-77.

9. Maniraj S.P. Credit Card Fraud Detection using Machine Learning and Data Science / Maniraj S.P., Aditya S., Shadab A., Swarna S. // International Journal of Engineering Research. — 2019.
10. Dornadula V.N. Credit Card Fraud Detection using Machine Learning Algorithms, / Dornadula V.N., Geetha S. // Procedia Computer Science. — 2019. —165. — 631-641.
11. Lebichot B. Deep-Learning Domain Adaptation Techniques for Credit Cards Fraud Detection / Lebichot B., Le Borgne YA., He-Guelton L., Oble F., Bontempi G. // Recent Advances in Big Data and Deep Learning. INNSBDDL 2019. Proceedings of the International Neural Networks Society. — 2020.
12. Carcillo F. Combining unsupervised and supervised learning in credit card fraud detection / Carcillo F., Borgne Y.L., Caelen O., Kessaci Y., Oble F., Bontempi G. // Information Sciences. — 2021. —557. — 317-331.

РАЗДЕЛ 4. НАУЧНЫЕ ДОКЛАДЫ ГРАНТОПОЛУЧАТЕЛЕЙ 2023 ГОДА – СОИСКАТЕЛЕЙ УЧЁНОЙ СТЕПЕНИ КАНДИДАТА НАУК

Алюшин А.М.
НИЯУ МИФИ, мл. научный сотрудник,
alyshin@list.ru

НОВЫЕ ПОДХОДЫ К МАРКИРОВАНИЮ ИНФОРМАЦИИ

Аннотация: Научная новизна проекта заключается в развитии комплексного подхода к защите и подтверждению валидности важных финансовых, распорядительных и юридических документов на бумажном и электронных носителях в информационно-коммуникационной среде предприятия, предполагающего использование биомаркеров (БМ), содержащих биометрическую информацию об авторе документа. Разработка методов, алгоритмов и технических средств технологии маркирования носителей значимой информации и ее верификации с использованием биометрических данных, является актуальной и востребованной в настоящее время задачей.

Ключевые слова: речевая подпись, биомаркер, аудиомаркер, спектрограмма, сонограмма, бинарная подпись, защита документов.

Одной из составляющих информационной среды предприятия является система документооборота, который в настоящее время представлен как в сугубо цифровом, так и в классическом бумажном виде. Надежность и устойчивость функционирования данной системы во многом определяют технологический прогресс предприятия, а также его финансовую устойчивость. Влияние таких факторов как автоматизация процессов управления предприятием, широкое применение средств компьютерной техники и цифровых информационно-коммуникационных каналов, имеет многоплановый характер на надежность системы документооборота предприятия. Так, широкая цифровизация предприятия, несомненно, способствует повышению производительности труда, экономии рабочего времени, созданию более эргономичных рабочих мест и внедрению более интеллектуальных форм трудовой занятости. К числу последних, прежде всего, следует отнести дистанционные формы занятости. Широкий переход на дистанционные формы занятости в период пандемии коронавируса многократно увеличил объем информации и документов, передаваемых по открытым каналам связи. Применяемые на практике средства подтверждения валидности документов (Рис. 1) с помощью широко распространенной технологии электронной подписи (ЭП) [2-5] позволяют повысить надежность документооборота в информационно-коммуникационной системе предприятия. Применение ЭП регламентируется законодательством всех экономически развитых стран.

Законодательством РФ регламентируется ряд документов, которые должны быть составлены и имеют юридическую силу только на бумаге (бумажном носителе). В первую очередь, это относится к финансовым документам, которые должны предъявляться проверяющим органам: акты приѐма/передачи, выставленные и предъявленные счета, приходные и расходные ордера, авансовые отчеты, накладные. Федеральный закон ФЗ № 48-ФЗ [6] и Конвенция [7], например, требуют оформления переводных и простых векселей исключительно на бумажном носителе. Аналогичное требование предъявляется к

нормативным актам, оформляемым на специальных бланках с гербами и эмблемами [8]. Основными преимуществами бумажного документооборота являются высокая устойчивость к воздействию компьютерных вирусов, надежность хранения, простота копирования. С точки зрения подтверждения валидности таких документов основными элементами защиты бумажного документа являются уникальные графические ключи, к которым, прежде всего, относятся бланки и печати предприятий. Наиболее важными здесь являются, безусловно, подпись автора документа и особенности почерка автора в случае использования рукописного документа. Достоинством такого ключа является то, что он содержит в своем составе биометрическую информацию об авторе документа. Однако развитие современных средств сканирования и копирования графической информации высокого разрешения существенным образом снижает надежность использования перечисленных элементов защиты бумажных документов. Кроме этого, одним из встречающихся на практике путей неправомерного использования личной подписи является ее получение под давлением либо при неадекватном состоянии автора. Анализ современных тенденций развития технологий подтверждения валидности документов позволил в качестве перспективного выделить комплексный подход. Такой подход использует преимущества как бумажной, так и электронной форм хранения и передачи данных в информационно- коммуникационной среде предприятия. При этом использование биометрической информации об авторе документа позволяет существенным образом повысить защищенность важных документов от их подделки и фальсификации. Анализ правовых аспектов использования биометрической информации [9, 10] подтвердил возможность ее использования для подтверждения валидности документов.

В последнее время развивается технология речевой подписи (РП) [11-12], которая в качестве маркеров использует речевые сообщения, смысловое содержание которых связано с сутью документа, а биометрические голосовые признаки связаны с автором документа [13]. При таком подходе получается повысить надежность хранения и передачи документов за счет:

− использования смысловой связи между содержанием используемого маркера и содержащимся текстом, при которой изменение текста будет порождать изменение маркера и наоборот;

− уникальности биометрических данных человека.

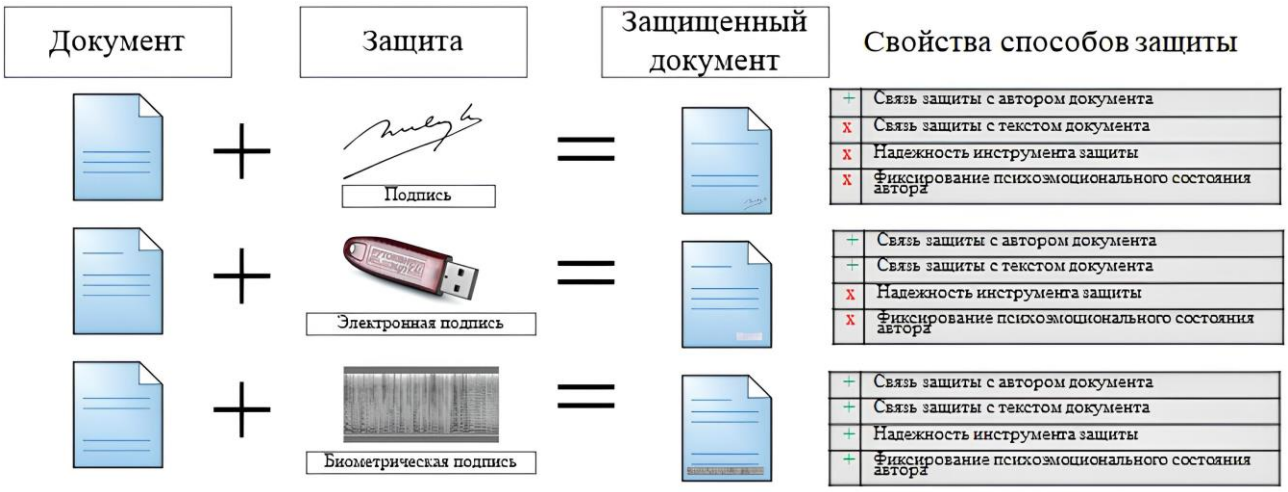


Рис. 1. Различные методы защиты документов и их свойства

Исходя из вышесказанного, можно сделать следующий вывод. Никакая из существующих технологий защиты документов не связывает текст документа, авторство документа с биометрическими данными человека. Именно поэтому наиболее высокоэффективной будет являться технология, которая бы связала валидность документа с биометрическими данными человека таким образом, что было бы невозможно произвести какие-либо изменения в документе без автора данного документа. Наиболее близкой к такой технологии является технология РП, которую целесообразно развить с целью обеспечения возможности передавать в составе маркера расширенный круг биопараметров, позволяющих с высокой степенью достоверности определять функциональное и психоэмоциональное состояние (ФПЭС) автора документа в момент его подписания, либо подготовки.

Всю совокупность биопараметров − частоту сердечных сокращений (ЧСС), вариабельность сердечного ритма (ВСР), артериальное давление (АД), частоту дыхания (ЧД), глубину дыхания (ГД), двигательную активность (ДА), сатурацию крови кислородом (SaO_2), определяющих ФПЭС автора документа, можно подразделить на два класса в зависимости от объема информации, необходимого для передачи в составе БП. К первому классу относятся биопараметры, временное изменение которых может быть описано с помощью одномерной (временной) функции. Ко второму классу относятся биопараметры, для передачи которых в составе БП целесообразно использовать временное изменение их спектра. В таблице 1 представлена классификация биопараметров по указанному признаку.

Табл. 1 – Классификация биопараметров человека

№ п/п	Биопараметры человека	Класс 1D/2D
1	ЧСС, АД, ЧД, ГД, SaO_2	**1D**
2	ВСР, ДА, РС	**2D**

Передача в составе БП биопараметров первого класса не сопряжена с техническими трудностями ввиду небольших информационных объемов передаваемых в составе БП данных. Иначе обстоит дело с биопараметрами второго класса.

Одним из наиболее информативных биопараметров второго класса, который позволяет достоверно определять текущее функциональное и психоэмоциональное состояние автора документа, является ВСР, графическое представление спектрограммы этого биопараметра достаточно уникально для каждого человека и по этой причине может быть использовано для передачи в составе БП информации для определения текущего состояния автора документа, а также для идентификации его личности.

На Рис. 2 показаны основные операции для разработанной методики синтеза БП на основе комплексной модели представления биометрических данных об авторе документа. Методика дает возможность передать в составе БП как голосовую информацию о наиболее важных частях документа, так и динамику изменения его ФПЭС. На рисунке представлена последовательность выполняемых действий при осуществлении декодирования БП рассмотренного вида.

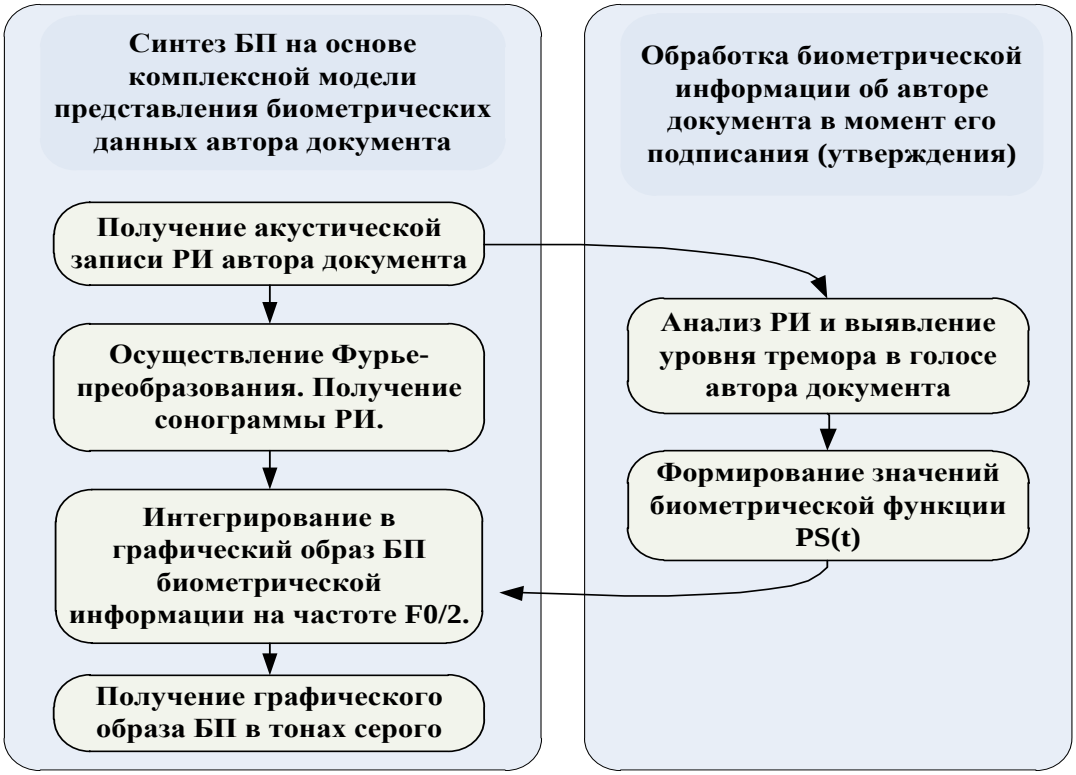


Рис 2 – Методика синтеза БП

Достоинством такого подхода на основе использования комплексной модели представления биометрической информации об авторе документа является возможность использования различных готовых алгоритмов и программных средств для оценки ФПЭС автора.

Цель исследований заключается в повышении уровня защищенности носителей информации от угроз незаконного использования и модификации. Задачами исследования являются:

- развитие и обоснование комплексного подхода к защите и подтверждению валидности важных финансовых, распорядительных и юридических документов на бумажном и электронных носителях в информационно-коммуникационной среде предприятия, предполагающего использование биомаркеров (Рис. 1) (БМ), содержащих биометрическую информацию об авторе документа, а также контекстную информацию защищаемого документа;
- исследование и разработка методов аудиомаркирования и биомаркирования для применения в защищенном документообороте предприятия;
- разработка методов и алгоритмов аудиомаркирования и биомаркирования цифровых изображений и цифровых аудиозаписей с целью их защиты от неправомерного использования;
- разработка программного обеспечения, реализующего созданные методы и алгоритмы;
- проведение экспериментального исследования эффективности разработанной технологии защиты важных документов, представленных на бумажных и электронных носителях.

СПИСОК ЛИТЕРАТУРЫ

1. Распоряжение Правительства Российской Федерации от 28 июля 2017 г. №1632-р «Программа «Цифровая экономика Российской Федерации» [Электронный ресурс]. Режим доступа: http://static.government.ru/media/ 6 files/gFM4FHj4PsB79I5v7yLVuPgu4bvR7M0.pdf (дата обращения: 19.08.2023).
2. Rath, T. Word image matching using dynamic time warping/ T. Rath, R. Manmatha // Proc. IEEE Conf. Computer Vision and Pattern Recognition, 18- 20 June 2003, Madison, WI, USA.–2003.– Vol. 2.– P. 521−527.
3. Zhu, G. Multi-scale structural saliency for signature detection / G. Zhu, Y. Zheng, D. Doermann, S. Jaeger // Proc. IEEE Conf. Computer Vision and Pattern Recognition (CVPR 2007), 18-23 June 2007, Minneapolis, Minnesota, USA.– 2007.– P. 1−8.
4. Fang, B. Off-line signature verification by the tracking of feature and stroke positions / B.Fang, C.H.Leung, Y.Y.Tang, K.W.Tse, P.C.K.Kwok, Y.K.Wong // Pattern Recognition.– 2003.–Vol. 36.– No. 1.– P. 91−101.
5. Zheng, Y.Machine printed text and handwriting identification in noisy document images /Y.Zheng, H.Li, D.Doermann // IEEE Trans. Pattern Analysis and Machine Intelligence. – 2004. – Vol. 26. – No. 3. – P. 337−353.
6. Secure Hash Standard (SHS). Federal information processing standards publication. – FIPS PUB 180-4. – 2015. – 32 p.
7. Конвенция о Единообразном Законе о переводном и простом векселе (Заключена в Женеве 07.06.1930) [Электронный ресурс]. Режим доступа: https://legalacts.ru/doc/konventsija-o-edinoobraznom-zakone-o-perevodnom-i/ (дата обращения: 19.04.2023).
8. Федеральный конституционный закон от 23 июля 2013 г. N 4-ФКЗ [Электронный ресурс]. Режим доступа: https://base.garant.ru/70418992/ (дата обращения: 19.04.2023).
9. Кочеткова, О.В. Особенности правового регулирования использования биометрических документов в Европейском Союзе и Российской Федерации // Фундаментальные исследования. – 2015. – №2–5. – С. 1118– 1122.
10. Кривогин, М.С. Особенности правового регулирования биометрических персональных данных // Право. Журнал Высшей школы экономики. – 2017. – № 2.
11. Дворянкин, С.В. Речевая подпись. – М.: ЦНТИ «Информсвязь». 2003.
12. Дворянкин, С.В. Компьютерные технологии защиты речевых сообщений в каналах электросвязи. – М.: МТУСИ, 1999. – 52 с.
13. Алюшин А.М. Особенности распознавания изображений речевой подписи на мобильных устройствах. / А.М. Алюшин, Н.С. Дворянкин // Безопасность информационных технологий –2015. – Т. 22. № 4. – С. 38-45.

Быстревский С.А.
Дальневосточный федеральный университет (ДВФУ), ассистент,
serg.by.and97@mail.ru

АЛГОРИТМ КОНФИДЕНЦИАЛЬНЫХ ВЫЧИСЛЕНИЙ НА ОСНОВЕ ГОМОМОРФНОГО ШИФРОВАНИЯ, ДЛЯ ПРОВЕДЕНИЯ НЕДИНАМИЧЕСКИХ АУКЦИОННЫХ ТОРГОВ

Аннотация: в рамках данной статьи предложен алгоритм конфиденциальных вычислений на основе гомоморфных преобразований. Так же показана корректность его работы, эффективность и безопасность. Применение гомоморфных преобразований выделяет принципиально новый подход к разработке алгоритмов конфиденциальных вычислений, так как на данный момент активно применяют схемы разделения секрета и искажения логического контура.

Ключевые слова: конфиденциальные вычисления, гомоморфное шифрование, система аукционных торгов, криптографические протоколы.

Введение

В современных условиях развития мировой экономики электронная коммерция всё больше и больше привлекает людей, желающих заняться торговлей, чему значительной мере способствует развитие интернет технологий. И с каждым днём, ведение бизнеса в интернете становится всё доступнее. Роль аукционов в международной торговле некоторыми товарами особенно велика. Например, через международные аукционы в США и Канаде реализуется свыше 80% продаваемой этими странами пушнины, в Дании – 90%, в Швеции и Норвегии – примерно 95%. Также на современном этапе развития земельного рынка в России особую актуальность имеют аукционные продажи земельных участков как способ приобретения земель для жилищного строительства. Также в настоящее время аукционные торги приобретают особую популярность в распределённых реестров так, как согласно исследованиям, всего с 2013 по 2017 года финансовые вложения в распределенные реестры, а именно блокчейн технологии, выросли более чем в 30 раз, и по прогнозам достигнут отметки в 176 миллиардов долларов к 2025 году.

В настоящее время существуют различные подходы к обеспечению конфиденциальности вычислений в рамках аукционных торгов.

Например, одним из подходов, который может использоваться для решения данной задачи это применение протокола блокчейн обеспечивая анонимизацию всех транзакций [1-3]. Дальнейшее развитие идея применения протокола блокчейн для решения проблемы конфиденциальных вычислений получила в работе [4], где совместно с технологией блокчейн применялась схема доказательства знания с нулевым разглашением для проверки корректности полученного результата конфиденциальных вычислений. Недостатком указанных протоколов является высокая вычислительная сложность необходимая для их выполнения. Для обеспечения безопасности вычислений при проведении аукционных торгов, в частности, был предложен алгоритм конфиденциальных вычислений на основе гомоморфного шифрования [5, 6]. Помимо указанного выше подхода можно выделить еще два подхода построения алгоритмов конфиденциальных вычислений: на основе схем разделения секрета и искажении логического контура [7,8]. Однако указанные протоколы также не

обеспечивают конфиденциальность вычислений в полной мере за счет трудоемкости выполнения, заложенных в их основу операция.

Рассмотрим вариацию протокола конфиденциальных вычислений для аукционных торгов на основе гомоморфного шифрования.

Гомоморфное преобразование

Пусть p – это большое простое число, а α и β это его первообразные члены. Тогда введём преобразование $E(x) = \alpha^x \beta^r (\mathrm{mod}\ p)$, где r – это случайное число от 0 до p-2. Такое преобразование будет гомоморфно отображать операцию сложения по модулю p-1 в операцию умножения по модулю p.

Суть алгоритма в том, что участник аукциона хочет заплатить цену x. К этому значению он применяет преобразование, приведённое выше, то есть находит $C = \alpha^x \beta^r (\mathrm{mod}\ p)$. Значения x и r участник хранит при себе в секрете, а значение C участвует в протоколе и играет роль цифровой подписи. И в конце если участник выиграет аукцион, то он предоставит значения x и r, после чего происходит проверка правильности значения C, если всё совпадает, то в ходе протокола участник не мошенничал и действительно его цена самая большая.

Процедура верификации

В протоколе понадобиться следующая процедура верификации данных:

Участник протокола может доказать системе, что его значение цены $x > x_0$, где $x \in [0, \frac{p-1}{2}]$ и $x_0 \in [0, \frac{p-1}{2}]$.

Протокол верификации можно описать следующим образом:

A – участник протокола, доказывающий, что $x \geq x_0$, где $x_0 \in [0, \frac{p-1}{2}]$, B – арбитр.

Вход: Участник A хранит значения x, r и $C = \alpha^x \beta^r (\mathrm{mod} p)$.

Выход: Участник A доказывает арбитру B, что $x \geq x_0$.

1. B → A: $C_0 = \alpha^{x_0} \beta^{r_0} (\mathrm{mod} p), x_0$
2. A: участник протокола генерирует следующие числа $w_1 \in [0, \frac{p-1}{6}]$ и $w_2 = w_1 - \frac{p-1}{6}$, чтобы или $x - x_0 + w_1 \in [\frac{p-1}{6}, \frac{p-1}{3}]$ или $x - x_0 + w_2 \in [\frac{p-1}{6}, \frac{p-1}{3}]$. И применяет к ним гомоморфное преобразование $W_1 = \alpha^{w_1} \beta^{r_1} (\mathrm{mod} p)$, $W_2 = \alpha^{w_2} \beta^{r_2} (\mathrm{mod} p)$.
3. A → B: C, W_1, W_2.
4. B → A: $b \in \{0, 1\}$.
5. Если b = 0:

5.1. A → B: w_1, w_2, r_1, r_2.

5.2. B: проверяет, если $W_1 = \alpha^{w_1} \beta^{r_1} (\mathrm{mod} p)$ и $W_2 = \alpha^{w_2} \beta^{r_2} (\mathrm{mod} p)$ и $|w_1 - w_2| = \frac{p-1}{6}$, w_1 и w_2 имеют разные знаки, то участник A прошёл проверку и его значение $x \geq x_0$.

6. Если b = 1:

6.1. A → B: $w = x - x_0 + w_z (\mathrm{mod}\ p - 1),\ u = r - r_0 + r_z\ (\mathrm{mod}\ p - 1)$, где $z \in \{1, 2\}$, которое выбрано таким образом, чтобы $w \in [\frac{p-1}{6}, \frac{p-1}{3}]$.

6.2. B: проверяет, если $C \cdot {C_0}^{-1} \cdot W_z = \alpha^w \beta^u (\mathrm{mod} p)$ и w ∈∈ $[\frac{p-1}{6}, \frac{p-1}{3}]$, то участник A прошёл проверку и его значение $x \geq x_0$.

Конец протокола.

Покажем, что данный алгоритм работает корректно. Для начала покажем, что участник, у которого $x \geq x_0$ сможет выполнить оба действия.

Если у участника A $x \geq x_0$ и $x \in \left[0, \frac{p-1}{2}\right], x_0 \in \left[0, \frac{p-1}{2}\right]$, то $x - x_0 \in \left[0, \frac{p-1}{2}\right]$. Тогда участник A сможет получить $x - x_0 + w \in \left[\frac{p-1}{6}, \frac{p-1}{3}\right]$ отняв или прибавив $w \in \left[0, \frac{p-1}{6}\right]$. Схематично это можно рассмотреть ниже на рисунке 1.

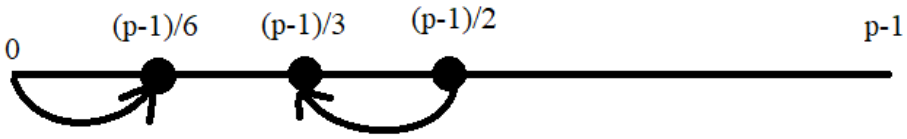


Рисунок 1 - Схема положения на числовой прямой

Алгоритмически выбор w_1 и w_2 можно задать следующим образом:

1) Если $x - x_0 \in \left[0, \frac{p-1}{6}\right]$, то к этому значению надо прибавить число, что бы оно лежало в промежутке $\left[\frac{p-1}{6}, \frac{p-1}{3}\right]$, то есть $w_1 \in \left[\frac{p-1}{6} - x + x_0, \frac{p-1}{6}\right]$, а значение $w_2 = w_1 - \frac{p-1}{6}$

2) Если $x - x_0 \in \left[\frac{p-1}{3}, \frac{p-1}{2}\right]$, то от этого значения надо отнять число, что бы оно лежало в промежутке $\left[\frac{p-1}{6}, \frac{p-1}{3}\right]$, то есть $w_2 \in \left[-\frac{p-1}{6}, \frac{p-1}{3} - x + x_0\right]$, а значение $w_1 = w_2 + \frac{p-1}{6}$

3) Если $x - x_0 \in \left(\frac{p-1}{6}, \frac{p-1}{3}\right)$, то можно как прибавить, так и отнять число, но так что бы оно не вышло за промежуток. То есть $w_1 \in \left[0, \frac{p-1}{3} - x + x_0\right]$, а значение $w_2 = w_1 - \frac{p-1}{6}$. Или $w_2 \in \left[\frac{p-1}{6} - x + x_0, 0\right]$, а значение $w_1 = w_2 + \frac{p-1}{6}$

Таким образом участник A, у которого $x \geq x_0$ способен выполнить оба условия и пройти алгоритм, при любом запросе от арбитра.

Теперь покажем, что если $x < x_0$, то участник не сможет выполнить оба условия.

Если у участника A $x < x_0$ и $x \in \left[0, \frac{p-1}{2}\right], x_0 \in \left[0, \frac{p-1}{2}\right]$, то $x - x_0 \in \left(\frac{p-1}{2}, p - 1\right)$, так как по гомоморфному преобразованию все операции сложения показателей степеней происходят по модулю p-1. Как видно из рисунка 1 из этого промежутка невозможно попасть в промежуток $\left[\frac{p-1}{6}, \frac{p-1}{3}\right]$ прибавив или отняв число $w \in \left[0, \frac{p-1}{6}\right]$. Таким образом если участник выполняет первое условие, то есть $w_1 \in [0, \frac{p-1}{6}]$ и $w_2 = w_1 - \frac{p-1}{6}$, то $x - x_0 + w \in \left(\frac{p-1}{3}, \frac{p-1}{6}\right)$ и участник проваливает второе условие. А если участник выполняет второе условие, то есть $x - x_0 + w \in \left(\frac{p-1}{3}, \frac{p-1}{6}\right)$, то или $w_1 > \frac{p-1}{6}$ или $w_2 < -\frac{p-1}{6}$ и участник проваливает первое условие.

Таким образом участник A, у которого $x < x_0$ способен выполнить только одно из двух условий и проходит алгоритм с вероятность $\frac{1}{2}$.

Теперь докажем безопасность алгоритма верификации. Если b = 0, то участник A в принципе не раскрывает своих секретных данных, так как w_1, w_2, r_1, r_2 сгенерированы только для данного протокола и никак не связанны с секретными значениями, таким образом из них нельзя получить никакой информации. Если b = 1, то проверяющий получает $w = x - x_0 + w_z$ и $u = r - r_0 + r_z$, где x и r это секретные значения, но проверяющий не может их узнать, так как он не знает значений w_1, w_2, r_1, r_2, которые он мог узнать, только если бы отправил значение b = 0.

Протокол нахождения наибольшей ставки

Теперь рассмотрим, как применив алгоритм верификации можно определить наибольшую из ставок участников.

Наша задача отсеивать людей до тех пор, пока не останется 1 участник аукциона сверху.

Допустим на некотором шаге в протоколе остались цены от [N, V]. То далее можно поступить следующим образом: берём середину этого интервала, то есть $\frac{N+V}{2}$. После проводим процедуру верификации на участке доказывая, что секретные числа больше $\frac{N+V}{2}$. Далее возможно три исхода:

1) Процедуру верификации смог пройти только один участник, тогда он и становиться победителем аукциона

2) Процедуру верификации смогли пройти больше одного участника, тогда остаются только эти участники и рассматривается промежуток $[\frac{N+V}{2}, V]$.

3) Все участники не прошли процедуру верификации, значит все участники продолжают участвовать в протоколе и рассматривается промежуток $[N, \frac{N+V}{2}]$

Как видим при первом исходе протокол завершает работу, а при втором и третьем уменьшает длину промежутка в два раза. Так как изначально длина промежутка $\frac{p}{2}$, то максимальное число итераций протокола это $\log_2 \frac{p}{2} = \log_2 p - 1$. То есть данный алгоритм конечен и полиноминален, так как линейно зависит от длины большого простого числа p.

В ходе алгоритма также важен выбор арбитром участников на проверку ставок. Данный аспект напрямую будет влиять на безопасность протокола.

Пусть в ходе алгоритма арбитр спрашивал участников в следующем порядке: 1, 2, 3, 4, …, n. Тогда в следующий раз он их должен спрашивать в обратном порядке: n, n-1, n-2, …, 1.

На этом закончен разбор алгоритма с помощью, которого реализовано сохранение конфиденциальности данных участников аукциона.

Заключение

В рамках данной работы разработан алгоритм конфиденциальных вычислений для аукционных торгов с закрытыми ставками, позволяющий узнать у кого из участников наибольшая ставка, при этом не раскрывая значения их ставок, даже для организаторов аукциона. Показана его корректность и безопасность. Данный алгоритм имеет полиномиальную сложность, что позволяет использовать его для проведения нединамических аукционных торгов даже с большими ставками. Для противодействия возможного обмана участниками аукциона использована цифровая подпись ставки участника. Также имитация действий других участников обнаруживается с использованием механизма проверки участников арбитром. Таким образом любое нарушения протокола может повлечь дисквалификацию из аукциона, так как будет свидетельствовать о сговоре или обмане. Можно отдельно отметить, что предложенный алгоритм конфиденциальных вычислений основан на гомоморфном шифровании, позволяя выделить принципиально новый подход к разработке подобного семейства алгоритмов.

Стоит отдельно отметить, что алгоритмы конфиденциальных вычислений, способные вычислить любую вычислимую функцию более важны, так как способны покрыть большее количество задач, кроме нединамических аукционов [9,10]. Рассмотрение возможности создания такого алгоритма конфиденциальных вычислений на основе гомоморфного шифрования требует отдельного исследования.

СПИСОК ЛИТЕРАТУРЫ

1. Al-Bassam M. et al. Airtnt: Fair exchange payment for outsourced secure enclave computations //arXiv preprint arXiv:1805.06411. – 2018.
2. Bentov I. et al. Tesseract: Real-time cryptocurrency exchange using trusted hardware //Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security. – 2019. – С. 1521-1538.
3. Cheng R. et al. Ekiden: A platform for confidentiality-preserving, trustworthy, and performant smart contracts //2019 IEEE European Symposium on Security and Privacy (EuroS&P). – IEEE, 2019. – С. 185-200.
4. Galal H. S., Youssef A. M. Succinctly verifiable sealed-bid auction smart contract //Data Privacy Management, Cryptocurrencies and Blockchain Technology. – Springer, Cham, 2018. – С. 3-19.
5. Казарин О. В. Разработка методов проактивной защиты информационных систем на основе конфиденциальных вычислений. //Вопросы защиты информации. 2013. № 3 (102). С. 68-80.
6. Варановский Н. П., Мартишин С. А., Храпченко М. В., Шокуров А. В. Пороговые схемы гомоморфного шифрования и защита информации в облачных вычислениях. //Вестник Московского университета. Серия 15: Вычислительная математика и кибернетика. 2017. № 1. С. 38а-44.
7. Gilad Asharovy, Yehuda Lindelly. A Full Proof of the BGW Protocol for Perfectly Secure Multiparty Computation. //DSPA: Issues of application of digital signal processing. 2018. Т. 8. № 1. С. 12-17.
8. Thomas Schneider, Michael Zohner. GMW vs. Yao? Ecient Secure Two-Party Computation with Low Depth Circuits. //ACS Sensors. 2017. Т. 2. № 8. С. 1128-1132.
9. Русаловский И. Д., Бабенко Л. К. Проблема полностью гомоморфной обработки целых чисел. //В сборнике: Безопасность информации и компьютерных сетей (SIN 2019). Материалы 12-й Международной научной конференции. 2019. С. 41-43.
10. Бабенко Л. К., Русаловский И. Д. Библиотека полностью гомоморфного шифрования целых чисел. //Известия ЮФУ. Технические науки. 2020. № 2 (212). С. 218-227.

Вишневский А.С.
МГТУ им Н.Э. Баумана, младший научный сотрудник,
andrey.s.vishnevsky@yandex.ru

АНАЛИЗ СЕМАНТИКИ МУЗЫКИ ПО СОПУТСТВУЮЩЕМУ ТЕКСТУ ДЛЯ СОНИФИКАЦИИ СЕТЕВЫХ АНОМАЛИЙ

Аннотация: сонификация применяется в различных областях техники как в составе мультимодальных систем, так и в исключительно звуковых пользовательских интерфейсах. Исследования эргономики слуховых дисплеев в средствах информационной безопасности сфокусированы на обнаружении сетевых атак с помощью синтезированных мелодий, звуков природы и генерации голоса. Данная работа посвящена экспериментальной оценке показателей качества обнаружения компьютерных атак на слух с помощью специальным образом подобранных звукозаписей музыки, исполненной профессиональными исполнителями. Проведенный эксперимент показал перспективность выбора музыки по тексту, на который она написана, для озвучивания сетевых аномалий.

Ключевые слова: компьютерные атаки, обнаружение аномалий, сонификация, обработка естественных языков, музыка

Введение

Повсеместное использование вычислительной техники, постоянная угроза компьютерных атак и недоверие к автоматизированным средствам защиты требуют присутствия человека в системе обеспечения безопасности информационных ресурсов. Данное исследование направлено на создание средств обнаружения сетевых угроз на слух, для создания возможности профессиональной работы в сфере защиты информации операторам с ограничениями по зрению. Предложенный подход отличается от существующих методов сонификации использованием текста, по которому написана музыка, для вызова ассоциаций с событиями информационной безопасности. Перспективность озвучивания данных с опорой на текст музыки заключается в более широком пространстве размерностей, чем при стандартной параметрической сонификации. В связанном с музыкой тексте можно найти ключевые слова по большему количеству тем, чем число параметров звука, используемых в существующих методах сонификации.

Состояние предметной области

Эксон исследовала возможность применения сонификации для снижения визуальной нагрузки на специалистов по реагированию на инциденты информационной безопасности [1 – 3, 7, 8, 15], предложила стандартизированную процедуру оценки эффективности сонификации и получила в ходе экспериментов от испытуемых долю правильных ответов от 25 до 96%, точность 100% и полноту обнаружения угроз от 60% до 100%. Дебаши экспериментально показал, что пользователь на слух точнее обнаруживает некоторые сетевые атаки, чем автоматизированные средства защиты, основанные на машинном обучении [4, 5]. Намин оценил утомляемость пользователей звукового интерфейса в средствах обнаружения сетевых атак [6]. Фолк и Дикстра экспериментально проверили эффективность озвучивания авторизации пользователей в корпоративной сети [9]. Сара Ленци предложила метод создания таксономии индикаторов компьютерных атак на водонапорные станции для иерархической сонификации по высоте тона, тембру, ритму и семантике звуков природы [10, 12, 15]. Лутц

сонифицировал процесс обнаружения сетевых соединений с серверами веб-трекинга и проверку надежности создаваемых пользователями паролей [11, 16]. Датта сонифицировал предупреждения о фишинге, наличии вредоносных программ и ошибках заполнения веб-форм, получив в ходе эксперимента долю верных ответов испытуемых от 4% до 96% [17]. Эксперимент Поладжика показал, что испытуемые распознают на слух по музыке эпохи барокко аномальный сетевой трафик с долей правильных ответов от 5% до 100% в зависимости от типа угрозы и сопоставленный мелодии [18]. Джонс исследовал применимость сонификации к уведомлению о кибер-угрозах, опросив студентов, как они воспринимают потенциальный ущерб от хакерских атак [19]. Исследования звуковых пользовательских интерфейсов, основанных на воспроизведении музыкальных звукозаписей опубликованы в рамках диссертационной работы [13, 20, 21].

Метод

Звукозаписи были сопоставлены аномальным сетевым запросам, обнаруженным с помощью сети веб-сайтов. Если с одного и того же ip-адреса поступали запросы к веб-сайтам в различных доменных зонах и содержащим контент на разных языках, это расценивалось как потенциальная нежелательная активность. Экспериментальные оценки такого метода обнаружения сетевых аномалий приведены в [22], а в данной работе мы исследуем эффективность их сонификации с помощью музыки. Текст песни, арии, либретто и даже название музыкального произведения содержит ключевые слова, по толкованиям которых можно оценить их смысловую близость к понятиям пользы и вреда, добра и зла. Если в связанном с музыкой тексте присутствовали слова, ассоциирующиеся с насилием, обманом, недобросовестным поведением, звукозапись сопоставлялась аномальным событиям. В случае отсутствия слов, переходы по толкованиям которых могли бы привести к понятиям вреда, звукозапись выражала нормальную легитимную сетевую активность. Интерактивные переходы по толкованиям всех слов, входящих в текст музыки, осуществлялись по словарям Даля, Ушакова, Ожегова и Кузнецова.

Пользователям было предложено прослушать десять музыкальных звукозаписей и ответить, возникает ли у них ассоциация с чем-либо опасным. Правильным считалось распознавание опасности по музыке, которая была сопоставлена аномальной сетевой активности.

Результаты эксперимента

Испытания прошли 12 добровольцев разных возрастов. Среди них были мужчины и женщины, музыканты и те, кто не слушает музыку, профессионалы в ИБ и работники из других сфер деятельности. Эксперимент проходил в два этапа. Сначала испытуемые отвечали на вопросы без знания схемы сонификации. Затем им объяснялась схема сонификации с опорой на текст и эксперимент повторялся. В результате были рассчитаны доля правильных ответов, точность, полнота и F1-мера. На (Рис. 1) показаны метрики качества ответов для всех испытуемых. Можно увидеть, что точность ответов повышалась после инструктажа. Несколько пользователей смогли показать стопроцентную точность ответов. Как правило, это были люди, которые слышали задействованные в эксперименте музыкальные отрывки ранее.

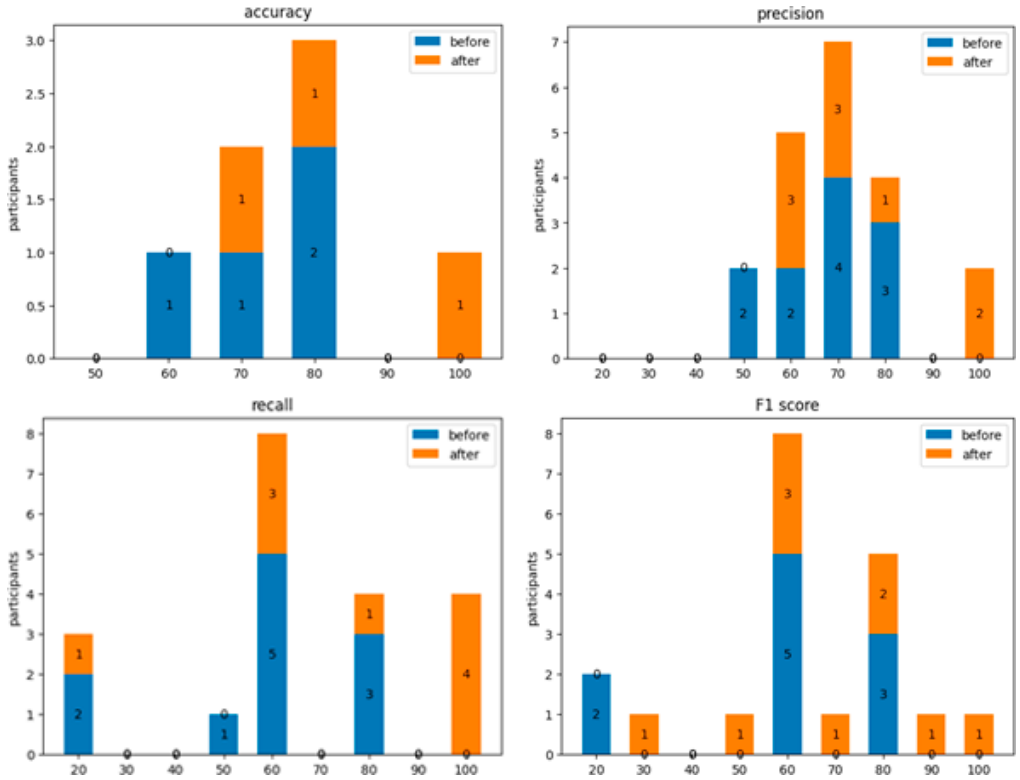


Рисунок 1 Доля правильных ответов, точность, полнота и мера F1 для всех испытуемых

Результаты музыкантов и любителей музыки показаны на (Рис. 2). Метрики качества их ответов отказались не ниже 50% до объяснения схемы сонификации и не ниже 60% после.

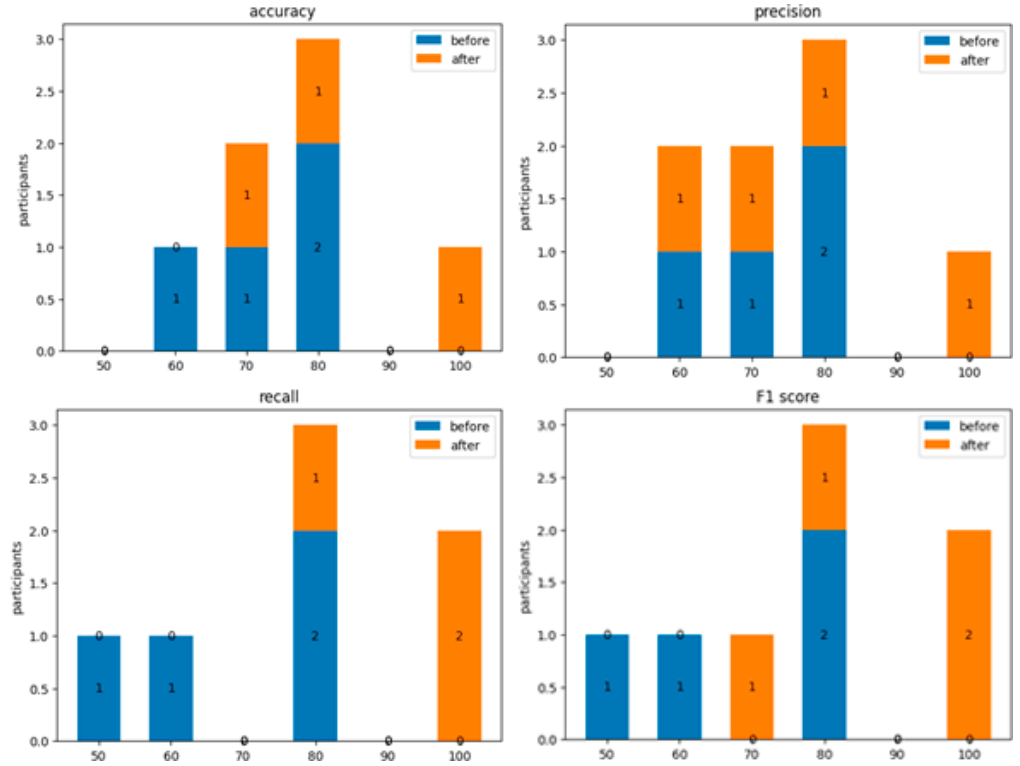


Рисунок 2 Доля правильных ответов, точность, полнота и мера F1 для музыкантов и любителей музыки

Выводы

У пользователей срабатывают полезные для анализа компьютерных атак ассоциации при прослушивании музыки. Схема сонификации аномалий с опорой на ключевые слова песен, романсов и арий показала наибольшую эффективность среди любителей классической

музыки и выпускников музыкальных учебных заведений различного уровня. Точность ответов удалось повысить за счёт объяснения пользователям принципа сопоставления музыки событиям информационной безопасности. Ожидается, что за счёт предварительного обучения можно добиться большей эффективности работы пользователей на слух. Мы надеемся, что предложенный метод озвучивания событий безопасности с опорой на текст позволит в будущем обойти ограничения по размерности кодируемых данных, накладываемые широко распространенными методами параметрической сонификации.

СПИСОК ЛИТЕРАТУРЫ

1. Axon L., Nurse J. A Formalised Approach to Designing Sonification Systems for Network−Security Monitoring // International Journal on Advances in Security. – 2017.
2. Axon L. M. et al. Sonification in security operations centres: what do security practitioners think? //arXiv preprint arXiv:1807.06706. – 2018.
3. Axon L. et al. Sonification mappings: estimating effectiveness, polarities and scaling in an online experiment // Journal of the Audio Engineering Society. – 2018. – V. 66. – №. 12. – pp. 1016-1032.
4. Debashi M., Vickers P. Sonification of network traffic flow for monitoring and situational awareness //PloS one. – 2018. – V. 13. – №. 4. – p. e0195948.
5. Debashi M. Interactive Sonification of Network Traffic to Support Cyber Security Situational Awareness. – University of Northumbria at Newcastle (United Kingdom). – 2018.
6. Namin A. S. et al. The Sounds of Cyber Threats // arXiv preprint arXiv:1805.08272. – 2018.
7. Axon L. et al. Hearing attacks in network data: an effectiveness study //Computers & Security. – 2019. – V. 83. – pp. 367-388.
8. Axon L., et al. Sonification to Support the Monitoring Tasks of Security Operations Centres // IEEE Transactions on Dependable and Secure Computing. – 2021 – V. 18. – №. 3. – pp. 1227-1244
9. Falk, C., Dykstra, J. Sonification with Music for Cybersecurity Situational Awareness. – 2019. – pp. 50-55. DOI:10.21785/icad2019.014.
10. Lenzi S. et al. Disclosing cyber-attacks on water distribution systems. An experimental approach to the sonification of threats and anomalous data // Sonification for Everyday Life: Proceedings of the 25th Annual International Conference on Auditory Display. – International Community on Auditory Display. – 2019. – pp. 125-132.
11. Lutz O. H. M. et al. Surfing in sound: Sonification of hidden web tracking // Georgia Institute of Technology. – 2019.
12. Moreno, A. et al. A sonification model for real-time anomaly detection in machine learning supported cybersecurity. DOI:10.13140/RG.2.2.11419.21287.
13. Вишневский А.С., Ключарев П.Г. Звуковой пользовательский интерфейс обманной системы / под. ред. А. А. Александрова // Безопасные информационные технологии. Сборник трудов Десятой международной научно-технической конференции – М.: МГТУ им. Н. Э. Баумана. – 2019. – p. 409
14. Axon L. et al. Data presentation in security operations centres: exploring the potential for sonification to enhance existing practice // Journal of Cybersecurity. – 2020. – V. 6. – №. 1. – p. tyaa004.

15. Lenzi S. et al. A design-driven sonification process for supporting expert users in real-time anomaly detection: Towards applied guidelines // EAI Endorsed Transactions on Creative Technologies. – 2020. – V. 7. – №. 23. – pp. e4-e4.
16. Lutz O. H. M. et al. That password doesn't sound right: interactive password strength sonification // Proceedings of the 15th International Audio Mostly Conference. – 2020. – pp. 206-213.
17. Datta P. et al. Warning users about cyber threats through sounds //SN Applied Sciences. – 2021. – №. 3. – С. 1-21.
18. Polaczyk J. et al. Compositional Sonification of Cybersecurity Data in a Baroque Style // Advances in Artificial Intelligence, Software and Systems Engineering: Proceedings of the AHFE 2021 Virtual Conferences on Human Factors in Software and Systems Engineering, Artificial Intelligence and Social Computing, and Energy. – 2021. – Springer International Publishing. – pp. 304-312.
19. Jones K. S. et al. Grouping and Determining Perceived Severity of Cyber-Attack Consequences: Gaining Information Needed to Sonify Cyber-Attacks // Journal on Multimodal User Interfaces. – 2022. – pp. 1-14.
20. Vishnevsky, A.S. et al. Sonification of information security events in auditory display: Text vocalization, navigation, and event flow representation // Journal of Accessibility and Design for All. – 2022. – №12(1). – pp. 116–133.
21. Vishnevsky, A.S. et al. Sonification of Information Security Incidents in an Organization Using a Multistep Cooperative Game Model / Rocha, A., Adeli, H., Dzemyda, G., Moreira, F. (eds) // Information Systems and Technologies. WorldCIST 2022. Lecture Notes in Networks and Systems. Springer, Cham. – 2022. – № 468.
22. Вишневский А.С. Обманная система для обнаружения хакерских атак, основанная на анализе поведения посетителей веб-сайтов // Вопросы кибербезопасности. – 2018. – № 3 (27). – С. 54-62.

Вовик А.Г.
МТУСИ, ассистент каф. ИСУиА
a.g.vovik@mtuci.ru

К ВОПРОСУ ФОРМАЛИЗАЦИИ МОДЕЛЕЙ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ В СИСТЕМАХ ИНТЕРНЕТА ВЕЩЕЙ

Аннотация: Исследование направлено на обоснование необходимости разработки численных моделей и метода управления информационной безопасностью. В качестве инструмента разработки предложен метод обеспечения требуемого уровня защиты информации в системах Интернета Вещей на основе нечетких моделей Мамдани. Предлагаемый метод может быть использован для синтеза автоматизированной системы управления информационной безопасностью систем Интернета Вещей.

Ключевые слова: «Интернет Вещей», «Управление информационной безопасностью», «Нечеткое моделирование», «Модель Мамдани».

По данным Oneside, всего в 2022 году количество подключенных IoT-устройств в России превысило 70 млн. Несмотря на то, что традиционным примером реализации технологии Интернета Вещей является концепция «умного дома», самыми распространенными сценариями использования M2M и IoT-технологий в 2022 году стали системы безопасности, подключенные камеры видеонаблюдения, интеллектуальные системы для транспорта и умные системы учета расхода воды и энергоресурсов [1].

Согласно докладу, к концу 2022 года общее количество подключенных IoT-устройств в России в сегментах B2B/B2G выросло до 55,8 млн шт, из которых 34,2 млн работало в сетях телеком-операторов. Затраты государства и бизнеса в РФ на внедрение M2M и IoT составили почти 114 млрд рублей. Темпы роста количестве устройств, подключенных к Интернету вещей в России представлены на рис. 1.

Рис. 1. Динамика роста технологии Интернета Вещей в России [1]

Достоверная статистика роста количества информационных инцидентов в системах интернета вещей в открытом доступе отсутствует, чему есть объективные причины: по большей части такие системы носят коммерческий характер, поэтому владельцы систем не стремятся обнародовать факты нарушения ИБ, опасаясь репутационных потерь. Однако отдельные факты информационных инцидентов известны в свободном доступе, что позволяет обоснованно предполагать, что обеспечение надлежащей защиты миллиардов устройств из категории «Интернет Вещей» исключительно важно.

Еще в 2007 г. исследователи показали, что электрогенератор может быть дистанционно выведен из строя путем его быстрого включения-выключения с помощью автоматического выключателя. В 2014 г. хакеры взломали промышленную сеть немецкого сталелитейного завода и заблокировали остановку доменной печи [2]. Таких подтвержденных фактов все больше с каждым годом.

Проблемы обеспечения ИБ в системах интернета вещей условно можно разделить на:

- противодействие хищению персональных данных и данных, раскрывающих информацию о поведении владельца и проч. – подпадает под действие нормативных актов (Федеральный закон № 152-ФЗ «О персональных данных» от 27.07.2006г.)
- противодействие нарушению работы систем интернета вещей (функциональная безопасность), нормативными актами не регламентируется.

Регулирование вопроса информационной безопасности интернета вещей со стороны государства носит противоречивый и непоследовательный характер. На сегодняшний день можно констатировать отсутствие специального государственного стандарта, посвященного регламентированию вопросов обеспечения информационной безопасности в системах Интернета Вещей. Можно признать, что деятельность регулирующих органов государственной власти в отношении проблем информационной безопасности интернета вещей не соответствует современным вызовам, при этом интересы непрерывности бизнес-процессов рассматриваются как безусловно приоритетные по отношению к обеспечению ИБ.

Например, 8 июля 2021 года, Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации решило отказаться от идеи по регистрации SIM-карт, устанавливаемых в банкоматах, счетчиков электроэнергии и другом IoT оборудовании.

Как сообщает РБК со ссылкой на проект постановления правительства, разработанный ведомством, юридические лица и индивидуальные предприниматели не должны вносить сведения о своих IoT-устройствах в Единую систему идентификации и аутентификации (ЕСИА), если договор об оказании услуг связи был заключен до 1 июня 2021 года. Причем делать это нужно будет только в момент смены оборудования.

В качестве обоснования такого решения в Минцифры считают, что регистрация SIM-карт устройств интернета вещей влечет за собой «большой и сложно реализуемый объем работы» и риски того, что большое количество техники, например банкоматы, перестанут работать, так как их функциональность напрямую зависит от оказываемых услуг связи [1].

Однако, недостаточная защищенность тех же банкоматов от сетевых атак различного типа может также быть причиной того, что банкоматы «перестанут работать», только при этом такая ситуация может усугубиться значительным материальным ущербом.

В настоящее время у технологии IoT с точки зрения безопасности информации есть множество существенных недостатков. По мнению ряда специалистов одним из важнейших недостатков считается низкий уровень безопасности личных данных пользователей [3].

По оценке компании Hewlett-Packard, больше 70% вещей с доступом к сети интернет, имеют уязвимость, связанную с небезопасным web-interface, а также проблемы вызывает слабая защищенность IP-адресов и их портов [4]. В результате взлома злоумышленники получают данные своих жертв, а также информацию о структуре и характеристиках системы, которые в дальнейшем используются по усмотрению злоумышленников. В случае, если атакованная система имеет определенную суммарную производительную мощь, злоумышленник может использовать это для нападения на определенные ресурсы (посредством организации DOS-атак). А учитывая огромное количество подключенных к сети устройств, даже при небольшой вычислительной мощности отдельного устройства, это может

представлять системную угрозу. Если же целью злоумышленника является эта конкретная система, то полученная им информация позволит осуществить свои преступные замыслы.

Принимая во внимание выше сказанное, обеспечение безопасности технологии IoT – это актуальная на сегодняшний день задача, решение которой еще не найдено [5-7].

Вместе с тем, сегодня мы можем по крайней мере, осознавать структуру проблематики обеспечения информационной безопасности Интернета Вещей.

1. Прежде всего, существует неопределенность в конкретизации собственно объекта защиты. Говоря об информационных системах, использующих технологии интернета вещей, очевидно, что сам термин «Интернет Вещей» подразумевает очень разные системы и по составу, и по целям, и по размеру предполагаемого ущерба, и по количеству потенциальных «жертв» – от «умных домов» до систем управления транспортом в городах, систем управления технологическими процессами, в том числе повышенной экологической опасности (IIoT) и т.д. Конкретизируя тип объекта защиты, появляется возможность построения более точной модели «угрозы-уязвимости-риски».
2. В отличие от традиционных автоматизированных систем (АС) существует проблема эффективных методов и способов защиты информации именно для систем интернета вещей. Так, например, многие, хорошо зарекомендовавшие себя в АС способы аутентификации неприменимы в ситуации M2M (биометрия, использование заранее известной пользователю-человеку нетривиальной информации и т.п.).
3. Проблема управления ИБ в системах интернета вещей, которая в существующей парадигме может быть сведена к задаче управления информационными рисками.

Последняя проблема представляет наибольший интерес, так как ее решение и создает условия поддержания заданного уровня защищенности информации в системе при постоянно меняющихся условиях:

- изменения во времени уровня информационных рисков в следствие появления новых угроз и выявления новых уязвимостей в системе, в том числе уязвимостей как к вновь появившимся, так и ранее уже известным угрозам;
- изменению структуры защищаемой системы – появлению новых элементов, изменению масштаба, появлению новых связей между элементами;
- «старению» (снижению эффективности) с течением времени жизни системы применяемых методов и способов защиты информации в этой системе. Под эффективностью в данном случае понимаем способность способа защиты решать поставленную задачу: обеспечивать надежную аутентификацию «вещей» при информационном обмене, обеспечивать противодействие сетевым атакам и т.д.

В настоящее время процессы управления информационной безопасностью регламентируются серией стандартов ГОСТ Р ИСО/МЭК 2700х [8], а также рядом документов ФСТЭК, например Методический документ «Методика оценки угроз безопасности информации» [9]. Для оценки защищенности информации в системе применяются положения стандартов ГОСТ Р ИСО/МЭК 15408-х-2012 «Методы и средства обеспечения безопасности информационных технологий. Критерии оценки безопасности». Однако следует учитывать, что указанные регламентирующие документы изначально ориентированы на традиционные автоматизированные системы и вопрос корректности прямого распространения содержащихся в этих документах норм и правил для систем IoT, учитывая специфику последних, весьма сомнителен. Вместе с тем основные подходы, такие как риско-ориентированный подход, декомпозиция защищаемой системы на информационные активы, - могут быть признаны универсальными по отношению к типу защищаемой системы.

Основной проблемой практического применения перечисленных нормативных документов при организации процесса управления информационной безопасностью, на взгляд автора, является то, что в их основе лежат вербальные модели, представляющие собой по сути рекомендации и описания последовательности и содержания этапов оценки рисков информационной безопасности и организации контрмер на неформальном (в данном случае русском) языке. Как известно, основными особенностями неформальных языков является их избыточность и наличие существенной неопределенности. Кроме того, вербальные неформальные модели как правило или вообще не предполагают численных оценок, или допускают использование экспертных групп для численной оценки значений некоторых вероятностных характеристик (например, при актуализации рисков).

Так, в качестве примера неформализованной модели укажем формулировку критерия соответствия мер защиты предъявляемым требованиям в стандарте ГОСТ Р ИСО/МЭК 15408-1-2012 [9] «для владельца актива важна убежденность в том, что:

- контрмеры являются достаточными, если контрмеры выполняют то, что заявлено, и угрозам, направленным на активы, обеспечивается противостояние;
- контрмеры являются корректными, если контрмеры выполняют то, что заявлено».

Известно, что применение контрмер для реализации стратегии снижения риска в информационной системе, т.е. фактически применение известных и доступных способов защиты информации требует материальных затрат. Они могут включать стоимость программного и аппаратного обеспечения, расходы на внедрение, эксплуатацию и ремонт, стоимость обучения специалистов и проч. Этот важный аспект также не нашел своего отражения в рассматриваемых нормативных документах.

Поиски возможности создания формальных моделей процессов управления информационной безопасностью в системах IoT, формализация оценки защищенности информации в системе является важнейшим направлением исследований.

В этой связи, целью работы является разработка формализованного метода управления информационной безопасностью на основе нечетких моделей Мамдани в целях обеспечения и поддержания требуемого уровня защиты информации в системах Интернета Вещей. Для достижения поставленной цели необходимо:

- выполнить исследование современного состояния проблемы УИБ в информационных системах, анализ специфики проблем защиты информации в системах Интернета Вещей;
- выполнить анализ требований руководящих документов и нормативных актов РФ в области управления информационной безопасностью;
- разработать метод построения численных моделей процесса управления информационной безопасностью в системах IoT;
- на основе полученных численных моделей разработать метод управления информационной безопасностью IoT-систем;
- разработать методику и рекомендации по практическому применению разработанного метода управления информационной безопасностью в системах интернета вещей;
- реализовать полученные результаты и выполнить апробацию предложенного метода.

В качестве критерия эффективности управления безопасностью может быть выбрано «поддержание заданного уровня защищенности информации в системе при минимизации затрат», который может быть формализован в общем виде (1.1):

$$\Pi_{эфф} = \begin{cases} R_t \to R_0 \\ C_t \to C_{min} \end{cases} \quad (1.1)$$

где:

$\boldsymbol{П_{эфф}}$ - критерий оптимального управления ИБ в системе IoT;

$\boldsymbol{R_t}$ - текущий уровень информационных рисков в системе;

$\boldsymbol{R_0}$ - заданный уровень информационных рисков в системе;

$\boldsymbol{C_t}$ - общие затрат на обеспечение информационной безопасности в системе.

В качестве **предлагаемых методов** для решения поставленных задач планируется использовать следующие методы научного исследования:

- сравнительный анализ;
- методы пространственной и временной структуризации системы;
- методы формализации информации разной степени структурированности и обработки данных в системе УИБ;
- методы моделирования сложных систем с неустранимой значительной неопределенностью: методы нечеткого моделирования на основе алгоритмов Мамдани, методы экспертных оценок, методы структуризации типа «дерево целей».

Научная новизна работы заключается в разработке и программной реализации метода управления ИБ в системе на основе предложенных математических моделей, позволяющего синтезировать автоматизированную систему управления ИБ.

Результатом выполнения работы станет математическая модель управления информационной безопасностью, разработанный на ее основе метод управления информационной безопасностью IoT-систем и методика создания автоматизированной системы управления информационной безопасностью.

СПИСОК ЛИТЕРАТУРЫ

1. Суомалайнен А. Интернет вещей: видео, аудио, коммутация. – Litres, 2022.
2. Грингард С. Интернет вещей: Будущее уже здесь. – Альпина Паблишер, 2016.
3. Клипов, Д.Д. Проблемы обеспечения безопасности в IoT [Текст] / Д.Д. Клипов, А.А. Рябцев// 55-я Междунар. науч. конф. «МНСК-2017: Информационные технологии» – Новосибирск, – 2017. – С. 37.
4. Карпова В. В., Балдынюк А. И. Информационные системы торгового предприятия //Актуальные вопросы развития современного общества, экономики и профессионального образования. – 2022. – С. 114-116.
5. Громыко П. С., Осанов В. А. Безопасность интернета-вещей. Проблемы техники и технологий телекоммуникаций ПТиТТ-2020: Материалы XXII Международной научно-технической конференции: материалы конференции. — Самара: ПГУТИ, 2020. — 393 с. — ISBN 978-5-907336-06-3.
6. Ревенков П. В., Бердюгин А. А. Кибербезопасность в условиях Интернета вещей и электронного банкинга //Национальные интересы: приоритеты и безопасность. – 2016. – №. 11 (344). – С. 158-169.
7. Евсютин О. О., Кокурина А. С. Обзор методов встраивания информации в цифровые объекты для обеспечения безопасности в «интернете вещей» //Компьютерная оптика. – 2019. – Т. 43. – №. 1. – С. 137-154.
8. ГОСТ Р ИСО/МЭК 27000-2021 Информационные технологии. Методы и средства обеспечения безопасности, 2021.
9. Методика оценки угроз безопасности информации
10. ГОСТ Р ИСО/МЭК 15408-1-2012 Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий, 2012.

Глозштейн Д. А.
ПГТУ, г. Йошкар-Ола, ст. преподаватель
GlozshtejnDA@volgatech.net

РАЗРАБОТКА И ИССЛЕДОВАНИЕ СИСТЕМЫ КВАНТОВОГО МОНИТОРИНГА ОПТОВОЛОКОННЫХ СЕТЕЙ СВЯЗИ ДЛЯ СИСТЕМ ВИДЕОКОНФЕРЕНЦСВЯЗИ

Аннотация. Проект направлен на реализацию системы квантового мониторинга сети связи. В рамках проекта предполагается разработать и обосновать безопасность системы квантового мониторинга сетевых атак (на физическом, канальном и сетевом уровне), модифицировать современные сетевые протоколы для совместного использования квантовых и классических технологий, а также довести скорость генерации квантового ключа до значений, приемлемых для использования системы для работы ресурсозатратных приложений, в частности, систем видеоконференцсвязи. Основными преимуществами представленных решений является высокая чувствительность системы к попыткам перехвата данных (вплоть до нескольких десятков фотонов), обеспечение устойчивости линии связи к некоторым видам атак (таким как атака с коррелированными помехами и прослушивание волокна),а также значительно более низкие затраты по сравнению с аналогичными решениями за счет использования для передачи квантового сигнала стандартных оптоволоконных сетей связи. Основным практическим результатом проекта является применение квантовых систем обеспечения безопасности в классических сетях. В частности, в проекте обосновывается их применение в системе квантового мониторинга линии связи на физическом уровне, которая может быть широко применимой в классических системах, например, в системе видеоконференцсвязи.

Ключевые слова: видеоконференцсвязь, квантовый мониторинг, квантовые сети, техническая защита информации, безопасность компьютерных сетей, квантовое распределение ключей.

Передача данных при проведении видеоконференций зачастую осуществляется по открытым телекоммуникационным сетям с использованием стандартных протоколов, а, следовательно, они доступны потенциальному нарушителю для проведения различных атак, поэтому исследования проблем обеспечения информационной безопасности видеоконференций приобретают особую актуальность.

Для обеспечения защиты необходимо применение алгоритмов шифрования, которые основаны на секретности ключей. Однако сами способы их распределения между получателем и отправителем могут быть уязвимы к атакам злоумышленников. Поэтому вопрос распределения ключей между пользовательскими устройствами представляет собой значимую научную проблему, решение которой необходимо искать в контексте появления новых технологий и угроз, связанных с созданием квантового компьютера. Известные способы доставки секретных ключей: с помощью доверенного курьера; с помощью алгоритмов с секретным ключом; с помощью схем выработки ключа на основе вычислительно сложных задач, — не позволяют добиться регулярной доставки независимых ключей в условиях нарушителя, обладающего квантовым компьютером и неограниченными вычислительными ресурсами. Алгоритмы с открытым ключом используют в качестве гарантии безопасности вычислительную сложность математических задач, однако использование алгоритмов, реализуемых на квантовом компьютере, ставит под сомнение эффективность такого подхода.

Перспективным решением проблемы снижения стойкости современных криптографических протоколов является использование квантовых технологий. Актуальность применения квантовых технологий определяется значительно более высоким уровнем стойкости алгоритмов к атакам злоумышленников за счет принципиально иного подхода к обеспечению безопасности, который основывается не на математической сложности задач, решаемых в классических протоколах шифрования, а на принципиальной невозможности воссоздать квантовое состояние при попытке получения его значения (теорема об отсутствии клонирования). Теоретически обосновано, что квантовое распределение ключей гарантирует невозможность вскрытия ключа. Таким образом, актуальность проведенного исследования состоит в необходимости решения задачи организации работы коммуникационных сетей на основе классических каналов связи, безопасность которых обеспечивается квантовыми технологиями, в частности, для систем видеоконференцсвязи.

Целью исследования является повышение эффективности защиты системы видеоконференцсвязи, адаптированной к существующим стандартам сетей передачи данных и готовой к применению на современном оборудовании.

Для достижения поставленной цели необходимо решить следующие **задачи**:

1. Выполнить исследование существующих решений в области организации видеоконференцсвязи;
2. Выполнить исследование квантовых технологий и способов их применения в сетях передачи данных в целом, и для систем видеоконференцсвязи в частности;
3. Предложить метод внедрения квантовых технологий защиты информации в существующую сетевую инфраструктуру без кардинальных изменений самой инфраструктуры;
4. Разработать структуру системы видеоконференцсвязи, использующую квантовую технологию защиты информации;
5. Разработать новый алгоритм расширения квантового ключа для поддержки соответствующей скорости и качества передачи данных в рамках системы видеоконференцсвязи при сохранении достаточного уровня безопасности передаваемых данных;
6. Модифицировать существующие протоколы передачи данных для работы с квантовыми методами передачи информации;
7. Выполнить математическое обоснование безопасности и качества передачи данных в предложенной систем;
8. Разработать интерфейс, обеспечивающий взаимодействие между квантовой технологией на физическом уровне и оператором системы видеоконференцсвязи на прикладном;
9. Провести экспериментальную проверку системы на устойчивость от стандартных атак на безопасность передаваемых данных.

Объектом исследования данной работы являются методы обеспечения безопасности систем видеоконференцсвязи. Предметом исследования являются системы видеоконференцсвязи, использующие квантовые технологии для повышения безопасности передаваемых данных.

При анализе современного состояния исследований в данной сфере стоит отметить, что работы в области видеоконференцсвязи проводятся в основном зарубежными учеными: C. Zhou, W. Feng, Z. Zhou, X. Tian, J. Tian, J. Li, J. Wang, W. Wu, L. Chen, W. Simpson, H. Yan, Z.

Sun, L. Zhang, H. Yuan, S. Braun, J. Taylor, B. Furht, SW. Smoliar, H. Zhang, Z. Kang, L. Yian-Feng, а также A. Mishra, J. Rosenberg, E. A. Walter, H. Xu, Y. Zhou, M. N. Thapa [8,9,10,11].

В работах отечественных авторов Синепола В.С., Кривошеи Д.О., Тупицына В.В., Савельева А.И., Прохорова В.В., Манаковой И.П., Старикова С.С., Кузнецова А.А., Семенова С.Г., Симоненко С.Н., Мелешко Е.В., Кизина В.С., Новикова С.Н., Яковлева Р.Н., предложены способы повышения надежности видеоконференцсвязи [3]. Однако все исследования связаны с работой классических систем видеоконференцсвязи и не учитывают расширяющиеся возможности современных квантовых компьютеров.

В области квантовых коммуникаций активно разрабатываются и изучаются протоколы квантового распределения ключей (КРК). Физика квантовой передачи информации описана в работах D. Baumester, A. Jekert, A. Cajlinger. Неоспоримый вклад в развитие технологии КРК внесли Ch. Bennett и G. Brassard, предложив первый протокол КРК ВВ84. В дальнейшем протокол был доработан самими авторами в более простой и применимой модификации В92 (Ch. Bennett). Впоследствии A. Jekert разработал протокол Е91, алгоритм которого обеспечивает мониторинг безусловной безопасности благодаря использованию состояний ЭПР (Эйнштейна-Подольского-Розена). Значительно повысить скорость передачи и надежность квантового канала удалось в протоколе Lo05 (H.K. Lo, X. Ma, K. Chen), основанном на определении частоты ошибок сигнала. Впоследствии та же группа исследователей предложила детектор-независимое КРК, которое подразумевает использование недоверенных узлов при передаче, что повышает устойчивость к атакам на квантовый канал и кратно увеличивает расстояние передачи. Кроме того, было предложено более устойчивое к шумам многомерное КРК (J. Mower, Z. Zhang, P. Desjardins), которое позволяет разрабатывать решения для беспроводных квантовых сетей доступа.

Исследованиями протокола КРК на основе полей-близнецов (TF-QKD) и его применением при передаче данных на большие расстояния занимается ряд лабораторий в Китае под руководством X-H. Tian, J-N.Zhang, X. Jiang и др. Разработку детектор-независимой модификации протокола (MDI-QKD) прорабатывают M. Curty, V. Zapatero, D.P. Nadlinger, B.C. Nichol, M. Ioannou, S. DiAdamo T. Van Leent и др. [4,6,7]. Проблемы квантовой коммуникации на основе запутанности фотонов в своих работах развивают Y.-G. Yang, G.-D.Gao, J. Liu, N. Zou, N. Leone и др. Существенный вклад в изучение применения технологии КРК в сетях смешанных топологий внесли N. Lütkenhaus, M. Mosca. В российском научном дискурсе вопросами применения квантовых технологий в передаче данных занимаются А.В. Козубов, А.А. Гайдаш, А.В. Глейм, Г.П. Мирошниченко, А.Е. Жиляев, Т.Ф. Камалов, А.В. Борисова и др. [1,2,5].

Для преодоления ограничения длины квантового канала аппаратура КРК объединяется в так называемые сети КРК с доверенными промежуточными узлами. При данном подходе квантовые ключи вырабатываются только между узлами сети, соединенными напрямую квантовым каналом. На прочие узлы квантовой сети (УКС) одни квантовые ключи передаются под защитой других выработанных квантовых ключей.

Все существующие решения в области квантовых коммуникаций обладают рядом общих, сложно разрешимых на данный момент недостатков. С теоретической точки зрения все протоколы КРК не являются достаточно надежными, так как при росте расстояния передачи данных растет уровень ошибок приема квантового сигнала, что значительно усложняет определение действий злоумышленника в сети. Кроме того, математически обоснованы и физически показаны ряд сетевых атак на квантовые коммуникации, которые

приводят либо к утрате данных, либо к получению злоумышленником квантово распределенного ключа. Важным недостатком является тот факт, что практически все современные безопасные алгоритмы КРК рассчитаны на крайне низкую скорость генерации квантового ключа. Весьма значимым нерешенным вопросом остается практическая реализация квантовых технологий. Значительно усложняет внедрение квантовых методов защиты информации и то, что для их использования требуется дополнительный канал квантовой связи, что еще больше увеличивает затраты на внедрение квантовых коммуникаций. В связи с этим становится очевидно, что необходима разработка эффективных способов применения квантовых технологий в построении реальных коммуникационных сетей. В частности, одной из актуальных задач является применение квантовых технологий для организации защищенной видеоконференцсвязи, а также разработка схемы организации сетевого взаимодействия в рамках сеанса видеоконференцсвязи на программном и аппаратном уровнях.

В исследовании применяется ряд классических научных методов. В частности, с помощью метода системного анализа формируется комплексная концепция построения системы защищенной видеоконференцсвязи на всех уровнях сетевого взаимодействия. Методы математического моделирования необходимы для построения системы квантового распределения ключей и математического обоснования безопасности используемых протоколов передачи данных. Методы теории защиты информации являются фундаментальной основой исследований и необходимы для рассмотрения устойчивости рассмотренной системы видеоконференцсвязи к деструктивным воздействиям. Методы теории кодирования используются при построении системы квантового мониторинга передаваемого сигнала на физическом уровне. Методы теории квантовой физики необходимы для обоснования основ работы квантово-защищенной системы связи с применением квантового распределения ключей.

Исследование основано на функционально-ориентированном и предметно-ориентированном подходах. При первом подходе применяется последовательная декомпозиция проблемы на отдельные, достаточно простые составляющие, обладающие функциональной определённостью. В частности, задача обеспечения безопасности сетевого взаимодействия между объектами системы видеоконференцсвязи должна быть разложена по уровням сетевого взаимодействия, на каждом из которых применяются свои требования и протоколы, обеспечивающие защиту информации. При использовании второго подхода формируются абстрактные модели реальных объектов, которые позволяют создать оптимальные (субоптимальные) системы, устанавливающие взаимосвязи между функциональными объектами (субъектами). Так, например, для математического обоснования безопасности выбранного протокола квантового распределения ключей необходимо построить математическую модель, позволяющую оценить степень сложности и вероятность успешного проведения атак на квантово-защищенную систему.

Научную новизну проводимых исследований и ожидаемых результатов работы можно изложить в следующих тезисах:

1. Предполагается разработать структуру системы видеоконференцсвязи с использованием квантовых технологий защиты информации, отличающуюся от известных систем использованием квантового мониторинга на физическом уровне, позволяющей обеспечить необходимый уровень безопасности при передаче данных.

2. Предлагается новый метод встраивания квантового ключа в поток данных

классической сети, отличающийся использованием генератора случайных чисел, что позволяет замаскировать сам факт использования квантовых технологий при организации системы видеоконференцсвязи.

3. Планируется определить новый алгоритм расширения квантового ключа для поддержки соответствующей скорости и качества передачи данных в рамках системы видеоконференцсвязи при сохранении достаточного уровня безопасности.

4. Разрабатывается математическая модель обоснования безопасности применения квантовых технологий в системах видеоконференцсвязи, построение которой позволяет доказать необходимую степень защищенности системы для её применения в прикладных целях.

Результаты данной работы с научно-теоретической точки зрения представляют развитие теории защиты информации в области применения квантовых технологий для обеспечения безопасности и систем КРК для доставки общих секретных ключей, в частности, в системах видеоконференцсвязи.

Практическую значимость результатов исследования можно представить более комплексно. Схема защиты передаваемых данных на физическом уровне с помощью системы квантового мониторинга позволит распознавать любые попытки воздействия на канал передачи данных. Для повышения защищенности системы и обеспечения целостности передаваемых сигналов, а также для снижения общей стоимости системы будут выработаны подходы к внедрению квантовых технологий защиты информации в существующую сетевую инфраструктуру. Для повышения скорости передачи данных с использованием квантового распределения ключей будет применен алгоритм расширения квантового ключа, что позволит обеспечить требуемую скорость передачи данных для сохранения качества передаваемых материалов в сеансе видеоконференцсвязи. Реализованная схема видеоконференцсвязи обеспечит надежную защиту целостности данных на физическом уровне при сохранении качества передаваемых данных. Кроме того, основные результаты исследования представляют практическую ценность для обеспечения безопасности любых систем, использующих сети передачи данных. Предложенные модификации современных протоколов передачи данных и оборудования позволят практически безболезненно внедрить данную систему в существующую инфраструктуру оптоволоконных сетей. Разработанный программный продукт, реализующий интерфейс оператора системы видеоконференцсвязи и системы квантового мониторинга, с помощью которого можно автоматически контролировать целостность передачи данных, обеспечит удобство использования квантовых методов защиты информации.

В исследовании выявляются и исследуются решения научных проблем, препятствующих применению квантовых методов обеспечения безопасности информации в системах видеоконференцсвязи. Схема системы видеоконференцсвязи с использованием квантовых технологий защиты информации, использующая квантовые технологии защиты информации на нескольких уровнях сетевого взаимодействия, обеспечит достаточный уровень безопасности при работе системы. Предложенный комплекс устройств может быть использован в качестве базового элемента для построения более сложных и обширных систем видеоконференцсвязи.

Основным практическим результатом проекта является применение квантовых систем обеспечения безопасности в классических сетях. В частности, в проекте обосновывается их применение в системе квантового мониторинга линии связи на физическом уровне, которая

может быть широко применимой в классических системах, например, в системе видеоконференцсвязи. Это отменяет необходимость прокладки специальных квантовых линий связи и значительно снижает затраты на их внедрение в классические системы коммуникаций. Кроме того, предложенные в проекте решения дают возможность применения квантовых коммуникаций в совокупности с ресурсозатратными приложениями, в частности, при использовании видеоконференцсвязи, требующего высокого качества передаваемых данных.

Работа может стать основой для дальнейших разработок в применении квантовых технологий для обеспечения информационной безопасности на более высоких уровнях сетевого взаимодействия.

Список литературы

1. Чистяков В.В., Гайдаш А.А., Козубов А.В., Глейм А.В. Исследование интерференции слабых когерентных многомодовых состояний для задач квантовой коммуникации с недоверенным приемным узлом // Научно- технический вестник информационных технологий, механики и оптики. — 2019. — №6 (19). — с. 966-972.

2. Кынев С.М., Чистяков В.В., Иночкин М.В., Анисимов А.А. Квантовые коммуникации на боковых частотах на основе отечественной элементной базы для волоконных линий связи // Фотон-экспресс. — 2021. —№6 (174). — с. 216.

3. Стариков С.С., Кель О.Л., Вольхин И.Л. Измерение шумов волоконно-оптических источников излучения // Вестник ПГУ. Физика. — 2019. — №1. — с. 66-73.

4. Ioannou M. et al. Receiver-Device-Independent Quantum Key Distribution. arXiv:2104.14574v3 [quant-ph]. — 2022. — p. 6-20.

5. Kozubov A., Gaidash A., Miroshnichenko G. Finite-key security for quantum key distribution systems utilizing weak coherent states. //arXiv:1903.04371. — 2019 — .

6. Lo H.-K., Curty M., Qi B. Measurement-Device-Independent Quantum Key Distribution // Physical Review Letters. — 2012. — V. 108. N 13. — P. 130503. doi:10.1103/PhysRevLett.108.130503

7. Mandil R., DiAdamo S., Qi B., Shabani A. Quantum key distribution in a packet-switched network. arXiv:2302.14005v1 [quant-ph]. 2023.

8. Wu W. P2P-based video conferencing security management strategy /W. Wu, B. Ej // International Conference on Multimedia Technology. - 2018.

9. Xu, F. Secure quantum key distribution with realistic devices. / F. Xu, X. Ma, , Q. Zhang, H.-K. Lo, J.-W.Pan, // Rev. Mod. Phys. — 2020. — №92. — pp. 61-69.

10. Zhang Z., Zhuang Q., Shapiro J. Experimental Quantum Key Distribution at 1.3 Gbit/s Secret-Key Rate over a 10-dB-Loss Channel. arXiv:1712.04973v1 [quant-ph] 2017.

11. Zhu, D.; Zheng, J.; Zhou, H.; Wu, J.; Li, N.; Song, L. A Hybrid Encryption Scheme for Quantum Secure Video Conferencing Combined with Blockchain. Mathematics 2022, 10, 3037. https:// doi.org/10.3390/math10173037.

Джуров А.А.
Донской Государственный Технический Университет, младший научный сотрудник
sashaz1696@yandex.ru

ИНТЕЛЛЕКТУАЛЬНАЯ ИНФОРМАЦИОННАЯ СИСТЕМА МОНИТОРИНГА И АНАЛИЗА КОНТЕНТА WEB-САЙТОВ ДЛЯ БЛОКИРОВАНИЯ ИХ ДЕСТРУКТИВНОГО ВОЗДЕЙСТВИЯ

Аннотация: Большинство программ аналогов работают по принципу хранения в базе данных ссылок на опасные и деструктивные сайты. В настоящее время такой подход устарел, так как базы не всегда актуальны и требуют постоянной актуализации, а скорость создания новых сайтов очень высока. В указанной работе подход по устранению ссылок на опасные и деструктивные сайты устроен таким образом, что на персональный компьютер ребенка/подростка или в организацию (компьютерный клуб и т.д.) устанавливается программа, которая анализирует все, что происходит на мониторе и блокирует то, что считает деструктивным контентом или нежелательной информацией. Данный метод позволяет в реальном времени производить анализ информации на наличие деструктивного контента и блокировать его. Реализация системы будет выполнено на языке программирования Python и библиотек: YOLO v8, Spacy, LDA Gesmi, Vosk.

Результатом работы станет информационная система, позволяющая в реальном времени производить анализ контента на компьютере ребенка/подростка или организации и блокировать деструктивный контент или нежелательную информацию. Указанный проект значим тем, что позволит не только организациям блокировать нежелательную информацию, но и использовать информационную систему для блокировки деструктивного контента в школах, компьютерных классах и на домашних рабочих компьютерах подростков и детей для противостояния призывам к массовым беспорядкам и отрицательному влиянию на их психологическое состояние.

Ключевые слова: деструктивный контент, web-сайт, информационная безопасность, безопасность детей, интеллектуальная система, YOLO, информационная система, анализ контента, технология LDA.

Целью проекта является: разработка интеллектуальной информационной системы мониторинга и анализа контента Web-сайтов с целью блокирования деструктивного контента. Для решения поставленной цели необходимо решать следующие задачи:

– создание программной части для оценки, классификации и блокирования деструктивных текстовых данных;

– создание программной части для оценки и блокирования деструктивных данных в аудио;

– создание программной части для оценки и блокирования деструктивных данных в видео;

– создание программной части для оценки и блокирования деструктивных изображений (включая изображения с деструктивным текстом).

В рамках проекта и диссертационной работы будет сделана система по анализу и блокировке деструктивного контента, которая позволит в дальнейшем блокировать аудио, видео, изображения с деструктивной направленностью. Анализ деструктивного контента в

тексте будет выполнятся с помощью нового метода с использованием технологий LDA и Word2vec. Для анализа обнаруженных объектов на изображении будет использована свёрточная нейронная сеть, обученная по специально подобранным наборам данных – датасетам. Работа, описание системы и тестирование войдет в одну из глав диссертации.

Возникновению активности исследований в области деструктивных сайтов способствовало большое количество детской и подростковой преступности, проявляющейся в школе, колледжах и университетах. В мировой практике не широко распространены исследования деструктивного контента, хотя он и является важным аспектом в защите безопасности граждан. В условиях современной информационной войны, к деструктивному контенту, помимо всего прочего, относится вражеская пропаганда, распространение ложной (фейковой) информации, призывы к террористической и противоправной деятельности, сбор денежных средств в пользу армии противника, и др.

Сложно переоценить роль глобальной сети интернет в жизни современного человека, которое охватило почти все без исключения сферы его деятельности: познавательной, развлекательной, деловой и иных [1,9,10,12-14,16]. На начало 2023 года, количество зарегистрированных сайтов насчитывает 1.13 млрд. и их количество с каждым годом увеличивается.

Уровень разработанности проблемы исследования можно оценить путем анализа трудов, имеющих отношение к тематике функционирования сетей с целью общения и распространения в них вредоносного контента. В данных трудах фигурируют вопросы: подходу фильтрации и идентификации деструктивного контента [2,6] описания опасного контента [5,19], который распространяется в сети; выявления угроз [3]; применения мер и средств противодействия опасной информации [7,20,21]. Однако, несмотря на множество ранее имеющихся трудов, перечисленные выше противоречия остаются неразрешенными.

Исследование деструктивных сайтов находится в центре внимания российских и зарубежных исследователей, при этом в нашей стране аналогичные исследования находятся на начальном этапе. Можно привести некоторые примеры - разбор DLP систем в поисках контента рассматриваются в работе Киздермишова А.А. [4]. Вопросы эффективности блокировки деструктивных групп в социальных сетях представлено в работе Самосват О. И. [15]. Анализ метрики деструктивного контента на видеохостинге рассмотрены Остапенко А.Г. [7], исследовались вопросы применения машинного обучения в процессе поиска деструктивной информации в web– контенте. Разработки отечественных ученых в аспекте фильтрации контента представлены в работе Сидорова Е.А. [17], где рассмотрена фильтрация контента на стороне провайдера. Общим недостатком отечественных исследований является недостаточное состояние изученности проблемы использования DLP системы для поиска и блокирования деструктивных сайтов.

Анализ и решение проблем деструктивного контента были рассмотрены многими авторами, но не все авторы рассматривали работы единой системы для блокировки деструктивного контента. Например, Н. В. Давидюк, В. А. Гостюнина, Д. Р. Байдулова, создали интеллектуальный метод идентификации деструктивных данных в тексте. Алгоритм представляет из себя блокировку ненормативной лексики по словарю.

Данный алгоритм имеет следующие недостатки:

– Использование словаря в системе, что влечет за собой постоянную актуализацию словаря.

– Поиск и блокировка ненормативной лексики, тогда как деструктивный контент не ограничивается только ненормативной лексикой.

– Алгоритм ищет и блокирует только текстовую информацию, но деструктивная информация может быть и в изображениях, видео и т.д.

– Низкая эффективность поиска деструктивного контента.

Одним из аналогов программы могут выступать антивирусы. Основной проблемой любых антивирусов с родительским контролем является – использование базы данных опасных сайтов и защита детей и подростков зависит от актуальной базы данных, что не является плюсом. Вторая основная проблема родительского контроля – родитель сам указывает запрещённые или разрешенные ссылки для ребенка, что тоже не совсем удобно.

Используемые методы для решения указанной проблемы - это технологии нейронных сетей и различных библиотек: YOLO v8 – анализ видео, фото материалов, YOLO V8 была выпущена в начале 2023г. и позволяет в реальном времени с высокой скоростью классифицировать объекты, Spacy – анализ текста, классификация текста, LDA Gesmi – анализ текста, Vosk – преобразование аудио материала в текст. Использование данного стека технологий, позволит реализовать программное средство для полного анализа контента на компьютере. План проводимых исследований включает в себя реализацию модели для блокировки деструктивного контента в тексте (сентябрь 2023-декабрь 2023), реализацию модели для блокировки деструктивного контента в изображениях и видео (декабрь 2023-апрель 2024), реализацию модели для блокировки деструктивного контента в аудиофайлах (апрель 2024-май 2024). Апробацией результатов станет внедрение в компьютерные клубы, школы и для личного использования информационной системы, которая позволит блокировать деструктивный контент в различных формах его информационного представления.

Новизна проекта заключается в том, что предложен новый подход к блокировке деструктивного контента в текстовом формате за счет использования двух последовательно выполняемых блоков программы: распознавание тематики текста (LDA) и с Word2vec — библиотека для получения векторных представлений слов на основе их совместной встречаемости в текстах, если не деструктивный контент, то показываем указанный текст.

Также предложен новый подход к блокировке деструктивного контента в изображениях и видео, за счет нейронной сети для распознавания объектов Yolo v8, способной определять объекты с высокой скоростью в реальном времени. Новизна этого подхода к решению задачи заключается в вычислении вероятности, с которой объект соответствует своему классу, с целью определения категории его классификации.

Будет предложена новая модель для анализа аудиоконтента. На первом этапе работы программы применяются технологии распознавания речи, с открытым исходным кодом и в виде встраиваемых компонентов (Google Speech Recognition; Speech Recognition – SpeechKit; Pocketsphinx; библиотека Vosk; gTTS), позволяющие преобразовывать речевой сигнал в цифровую информацию в виде текстовых данных. Для этого использовано программное обеспечение, поставляемое вместе с операционной системой Windows 10 – CMD и PowerShell.

На втором этапе, заранее распознанные текстовые данные анализируются на наличие деструктивного содержания с помощью технологий обработки естественного языка NLP, и в случае его нахождения, блокируются. В дальнейшем можно расширить языковую базу.

Результатом указанной работы станет интеллектуальная информационная система, которая позволит в реальном времени производить анализ контента как на компьютере

организации, так и компьютере ребенка или подростка и блокировать деструктивный контент (аудио, видео, изображения, текст).

В результате выполнения работы будет реализовано программное средство, позволяющее в онлайн режиме блокировать деструктивный контент во всех формах его проявления в сети (аудио, видео, текстовая информация, изображения). Программное средство будет состоять из 4 модулей, где каждый модуль будет отвечать за анализ и блокировку определенного типа информации. Каждый из модулей будет иметь свои библиотеки для анализа (т.е. использовать различные технологии, нейронные сети). Данная разработка соответствует стратегии НТР РФ перехода к цифровым передовым интеллектуальным технологиям. Апробацией разработанной системы будет внедрение ее в компьютерные клубы, школы, а также личное использование родителей на компьютерах, где работают дети. Система окажет помощь обществу и государству в защите от источников опасности (терроризма и экстремизма. В рамках реализации проекта будут подготовлены свидетельства регистрации программ для ЭВМ.

СПИСОК ЛИТЕРАТУРЫ

1. Воронина, И. Е., Гончаров В. А. Анализ эмоциональной окраски сообщений в социальных сетях (на примере сети "В_Контакте") / И. Е. Воронина, В. А. Гончаров // Компьютерная лингвистика и обработка естественного языка. - 2015. № 4. С. 151 -158.

2. Давидюк, Н. В. Интеллектуальный алгоритм идентификации деструктивной информации в тексте / Н. В. Давидюк, В. А. Гостюнина, Д. Р. Байдулова // Вестник Астраханского государственного технического университета. Серия: Управление, вычислительная техника и информатика – 2019 / DOI: 10.24143/2072-9502-2019-2-29-39.

3. Джуров, А. А. System for detecting of potentially dangerous communications of network users. / А.А. Джуров, Е. А. Ревякина, Л. В. Черкесова, Н. В. Болдырихин, Е. Н. Климова, И. А. Енгибарян //Fundamental and Applied Scientific Research in the Development of Agriculture in the Far East" (AFE-2022). - 2023.

4. Киздермишов А. А., Киздермишова С. Х. К вопросу о вводе в эксплуатацию DLP-систем // Вестник Адыгейского государственного университета. Естественно-математические и технические науки. 2017. №4. С. 128-133.

5. Карданов, А. Р. Экстремистский контент в социальных медиа: анализ основных трендов и мер противодействия / А. Р. Карданов, Д. А. Карданова // Журнал прикладных исследований – 2022 / DOI 10.47576/2712-7516_2022_11_2_169.

6. Мельник, Э.В. Стратегии и технические средства для предотвращения виктимного поведения пользователей в информационном пространстве / Э. В. Мельник, А. Б. Клименко // Известия Тульского государственного университета. Технические науки - 2019.

7. Остапенко, А.Г. Метрики деструктивного контента на видеохостинге YouTybe / А. Г. Остапенко, В. Е. Кунавин, В. С. Сидельников, О. А. Остапенко // Информация и безопасность – 2018 - Том 21. Ч.3 - С. 282-289.

8. Остапенко, А. Г. Модель процессов распространения деструктивного контента в региональном интернет пространстве для сети Facebook / А. Г. Остапенко, А. В. Ещенко, Г. А., Остапенко, К. В. Симонов // Информация и безопасность. - 2018. Том 21. Ч.4. - С. 441-455.

9. Остапенко, А. Г. Организация мониторинга постов социальной сети ВКонтакте с помощью интерфейса VKAPI / А. Г. Остапенко, Е. Р. Нежельский, М. Н. Степанов, Е. Ружицкий, А. В. Заряев // Информация и безопасность. - 2018. Том 21. Ч.3.- С. 407-415.

10. Остапенко, А. Г. Социальные сети и деструктивный контент / А. Г. Остапенко, А. В. Паринов, А. О. Калашников, В. Б. Щербаков, А. А. Остапенко; под общ. ред. Д. А. Новикова // научно-техническое издательство «Горячая линия – Телеком». - 2017. - 276с.

11. Охапкина, Е. П. Идентификация деструктивной информации в социальных сетях на основе модели векторного пространства / Охапкина Е. П., Охапкин В. П., Казарин О. В. // Сборник научных трудов Российской научной конференции. Интеллектуальные системы в информационной конфронтации. -Издательство ФГБО в РГУ им. Г. В. Плеханова Москва. - 2016. - С. 350-360.

12. Пазельская, А. Г. Метод определения эмоций в текстах на русском языке / А. Г. Пазельская, А. Н. Соловьев // Компьютерная лингвистика и интеллектуальные технологии: сборник научных статей. М.: Издательство РГГУ -2011. - 10 (17). - С. 510-522.

13. Паринов, А. В. Социальные сети как среда распространения деструктивного контента / А.В. Паринов, Д.В. Гусев., Е. В. Гусев, В. А. Кургузкин, С. С. Тихонова // Информация и безопасность. - 2017. - Т. 20. - № 1. - С. 5-38.

14. Радько, Н. М. Вирусные эпидемии в информационно-телекоммуникационных сетях: оценка вероятности заражения / Н. М. Радько, Е. Н. Пономаренко, А. О. Калашников, Р. К. Бабаджанов // Информация и безопасность. -2016. - № 1, -Т. 19. - С. 6-23.

15. Самосват, О. И. Эффективность блокировки деструктивных групп в социальных сетях / О. И. Самосват, Т. С. Брежнева, Е. Р. Шмеерова // Вестник Московского государственного областного университета (электронный журнал) - 2020. № 1. ISSN 2224-0209.

16. Сафронова, В. В. Риск-анализ и прогнозирование ареала распространения деструктивного контента в сообществе «МДК» / В. В. Сафронова,К. В. Сибирко, Й. Воришек, В. И. Белоножкин, Л. В. Паринова // Информация и безопасность. - 2018. - Т. 21. - № 3. - С. 399-401.

17. Сидорова, Е. А. Подход к фильтрации запрещенного контента в веб-пространстве / Е. А. Сидорова, И. С. Кононенко, Ю. А. Загорулько // Институт систем информатики имени А. П. Ершова СО РАН, Новосибирский государственный университет, Новосибирск, Россия.

18. Cherckesova, L. V. Development of safety monitor from destructive influences of web-sites and social networks of internet / L. V. Cherckesova, A. A. Zelensky, E. A. Revyakina, O. A. Safaryan, D. A. Korochentsev // E3S Web of Conferences. – 2021. – P. 273.

19. Khachidogov, R. A. Problems of detecting and blocking destructive media content in social networks / R. A. Khachidogov // Journal of Applied Research – 2022/ DOI:10.47576/2712-7516_2022_11_2_161.

20. Parinov A. V. Risk-simulation of processes of distribution of destructive content on social network taking into account its growth / A. V. Parinov, E. A. Shvartskopf V. S., Zarubin A. V. Zariaev N. I. Barannikov // AP - International Journal of Pure and Applied Mathematics. - 2018 - Volume 119 No. 15 - Pp. 2633-2637.

21. Parinov, A. V. Risks of multinetwork world order and monitoring of social networks regarding detection of destructive content / A. V. Parinov, E. S. Sokolova, A.O. Kalashnikov, N. M. Tikhomirov, E. Y Chapurin // AP - International Journal of Pure and Applied Mathematics. - 2018. - Volume 119, № 15. - Pp. 2587-2591.

Логинова А.О.
ФГБОУ ВО МГЛУ, ведущий специалист отдела информационной безопасности Департамента цифрового развития
a.loginova@linguanet.ru

РАЗРАБОТКА МЕТОДИКИ ОБНАРУЖЕНИЯ ИНТЕРНЕТ-БОТОВ НА ОСНОВЕ АНАЛИЗА ЛИНГВИСТИЧЕСКИХ ХАРАКТЕРИСТИК СООБЩЕНИЙ

Аннотация: В настоящем исследовании проводится анализ лингвистических характеристик сообщений реальных пользователей интернет-средств массовой коммуникации (далее – интернет-СМК) и интернет-ботов, имитирующих их поведение. На основе результатов проведённого анализа выявляются демаскирующие признаки сообщений социальных интернет-ботов. Оценивается перспектива обнаружения аккаунта социального интернет-бота по лингвистическим характеристикам публикуемых им сообщений. По результатам настоящего исследования будет предложен новый подход к обнаружению интернет-ботов в интернет-СМК, основанный на выявлении лингвистических демаскирующих признаков социальных интернет-ботов в сообщениях пользователей.

Ключевые слова: информационно-психологическая безопасность, социальные интернет-боты, демаскирующие признаки интернет-бота, квантитативный анализ коротких электронных сообщений, структурно-вероятностная модель сообщения социального бота, интернет-средства массовой коммуникации.

Сегодня использование механизмов информационного воздействия на социум становится неотъемлемой частью ведения не только пропагандистской деятельности противоборствующих политических лагерей, но также и боевых действий в целом. Эксперты отмечают возросшую роль информационных операций в киберпространстве. [1, 2] В настоящем исследовании социальные интернет-боты рассматриваются как один из инструментов дезинформации, дискредитации соперников политической гонки.

Цель диссертационного исследования: разработка качественно новой методики обнаружения социального интернет-бота, основанной на лингвистическом анализе коротких электронных сообщений пользователей в интернет-средстве массовой коммуникации.

Для достижения поставленной цели в ходе настоящего исследования необходимо решить следующие задачи:

1) провести квантитативный и сравнительный анализ корпусов текстов, составленных из текстов, авторства людей, и корпуса текстов, составленного из коротких электронных сообщений интернет-ботов, в политическом дискурсе;

2) разработать структурно-вероятностную модель сообщения социального интернет-бота;

3) упорядочить установленные признаки сообщений, принадлежащих интернет-ботам по значимости [3];

4) разработать методику обнаружения интернет-ботов на основе анализа лингвистических характеристик сообщений;

5) представить программную реализацию методики обнаружения интернет-ботов на основе анализа лингвистических характеристик сообщений;

6) провести оценку эффективности разработанной методики обнаружения интернет-ботов на основе анализа лингвистических характеристик сообщений.

Гипотеза настоящего исследования заключается в том, что сообщения социальных интернет-ботов в политическом дискурсе отличаются от сообщений людей частотой использования тех или иных токенов, единиц языка, [1] но также сгенерированные сообщения ботов преимущественно состоят из словосочетаний официальных лиц, в адрес некоторых лиц, событий или явлений, в отношении которых ведётся пропаганда, дезинформация или другие виды информационно-психологического воздействия [4].

Новизна исследования заключается в следующем:

– переоценивается значимость токенов, используемых для атрибуции текстов коротких электронных сообщений людей [5], для обнаружения аккаунтов интернет-ботов в социальной сети;

– устанавливаются признаки сообщений интернет-ботов в социальной сети;

– на основе выделенных признаков формируется качественно новая методика обнаружения социального интернет-бота, основанная на лингвистическом анализе коротких электронных сообщений пользователей социальной сети;

– представляется программная реализация качественно новой методики обнаружения социального интернет-бота.

Проведенный анализ подходов к обнаружению интернет-ботов оказал, что существующие методики направлены на выявление класса вредоносных ботов, из которого реальную угрозу представляют социальные боты, имитирующие поведение человека. [6, 7] Описанные в работах подходы к обнаружению автоматических или автоматизированных социальных акторов основаны на выявлении групп признаков, проявляющихся в:

а) оформлении страницы аккаунта социальной сети, который управляется ботом. Примером реализации алгоритма обнаружения интернет-ботов по специфике контролируемого ботом аккаунта - InstaHero, предназначенную для анализа подписчиков аккаунта, поиска и удаления ботов из числа подписчиков в социальной сети Instagram[1]. Пользователю программного обеспечения предлагается проверить свой аккаунт в социальной сети Instagram на наличие подписчиков-ботов по наличию фото профиля (аватара), языку профиля, возрасту, дате последней публикации на странице аккаунта. Аналогичный алгоритм поиска ботов среди подписчиков аккаунта в социальных сетях Вконтакте и Instagram применяется в программе SocialKit.

б) активности аккаунта: количестве сообщений, отправляемых за единицу времени, времени отправки сообщений, количестве пользователей, получивших/прочитавших сообщение, графам пользовательского поведения [8 – 12];

в) пересечении вышеуказанных групп признаков [13 – 17].

Работы, посвящённые обнаружению интернет-ботов по содержательной части электронного сообщения в открытых источниках опубликованы не были. При этом разработка методики обнаружения ботов по лингвистическим характеристикам признакам сообщений возможна, на что указывает ряд исследований, направленных на решение задачи атрибуции текстов коротких электронных сообщений интернет-пользователей в социальных сетях. [6]

Теоретической базой для исследования послужат работы по идентификации пользователей по содержательной части электронных сообщений в социальных сетях.

[1] Социальная сеть Instagram запрещена на территории РФ

Разработкой данной проблемой занимались А.А. Воробьева [5], М.Е. Сухопаров [18]. Примером реализации алгоритма обнаружения интернет-ботов на основе графов пользовательского поведения является программа GetPapasBot предназначена для работы в социальной сети Instagram[2]).

Предлагаемые методы и подходы к решению поставленных задач приводятся в табл. 1.

Табл.1. Предполагаемые методы и подходы к решению задач настоящего исследования

№ п/п	Научная задача	Методы исследования, этапы реализации проекта
1.	провести квантитативный и сравнительный анализ корпусов текстов, составленных из текстов авторства людей, и корпуса текстов, составленного из коротких электронных сообщений интернет-ботов, в политическом дискурсе;	– *создать корпуса* текстов электронных сообщений людей в социальной сети; – *создать корпус* текстов коротких электронных сообщений социальных ботов в социальной сети; – *выдвинуть статистические гипотезы*; – *провести анализ* употребляемости токенов в корпусах текстов людей и ботов; – *проверить выдвинутые статистические гипотезы*
2.	разработать структурно-вероятностную модель сообщения социального интернет-бота	– *сравнить результаты* а*нализ* употребляемости токенов в корпусах текстов людей и ботов; – *разработать модель* сообщения интернет-бота
3.	упорядочить установленные признаки сообщений, принадлежащих интернет-ботам по значимости	– *рассчитать весовые коэффициенты* лингвистических признаков сообщения интернет-бота
4.	разработать методику обнаружения интернет-ботов на основе анализа лингвистических характеристик сообщений пользователей социальной сети	– разработать методику обнаружения интернет-ботов путём *синтеза результатов,* полученных на более ранних этапах исследования
5.	представить программную реализацию обнаружения интернет-ботов на основе анализа лингвистических характеристик сообщений;	– *программное моделирование* методики обнаружения интернет-бота
6.	*провести оценку* эффективности разработанной методики обнаружения интернет-ботов на основе анализа лингвистических характеристик сообщений	

[2] Социальная сеть Instagram запрещена на территории РФ.

Ожидаемые научные результаты: разрабатываемая методика обнаружения интернет-ботов на основе анализа лингвистических характеристик сообщений и её программная реализация в целом способствуют достижению цели направления «Информационная безопасность» Национальной программы «Цифровая экономика Российской Федерации», а именно достижения состояния защищенности личности, общества и государства от внутренних и внешних информационных угроз. В современном мире всё большее применение находит практика информационного воздействия, поэтому реализация информационной функции государства неразрывно связана с обеспечением внутренней и внешней информационной безопасности, а также информационно-психологической безопасности личности и общества в целом.

Планируемые к получению результаты исследования могут быть включены в учебный процесс по подготовке специалистов уровня бакалавр (направление подготовки 10.03.01 Информационная безопасность «Организация и технология защиты информации») и уровня магистр (направление подготовки 10.04.01 Информационная безопасность профиль «Информационная безопасность в международном сотрудничестве») в курс дисциплины по организационно-правовым основам обеспечения информационной безопасности, современным информационным технологиям.

СПИСОК ЛИТЕРАТУРЫ

1. Логинова А. О. Обнаружение интернет-бота по структурно-вероятностной модели электронного сообщения / А. О. Логинова // Вестник Воронежского института МВД России. — 2022. — №3. — С. 105 – 114.
2. Киберпространство стало новым местом ведения боевых действий — глава Microsoft [Электронный ресурс] — Режим доступа: https://www.securitylab.ru/news/531785.
3. Логинова, А. О. Перспектива использования лингвистических характеристик текстов сообщений для обнаружения социального интернет-бота / А. О. Логинова // Международная научно-практическая конференция по компьютерной и информационной безопасности (INFSEC 2023). — Екб.: ООО «Институт цифровой экономики и права», 2023. — С. 82– 86.
4. Логинова А. О. Выявление демаскирующих признаков социального бота на синтаксическом уровне генерируемого сообщения / А.О. Логинова, Д. В. Алейникова // Вестник Воронежского государственного университета. Серия: Системный анализ и информационные технологии. — 2023. — №1. — С. 139 – 147.
5. Воробьева, А. А. Методика идентификации Интернет-пользователя на основе стилистических и лингвистических характеристик коротких электронных сообщений [Текст] : дис. … канд. тех. наук: 05.13.19 : защищена 14.07.2017 / Воробьева Алиса Андреевна. — СПб, 2017. — 154 с.
6. Логинова, А. О. Анализ существующих подходов к классификации и типологии ботов / А. О. Логинова // Инновационные технологии: теория, инструменты, практика. – Пермь: ПНИПУ, 2020. — Т. 1. — С. 462– 467.
7. Логинова А. О. Подходы к обнаружению социальных интернет-ботов / А. О. Логинова // Информация и безопасность. — 2022. — Т. 25. — ВЫП. 2. — С. 201 – 208.
8. Efthimion P. G. Supervised Machine Learning Bot Detection Techniques to Identify Social Twitter Bots / P. G. Efthimion, S. Payne, N. Proferes // SMU Data Science Review. — 2018. — Vol.1.— № 2. — Article 5.

9. Minnich A. BotWalk: Efficient Adaptive Exploration of Twitter Bot Networks / A. Minnich, N. Chavoshi , D. Koutra , A. Mueen // IEEE/ACM International Conference on Advances in Social Networks and Mining. – 2017. — Doi.org/10.1145/3110025.3110163/.
10. Кочкаров А. А. Выявление ботов в социальных сетях на примере LiveJournal / А. А. Кочкаров, Н. В. Калашников, Р. А. Кочкаров // Мир новой экономики. — 2020. — № 14(2). — С. 44 – 50.
11. Менщиков А. А. Метод обнаружения веб-роботов на основе анализа графа пользовательского поведения / А. А. Менщиков, Ю. А. Гатчин // Программные продукты и системы. — 2019. — Т. 32. — № 4.
12. Чесноков, В. О. Алгоритмическое и программное обеспечение анализа графов ближайшего окружения для выявления ботов и определения неуказанных атрибутов пользователей в онлайновых социальных сетях [Текст] : дис. ... канд. тех. наук: 05.13.11 : защищена 27.02.2019 / Чесноков Владислав Олегович. — М., 2018. — 200 с.
13. Santia G. C. Detecting Social Bots on Facebook in an Information Veracity Context / G. C. Santia, M. I. Mujib, J. R. Williams // Proceedings of the International AAAI Conference on Web and Social Media. — 2019. — 13 (01). — P. 463 – 472.
14. Bebensee B. Leveraging node neighborhoods and egograph topology for better bot detection in social graphs / B. Bebensee, N. Nazarov, B-T. Zhang // Social Network Analysis and Mining. — 2021.— 11:10. — P.1–14.
15. Менщиков А. А. Алгоритм и методика обнаружения и противодействия веб-роботам / А. А. Менщиков, Ю. А. Гатчин // Научно-технический вестник Поволжья. — 2019. — № 6. — С. 141–143.
16. Менщиков А. А. Метод обнаружения веб-роботов на основе семантического анализа посещенных страниц / А. А. Менщиков, Ю. А. Гатчин // Вестник компьютерных и информационных технологий. — 2019. — № 12 (186). — С. 40–45.
17. Менщиков, А. А. Методы обнаружения и противодействия автоматизированному сбору информации с веб-ресурсов [Текст] : дис. ... канд. тех. наук: 05.13.19 / Менщиков Александр Алексеевич. — М., 2019 — с. 265.
18. Сухопаров, М. Е. Методика идентификации пользователей порталов сети Интернет на основе методов математической лингвистики [Текст] : дис. ... канд. тех. наук: 05.13.19 : защищена 30.12.2015 / Сухопаров Михаил Евгеньевич. — СПб, 2015 — с. 108.

Любухин А.С.
РГЭУ (РИНХ), аспирант,
r.vv2020@mail.ru

МЕТОДИКА ОЦЕНКИ ИНФОРМАЦИОННЫХ РИСКОВ ПРИ ПРОВЕДЕНИИ АУДИТА БЕЗОПАСНОСТИ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ

Аннотация: Проблема оценки информационных рисков объектов критической инфраструктуры является актуальным вопросом научного исследования в сфере информационной безопасности. В данном материале анализируется проект по разработке методики оценки информационных рисков объектов критической инфраструктуры, исходя из анализа результатов теоретических исследований и публикаций. Автором определены цель и задачи исследования, а также ожидаемые результаты, научная новизна и используемые научные методы. Также в материале содержатся сведения о научном заделе автора по рассматриваемой проблеме с кратким обзором научных наработок.

Ключевые слова: информационные риски, оценка рисков, аудит безопасности, объекты критической информационной инфраструктуры, методы экспертных оценок и нечеткой логики, модель оценки информационных рисков, критерий функциональной полноты.

Решение проблемы оценки рисков информационной безопасности для объектов критической информационной инфраструктуры (КИИ) в современных условиях является весьма актуальной задачей, обусловленной глобальными изменениями миропорядка и геополитической ситуации в связи с событиями февраля 2022 года. С этого момента атаки на государственные ресурсы РФ стали все более частым и сложнопостроенным явлением, направленным на реализацию на практике деструктивного воздействия на ресурс для нарушения конфиденциальности, целостности и доступности защищаемой информации, от которой зависит безопасность государства.

Хакерские атаки на информационные ресурсы нашей страны трансформировались с коммерциализированных в межгосударственные, направленные на снижение имиджа государства, запугивание и иные деструктивные явления и события. Данные явления, в том числе, побудили к нормативно-правовым трансформациям, к которым можно отнести изменения и в законодательстве о защите критической инфраструктуры, и запрет на использование в ближайшей перспективе иностранного программного и аппаратного обеспечения, и создание Межведомственной комиссии при Совете Безопасности РФ для достижения технологического суверенитета, который является неотъемлемой частью факторов, оказывающих существенное влияние на систему национальной безопасности в целом и безопасность критической информационной инфраструктуры в частности. Данные вопросы детально проанализированы автором проекта и представлены в виде публикаций и выступлений на конференциях [1-3].

Переход к передовым цифровым, интеллектуальным производственным технологиям, роботизированным системам, новым материалам и способам конструирования, создание систем обработки больших объемов данных, машинного обучения и искусственного интеллекта сопоставимы с направлениями Стратегии научно-технологического развития Российской Федерации и федеральных проектов. Автоматизация процесса оценки информационных рисков при проведении аудита безопасности объектов критической

информационной инфраструктуры является актуальной задачей, которая соотносится с вышеописанным направлением, приоритетным для государства.

Крайне важно рассматривать проблему оценки информационных рисков КИИ при проведении аудита безопасности как составную часть общей системы информационной безопасности, что четко прослеживается в [4-8]. Причины возникновения рисков информационной безопасности на объектах КИИ, актуальные методики оценки информационных рисков, анализа механизмов и особенностей проведения аудита безопасности, анализ процесса управления информационными рисками, представлены в исследованиях [9-13].

Неотъемлемым элементом исследования является формулировка понятия «информационного риска», которое включает в себя среди прочего и понятие «угроза информационной безопасности». Следовательно, существенным дополнением, необходимым для полноценного исследования является Методика оценки угроз безопасности информации [14], анализ которой позволяет сформировать основные источники информационных рисков для защищаемых объектов.

Анализ нормативных документов, регламентирующих оценку и управление рисками, показал, что наиболее известными и используемыми являются международные и российские стандарты [15-19], которые содержат руководство по оценке риска опасных событий для включения в реестр риска, технологии оценки рисков и особенности менеджмента рисков, включая терминологию и основные принципы. Это позволило сформировать единую картину рассматриваемой проблемы и структуру управления рисками в качестве основы научного исследования [20, 21]. Анализ ситуации в технологической сфере РФ, геополитической картины мира, а также литературных источников, посвященных исследованиям в области оценки информационных рисков доказывает очевидность необходимости проведения дополнительных исследований в области оценки информационных рисков объектов КИИ.

Целью исследования является оптимизация процесса оценки информационных рисков путем разработки более совершенной методики оценки информационных рисков с использованием характеристик и особенностей научного метода функциональной полноты, использованием которого анализируется в [22-23]. .

Для достижения поставленной цели необходимо решить следующие задачи:

1. Анализ теоретико-понятийного аппарата вопроса оценки информационных рисков, аудита безопасности и сферы КИИ;

2. Исследование нормативно-правового обеспечения защиты объектов КИИ, аудита безопасности и менеджмента рисков;

3. Анализ существующих методик оценки информационных рисков с выявлением основных достоинств и недостатков;

4. Построение концептуальной модели оценки информационных рисков и сопутствующих процессов с теоретическим обоснованием выбора инструментария моделирования;

5. Анализ сформированных концептуальных моделей и подготовка информационно-методического обеспечения исследования;

6. Обоснование целесообразности использования метода функциональной полноты для оценки информационных рисков как одного из этапов оценки разрабатываемой методики;

7. Анализ способов формирования входных данных для оценки информационных рисков;

8. Разработка механизма оценки рисков с помощью критерия функциональной полноты;

9. Автоматизация процесса оценки рисков программными средствами;

10. Теоретическое обоснование и анализ эффективности применения результата исследования

Основная идея научного исследования заключается в разработке методики оценки информационных рисков путем комбинирования методов экспертных оценок, нечеткой логики и функциональной полноты на основе анализа публикаций российских ученых [24-28]. Научным заделом в данных вопросах является теоретический анализ применения нечеткой логики для оценки информационных рисков, опубликованный автором в журнале из перечня ВАК [29].

Для полноценного устранения проблемы оценки рисков требуется формирование теоретико-методологической базы исследование в виде комплекта концептуальных моделей процесса оценки информационных рисков и сопутствующих процессов (категорирование критически важных объектов, аудит безопасности, категории объектов КИИ), фрагмент которого представлен в [30] с последующим их анализом,

Научная новизна исследования заключается в разработке методики оценки информационных рисков объектов критической инфраструктуры с использованием критерия функциональной полноты с возможностью автоматизации вычисления величины риска информационной безопасности. Использование метода функциональной полноты в ходе реализации новой методики позволит исключить такие недостатки как:

- субъективность экспертов при проведении оценки рисков;
- недостаточная точность вычислений результатов оценки рисков;
- высокие трудозатраты;
- необходимость большого количества высококвалифицированных специалистов в области информационной безопасности;
- длительный процесс оценки рисков.

Результатом научного исследования является методика оценки информационных рисков с использованием критерия функциональной полноты с теоретико-практическими результатами апробации разработки, включая программную реализацию процесса оценки рисков, а также комплект моделей процессов оценки рисков и категорирования критически важных объектов в качестве информационного сопровождения процесса оценки рисков.

Результат может быть применен для оценки информационных рисков критически важных объектов, а также, впоследствии, может быть адаптирован для оценки рисков других информационных систем. Также материалы исследования могут использоваться в качестве практического пособия при обучении студентов направления «Информационная безопасность» для формирования у них практических навыков оценки информационных рисков.

СПИСОК ЛИТЕРАТУРЫ

1. Любухин, А. С. Основные тенденции и проблемы развития правового регулирования информационной безопасности РФ (на примере критической информационной инфраструктуры) / А. С. Любухин // Молодежная инициатива - 2023 : Сборник статей Городской научно-практической конференции, Ростов-на-Дону, 17–18 марта 2023 года / Под редакцией С.А. Литвиновой, И.А. Хашева, С.Л. Нужнова, Д.С. Труханович, М.Н. Ашировой. – Ростов-на-Дону: ЮРИУФ РАНХиГС, 2023. – С. 157-163.

2. Любухин, А. С. Трансформации в нормативно-правовом регулировании сферы критической информационной инфраструктуры в условиях внешних рисков / А. С. Любухин // Старт в науке 2022 : Сборник статей Международного научно-исследовательского конкурса. В 2-х частях, 30 мая 2022 года. Том Часть 2. – Петрозаводск: МЦНП «Новая Наука» 2022. – С. 109-113.

3. Любухин, А. С. Критическая информационная инфраструктура Российской Федерации в условиях санкций и импортозамещения / А. С. Любухин // Научный альманах Центрального Черноземья. – 2022. – № 1-5. – С. 110-115.

4. Курило А.П., Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. Вопросы управления информационной безопасностью. Учебное пособие. Изд-во: Горячая Линия-Телеком, Москва. 2013. 244 с.

5. Девянин П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками. Учебное пособие для вузов – М.: Горячая линия – Телеком, 2019. – 338 с.

6. Аудит информационной безопасности компьютерных систем. Учебное пособие для вузов / Р.В. Гибилинда, А.С. Коллеров, Н.И. Синадский и др. – М.: Горячая линия – Телеком. 2022. – 126 с.

7. Макаренко С.И. Аудит безопасности критической инфраструктуры специальными информационными воздействиями. Монография. – СПб.: Наукоемкие технологии, 2018. – 122 с.;

8. Милославская Н.Г. Научные основы построения центров управления сетевой безопасностью в информационно-телекоммуникационных сетях. – М.: Горячая линия – Телеком. 2022. 272 с.

9. Малюк А.А. Основы политики безопасности критических систем информационной инфраструктуры. Учебное пособие. Изд-во: Горячая Линия-Телеком, Москва. 2018., 314 с;

10. Астахов А.М. Искусство управления информационными рисками. Учебное пособие. Изд-во: Профобразование, Саратов, 2017., 312 с.;

11. Милославская Н.Г., Толстой А.И. Управление инцидентами информационной безопасности. Учебное пособие для вузов. – М.: Горячая линия – Телеком. 2022. – 272 с.

12. Макарова О.С., Поршнев С.В.. Методика прогнозирования изменения вектора компьютерной атаки с точки зрения нарушителя / Под ред. Доктора техн. Наук, профессора С.В. Поршнева. – М.: Горячая линия – Телеком. 2022. – 220 с.

13. Милославская Н.Г., Толстой А.И. Управление рисками информационной безопасности. Учебное пособие для вузов. – М.: Горячая линия – Телеком. 2022. – 224 с.

14. Методический документ. Методика оценки угроз безопасности информации. Утвержден ФСТЭК России 5 февраля 2021 г. [Электронный ресурс] Режим доступа: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/2170-metodicheskij-dokument-utverzhden-fstek-rossii-5-fevralya-2021-g

15. ГОСТ Р 58771-2019 «Менеджмент риска. Технологии оценки риска». М.: Стандартинформ, 2009.

16. ГОСТ Р 58771-2019 «Менеджмент риска. Принципы и руководство». М.: Стандартинформ, 2009.

17. ГОСТ Р 51901.23-2012 Менеджмент риска. Реестр риска. Руководство по оценке риска опасных событий для включения в реестр риска». М.: Стандартинформ, 2020.

18. ГОСТ Р 51897-2011 / Руководство ИСО 73.2009 «Менеджмент риска. Термины и определения». М.: Стандартинформ, 2019.

19. NIST Special Publication (SP) 800-30 “Guide for Conducting Risk Assessments (Revision 1, 2012).

20. Любухин, А. С. Основы комплексного подхода к анализу информационных рисков / А. С. Любухин // Наука и образование: отечественный и зарубежный опыт : сборник трудов международной научно-практической конференции, 21 декабря 2020 года. – Белгород: ООО ГиК, 2020. – С. 10-14.

21. Любухин, А. С. Стандартизация в области риск-менеджмента: зарубежный и отечественный опыт / А. С. Любухин // Современная наука: традиции и инновации : Сборник научных статей по итогам IV молодежного конкурса научных работ. – Волгоград : Научный издательский центр "Абсолют", 2021. – С. 18-22.

22. Г. Н. Хубаев Сравнение сложных программных систем по критерию функциональной полноты // Программные продукты и системы. 1998. №2. URL: https://cyberleninka.ru/article/n/sravnenie-slozhnyh-programmnyh-sistem-po-kriteriyu-funktsionalnoy-polnoty (дата обращения: 09.09.2023).

23. Щербаков С.М. Метод анализа сложных систем по критерию функциональной полноты: расширение и адаптация // Системное управление. – 2010. – Выпуск 2(8).

24. Куркина Е.П., Шувалова Д.Г. Оценка риска: экспертный метод// Проблемы науки. 2017 №1(14) [Электронный ресурс] Режим доступа: https://cyberleninka.ru/article/n/otsenka-riska-ekspertnyy-metod

25. Олейви Х.З. Метод экспертных оценок как метод оценки хозяйственного риска на предприятии // Актуальные проблемы гуманитарных и естественных наук. 2014 № 5-1 [Электронный ресурс] Режим доступа: https://cyberleninka.ru/article/n/metod-ekspertnyh-otsenok-kak-metod-otsenki-hozyaystvennogo-riska-na-predpriyatii

26. Бикетов А.Н., Глебова О.В., Мельникова О.Ю. Система оценки рисков, основанная на применении нечеткой логики // Приволжский научный вестник. 2014. №12-3 (40) [Электронный ресурс] Режим доступа: https://cyberleninka.ru/article/n/sistema-otsenki-riskov-osnovannaya-na-primenenii-nechetkoy-logiki

27. Глушенко С.А. Применение механизма нечеткой логики для оценки риска инвестиционно-строительных проектов // Вестник РГЭУ (РИНХ). 2014. №3(47) [Электронный ресурс] Режим доступа: https://cyberleninka.ru/article/n/primenenie-mehanizma-nechetkoy-logiki-dlya-otsenki-riska-investitsionno-stroitelnyh-proektov

28. Сибикина И.В. Анализ рисков информационной безопасности с использованием системы нечеткого вывода // Научный вестник Science Bulletin of the NTSU, том 65, №4, 2016. С. 121-134.

29. Любухин, А. С. Методы анализа рисков информационной безопасности: нечеткая логика / А. С. Любухин // International Journal of Open Information Technologies. – 2023. – Т. 11, № 2. – С. 66-71.

30. Любухин, А. С. Моделирование процесса категорирования объектов критической информационной инфраструктуры / А. С. Любухин // Информационная безопасность цифровой экономики : материалы XIX научно-практической конференции, Улан-Удэ, 07–11 июня 2023 года. – Новосибирск: Сибирский государственный университет телекоммуникаций и информатики, 2023. – С. 45-56.

Медведев М.А.
Федеральное государственное бюджетное
образовательное учреждение высшего
образования «Новосибирский государственный
технический университет» (НГТУ),
Ассистент кафедры защиты информации, Аспирант
m.medvedev@corp.nstu.ru

РАЗРАБОТКА МЕТОДИКИ ФОРМИРОВАНИЯ «ГРАФОВ ЗНАНИЙ» (KNOWLEDGE GRAPH) ДЛЯ СИСТЕМЫ СЕМАНТИЧЕСКОЙ КОНТЕНТ-ФИЛЬТРАЦИИ СЕТЕВОГО ТРАФИКА

Аннотация: Все большую актуальность набирает необходимость в разработке новых современных систем семантической контентной фильтрации сетевого трафика, в связи с увеличением количества источников нежелательного контента. Разработка технологии семантической контентной фильтрации сетевого трафика с применением технологий искусственного интеллекта должна обеспечить возможность разработки решений контент-фильтрации нового поколения с функционалом семантического анализа данных и повысить общий уровень защищённости конечного пользователя от злонамеренного контента. Данная разработка позволит на базе разработанных технологий создавать системы контент фильтрации нового поколения. Основные преимущества данной технологии заключается в высокой степени автоматизации процессов выявления источников злонамеренного трафика, направленных на снижение количества ложных срабатываний и учитывающие изменяющийся ландшафт используемых пользователями ИТ и злоумышленниками методов формирования злонамеренного трафика на основе автоматической генерации графов знаний для обучения искусственного интеллекта (ИИ) и формирования наборов семантических правил. Используя разработанную технологию семантической контент фильтрации, государство сможет обеспечивать технологический суверенитет и снизить зависимость от иностранных технологий. Это позволит качественно перейти на новый более совершенный подход к выявлению нежелательного трафика, что становится все более важным в условиях цифровизации современного общества. А также с недавним началом СВО, мир изменил вектор развития с глобализации на децентрализацию информационного пространства и в связи с этим технологии семантической контент фильтрации приобретают все большую ценность. За последний год значительно увеличилось количество DDOS-атак на инфраструктуру страны и ценность данной разработки заключается в том, что будет произведен переход от статических методов анализа информации к динамическим, что приведет к повышению уровня защиты информационного пространства РФ.

Ключевые слова: Искусственный интеллект, компьютерные сети, семантическая контент фильтрация.

Целью исследования является разработка интеллектуального алгоритма семантической контент-фильтрации сетевого трафика.

Тема научного проекта в рамках реализации гранта «Разработка методики формирования «графов знаний» (Knowledge Graph) для системы семантической контент-фильтрации сетевого трафика» имеет тесную взаимосвязь с темой диссертации «Разработка

интеллектуальной системы семантической контент-фильтрации сетевого трафика» в рамках изучения различных методов фильтрации контента, самого объекта исследования – трафик и в целом поставленных задач.

Задачи исследования:

- Исследование существующих методов автоматизированного определения типа контента во входящем трафике.
- Исследование существующих методов проверки, анализа и актуализации белых и черных списков фильтрации на основании семантической модели контента.
- Формирование требований к методике автоматизированного определения типа контента во входящем трафике.
- Разработка методики автоматизированного определения типа контента во входящем трафике.
- Разработка методики проверки, анализа и актуализации белых и черных списков фильтрации на основании семантической модели контента.
- Разработка метаматематических моделей на основании разработанных методик проверки, анализа и актуализации белых и черных списков фильтрации на основании семантической модели контента.
- Разработка и внедрение ПО, реализующего модели и методики проверки, анализа и актуализации белых и черных списков фильтрации на основании семантической модели контента.

Графы являются мощным и гибким способом представления данных. Графовая база данных применяется для использования графовых алгоритмов при обработке данных, установления логических связей и предоставления информации пользователю. Эта технология позволяет проводить всесторонний, глубокий и интеллектуальный анализ информации.

Графы знаний часто используют таксономии для организации понятий и установления связей через отношение «является» или «гипероним-гипоним». В таксономии гипероним является более общим понятием, а гипоним является более конкретным понятием. Таксономии представляют собой ориентированный ациклический граф, а отношение гиперонимии в таксономии является транзитивным и антисимметричным. Эта иерархия необходима для использования в логическом выводе, который важен для анализа текстов на естественном языке. Более формально отношение R называется отношением частичного порядка на некотором множестве M, если оно удовлетворяет следующим свойствам, которые в своем исследовании указывали Колмогоров А., Фомин С. [1]:

1. Рефлексивность. $\forall a \in M : (aRa)$,
2. Транзитивность. $\forall a,b,c \in M : (aRb) \Lambda (bRc) \Rightarrow (aRc)$,
3. Антисимметричность. $\forall a,b \in M : (aRb) \Lambda (bRa) \Rightarrow a = b$

В работе Жуков Н.А. и Куликов И.А. ссылаются на Тихомирова М.М. «Методы автоматизированного пополнения графов знаний на основе векторных представлений» предложил два подхода к решению задачи пополнения таксономии новыми словами, представленными на рисунке 1 [2].

Рис. 1. Ресурсы в задаче пополнения таксономии

Другие авторы Карачанская Е.В. и Соседова Н.И. исследовали метод выявления аномалий сетевого трафика [3].

Авторы исследования предложили метод, который основан на алгоритме, использующем свойства самоподобия сетевого трафика. Работа метода включает в себя запуск программы, перехват трафика, обработку трафика разработанным алгоритмом и реакцию на аномалию.

А.И. Гетьман и М.К. Иконникова исследовали проблему классификации сетевого трафика с использованием методов машинного обучения [4]. Классификация сетевого трафика рассматривается как задача обучения с учителем, и для ее решения применяются такие методы машинного обучения как:

1) наивный байесовский классификатор;

2) метод опорных векторов;

3) метод k-ближайших соседей;

4) деревья принятия решений (с разными алгоритмами построения дерева: CART, C4.5, C5.0);

5) методы бэггинга (случайный лес);

6) методы бустинга (Adaboost, XGBoost);

7) разные виды нейронных сетей: CNN, CNN+RNN, CNN+LSTM, SAE.

В рамках решения задач по классификации сетевого трафика наиболее часто используемым методом является использование математических моделей. Эти модели помогают решить следующие задачи [7]:

1) прогнозирование трафика для оценки программных и аппаратных ресурсов, таких как необходимая минимальная пропускная способность узла трафика и определение размерности

буфера для получения минимальных значений возможных количественных признаков, допустимых в рамках задач оценки потерь и задержки пакетов трафика;

2) выявление зависимостей количественных и качественных характеристик сети и оценки влияния на них алгоритмов управления трафиком;

3) выявление не стандартизированных процессов при передаче трафика, к примеру фрактальность и пульсация трафика;

4) классификации объектов в реальных сетях с использованием генераторов трафика для имитации потоков между объектами сети [5];

5) анализ количественных и качественных характеристик источника сетевого трафика и идентификация сигнатур, связанных с этим источником трафика [6].

В основе ряда моделей трафика лежат стационарные случайные процессы X(t) с различными законами распределения, с помощью которых воспроизводятся характеристики трафика (количество пакетов, полученных или отправленных в течение определенного промежутка времени; $\{\tau i\}$, где i = 1,2, … интервалы между пакетами ; длины пакетов $\{li\}$, i = 1,2, …, последовательность направлений передачи пакетов $\{\delta i\}$ i = 1,2, … .

В зависимости от методологии и описания X(t) модели делятся на группы, наиболее часто встречающиеся:

1) Пуассоновская модель трафика;

2) модели трафика с «тяжелым хвостом»;

3) модели на основе цепей Маркова;

4) модели трафика на основе теории фракталов;

5) модели на основе стохастических временных рядов.

Один из самых распространенных способов автоматического определения типа контента во входящем трафике и его ограничения – использование системы черных и белых списков. Черные и белые списки содержат набор правил классификации данных внутри информационных пакетов, по которым фильтруется нежелательный контент.

Стандарт, который описывает технические аспекты блокировки и фильтрации интернет-услуг, называется RFC7754 [8].

Фильтрация организуется двумя способами:

- работа по «чёрному» списку: РАЗРЕШИТЬ всё кроме;

- работа по «белому» списку: ЗАПРЕТИТЬ всё кроме.

Белые списки ограничивают доступ только к разрешенному контенту, в то время как черные списки ограничивают доступ только к запрещенному контенту. Пользовательские черные списки запрещают доступ, а белые списки разрешают доступ к веб-сайтам [9].

Обычно система фильтрации трафика использует наборы правил, известные как «черные списки» и «белые списки». Черные списки содержат записи (URL-адресов, IP-адресов, TCP-портов и т. д.), которые нужно блокировать, а белые списки содержат записи, которые разрешены, блокируя все остальное [10].

На сегодняшний день в области интеллектуального алгоритма контент-фильтрации сетевого фильтра решение задач сетевого трафика сводится к выявлению сигнатуры, то есть все решения сводятся к сигнатурному выявлению нежелательного контента, а именно совпадения – реагируем. Наше предложение следующее, что при помощи существующих уже решений к ним внедрить интеллектуальный алгоритм, который будет обогащать существующие черные и белые списки дополнительными вариантами одного и того же слова и типа контента, а также будет построен граф знаний и сформированы на основе него

математические модели, на основе которых уже будет построен интеллектуальный алгоритм семантической контент фильтрации сетевого трафика.

Разработка нового подхода к анализу трафика позволит непрерывно обеспечивать контент-фильтрацию объектов защиты. Разработка интеллектуального алгоритма управления автоматизированным системами в рамках задач автоматической контент фильтрации позволит экономить ресурсы по формированию черных и белых списков, также позволит более эффективно решать проблемы нежелательного трафика при помощи определения типа контента во входящем трафике. Примерами использования таких систем могут быть образовательные учреждения, которые нуждаются в цензурировании информации.

СПИСОК ЛИТЕРАТУРЫ

1. Колмогоров А., Фомин С. Элементы теории функций и функционального анализа, 2018.

2. Жукова Н.А., Куликов И.А. Практические аспекты использования графов знаний для моделирования телекоммуникационных сетей, 2020, Стр. 39-43

3. Карачанская Е.В., Соседова Н.И. Метод выявления аномалий сетевого трафика, основанный на его самоподобной структуре, 2019, Стр. 98-110

4. Гетьман А.И., Иконникова М.К. Обзор методов классификации сетевого трафика с использованием машинного обучения. Труды ИСП РАН, том 32, вып. 6, 2020 г., стр. 137-154.

5. Имитатор сетевого трафика / П.А. Будко, Д.Н. Рыжкова, Ж.О. Карпова, Д.В. Воронина // Техника средств связи. – 2018. – № 2 (142). – С. 86–98.

6. Ефимов А.Ю. Использование энтропийных характеристик сетевого трафика для определения его аномальности // Программные продукты и системы. – 2021. – Т. 34, № 1. – С. 83–90.

7. Сравнительный анализ современных трендов в области моделей трафика сетей передачи данных / И.Л. Рева, А.В. Иванов, М.А. Медведев, И.А. Огнев // Системы анализа и обработки данных. – 2022. – № 2 (86). – С. 55–68.

8. RFC 7754 - Technical Considerations for Internet Service Blocking and Filtering. – URL: https://www.rfc-editor.org/info/rfc7754 (дата обращения: 14.09.2023)

9. Бухарин В. В., Закалкин П. В., Карайчев С. Ю., Бречко А. А. Метод защиты сервера услуг от DDOS атак за счет использования списков IP-адресов // Вопросы оборонной техники. Серия 16: технические средства противодействия терроризму. 2019. №11–12. С. 29–35.

10. Медведев М. А., Рева И. Л. Анализ подходов к фильтрации трафика и эффективность применения черных и белых списков // Вестник СибГУТИ. 2023. Т. 17, № 1. С. 107–116.

Огур М.Г.
ФГАОУ ВО «Северо-Кавказский федеральный университет», старший преподаватель кафедры компьютерной безопасности,
mogur@ncfu.ru

РАЗРАБОТКА МЕТОДА ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ С ИСПОЛЬЗОВАНИЕМ СЦЕНАРИЕВ МНОГОВЕКТОРНЫХ АТАК В ДЕЦЕНТРАЛИЗОВАННОЙ IOT СРЕДЕ

Аннотация: не соответствующий заданным требованиям уровень информационной безопасности в IoT-устройствах приводит к их компрометации как внутри, так и вне инфраструктуры IoT, что может привести к утечке данных, финансовым убыткам и другим проблемам. Соответствующая проблема требует разработки новых подходов к обеспечению безопасности IoT.

Существующие методы обнаружения атак на IoT-устройства эффективны, но имеют ограничения, такие как невозможность обнаружения неизвестных атак, низкая эффективность при обнаружении многовекторных атак, высокое количество ложных срабатываний и длительное время отклика. Также важно выбирать подходящий минимальный набор признаков для обнаружения атак.

Наборы данных для обнаружения атак на IoT-устройства часто несбалансированы, что может влиять на результаты прогностических моделей. Традиционные модели машинного обучения также ограничены в предсказании новых атипичных атак, не учитываемых в существующих бюллетенях безопасности.

Ключевые слова: информационная безопасность, IoT (интернет вещей), машинное обучение, матрицы угроз, федеративная модель обучения.

Цель исследования состоит в повышении эффективности обнаружения вторжений с использованием сценариев многовекторных атак в децентрализованной IoT среде.

Для достижения поставленной цели необходимо решить следующие научные задачи:

1. Разработать математическую модель реализации многовекторных атак на IoT системы на основе анализа потока сетевого трафика.
2. Разработать модель угроз нарушения информационной безопасности процесса доверенного взаимодействия устройств IoT системы, формализующую сценарии многовекторных атак.
3. Разработать масштабируемый метод обнаружения многовекторных атак на скомпрометированные устройства IoT системы с использованием алгоритмов машинного обучения.
4. Разработать методику обнаружения и противодействия многовекторным угрозам нарушения информационной безопасности децентрализованной IoT системы.
5. Разработать имитационную модель масштабируемого метода многовекторных атак с учетом ограничений вычислительных и информационных ресурсов IoT-устройств.

Данные цели и задачи соответствуют задачам соответствующего диссертационного исследования в рамках паспорта специальности 2.3.6 «Методы и системы защиты информации, информационная безопасность», так как они направлены на разработку новых методов и систем защиты информации, в частности, на повышение эффективности систем

обнаружения вторжений и обеспечение конфиденциальности в IoT системах, что в свою очередь повышает уровень информационной безопасности.

Недостаточный уровень безопасности IoT-устройств угрожает их возможной компрометацией и может вызвать разнообразные проблемы, включая взлом, утечку данных, финансовые убытки и физические повреждения. Следует рассмотреть новые методы безопасности IoT, учитывая появление многовекторных атак, увеличивающих риск.

Многовекторная атака на IoT устройство – это сложный тип кибератаки, включающий использование нескольких уязвимостей в разных слоях архитектуры системы IoT. Она может включать атаки по сетевому протоколу, внедрение вредоносного программного обеспечения и нарушение физической безопасности устройств. Эти атаки угрожают целостности, конфиденциальности и доступности данных, обрабатываемых в системах IoT. Поэтому обнаружение многовекторных атак на IoT устройствах играет важную роль в обеспечении их безопасности [1].

Отдельные типы атак, такие как UDP, ICMP или HTTP GET, используемые злоумышленниками стали более сложными в разрезе систем IoT, включая комбинированные методы для обхода существующей защиты. Атакующие стремятся нарушить работу системы комплексно, инициируя примитивные атаки, заставляя систему активировать защитные механизмы на уровне приложения, а затем следует более сложная атака, обходящая установленную защиту и поражающая всю систему. Среди атак на IoT в 2021-2022 годах одновекторные составили 65,7%, а многовекторные – 34,3%, что обусловлено увеличением выпуска бюллетеней безопасности для продуктов IoT на 27% [2].

Для моделирования угроз информационной безопасности в доверенном взаимодействии IoT-устройств необходимо учитывать идентификацию доверенных и недоверенных устройств, включая недоверенные устройства, подключенные к сети. Рассматриваются различные типы многовекторных атак на прикладном, сетевом и физическом уровнях. Далее, определяются сценарии использования системы IoT и соответствующие угрозы информационной безопасности. Разные сценарии, такие как мониторинг производства и медицинских устройств, имеют разные угрозы. В каждом сценарии учитываются типы атак, их вероятности и методы защиты [3].

В работе [4] рассматривается модель угроз для IoT-устройств, используя методы STRIDE и DREAD для качественной и количественной оценки атак, а также матрица рисков для оценки их потенциальных воздействий. Модель определяет риски атрибутов атаки и исследует матрицу MITRE ATT&CK для выявления возможных атак на компоненты IoT системы, формируя список угроз. Однако основным недостатком этих моделей является их жесткая настройка под конкретные IoT системы.

Анализ методов обучения алгоритмов для обнаружения атак на системы IoT выявил недостаточную точность в обнаружении многовекторных атак. Улучшение точности можно достичь через разработку комплексного метода, который комбинирует методы машинного обучения, децентрализации и федерации данных. Один из таких подходов включает создание локальных моделей машинного обучения на различных устройствах системы IoT, которые затем объединяются в общую модель с использованием методов федеративного обучения. Соответствующая общая модель способна обнаруживать многовекторные атаки на IoT-устройствах [5].

Следующий рассмотренный подход – использование блокчейна для объединения данных устройств IoT и создания общей модели машинного обучения для обнаружения многовекторных атак [6].

Машинное обучение автоматизирует обнаружение и анализ кибератак. В [7] рассматриваются методы машинного обучения для обнаружения и моделирования многовекторных атак на IoT-устройства.

В [8] предложена интеллектуальная структура на основе метаэвристики для обнаружения киберугроз с использованием ансамблевого выбора признаков и классификации. Метод показал высокую точность, скорость обнаружения и метрику F1, но не учитывает минимизацию простоев оборудования.

Существующие системы обнаружения вторжений (IDS) защищают сети, но требуют больших вычислительных ресурсов и имеют задержки. Исследования авторов [8] нацелены на эффективные методы выбора признаков и построение моделей нарушителей в реальном времени в IoT и SCADA сетях. С учётом ограниченных ресурсов узлов IoT, разработка адаптивного метода обнаружения вторжений становится критически важной задачей.

В [9] представлена новая система обнаружения вторжений в сельскохозяйственных сетях IoT с использованием набора данных NSL KDD и архитектур CNN, таких как VGG16, Inception и Xception. Сравнивается с классическими методами машинного обучения по точности, F1-оценке, полноте и точности. Однако метод ограничен в адаптивности при обнаружении атак.

В исследовании [10] представлена трехэтапная структура глубокого обнаружения вредоносных программ (DMD-DWT-GAN) для сельского хозяйства на базе IoT (IoT-SA). Она объединяет дискретное вейвлет-преобразование (DWT) и генеративно-состязательную сеть (GAN). DWT используется для разрешенного анализа изображений, разделяя их на коэффициенты аппроксимации и детализации. Для более глубокого анализа вредоносных программ используется сверточная нейронная сеть (CNN). Платформа оценивается на двух наборах данных - вредоносном ПО IoT и Malimg, достигая точности 99,99% в обоих случаях, превосходя современные модели. Однако выделяются высокие требования к вычислительным ресурсам и сложность начальной настройки в новой инфраструктуре.

За последние десять лет исследователи из академических и промышленных секторов активно использовали машинное обучение для создания систем обнаружения вторжений в компьютерные сети. Однако обнаружение вторжений в IoT остается недостаточно исследованным. Многие из них применяли несбалансированные наборы данных, что может привести к неудовлетворительным результатам в предсказании вторжений. Модели, обученные на таких данных с использованием традиционных функций потерь, не способны точно предсказывать атипичные многовекторные атаки, не включенные в регулярные бюллетени безопасности [11].

IoT системы предоставляют доступность данных сенсоров в традиционных архитектурах, но имеют недостатки, такие как высокая задержка, низкая трассируемость данных в реальном времени и ограниченный уровень безопасности. Появляются также и новые проблемы в области безопасности и конфиденциальности из-за роста числа подключенных умных устройств IoT и разнообразия генерируемых данных [12].

Каждый уровень стека безопасности IoT предоставляет собственные механизмы безопасности. Уровень безопасности IEEE 802.15.4 обеспечивает шифрование данных с использованием AES-CCM. Этот протокол имеет фиксированный ключ размером 128 бит и

использует тот же размер блока открытого текста. Сетевой уровень зависит от IPv6 и полагается на IPSec для обеспечения безопасности взаимодействия с Интернетом. На транспортном уровне механизм безопасности зависит от применяемого прикладного протокола: DTLS для CoAP и SSL/TLS для MQTT [13]. Основные проблемы безопасности IoT связаны с интеграцией множества технологий и разнообразием оконечных устройств с различными характеристиками. Контроль над оконечными устройствами часто ограничен [14].

В рамках проекта предлагается новый метод обнаружения многовекторных атак в децентрализованных IoT средах, использующий методы машинного обучения и дискретного анализа.

Новизной первой задачи является учет архитектурных особенностей IoT устройств при разработке математической модели многовекторных атак. Предлагается оригинальный подход, учитывающий неравномерность трафика и разнородность данных в IoT.

Решение второй задачи направлено на определение вероятных способов атаки и уязвимых мест в доверенном взаимодействии IoT-устройств, что позволит разработать эффективные механизмы защиты, учитывающие конкретные атаки и предотвращающие их.

Третья задача решается с использованием метода выявления признаков многовекторных атак на системы IoT. Она направлена на обеспечение конфиденциальности данных в условиях масштабирования угроз.

Четвертая задача предлагает новую методику обнаружения и предотвращения вторжений в системы IoT с использованием масштабируемого метода выявления признаков многовекторных атак. Разработанная методика снизит количество ложных срабатываний и улучшит производительность системы обнаружения нарушений.

Пятая задача заключается в имитационном моделировании разработанных методов и оценке их эффективности с учетом функциональных ограничений IoT-устройств. Это позволит применить методы на практике и оценить их применимость в реальных условиях использования IoT-устройств. Практическая значимость предлагаемых решений в области безопасности IoT обусловлена возможностью достижения высоких показателей информационной безопасности за счет использования разработанных технических решений. Предлагаемые модели, методы и алгоритмы позволят эффективно бороться с различными угрозами безопасности, такими как многовекторные атаки и вторжения в систему. Решение задачи позволит повысить отказоустойчивость системы и обеспечить безопасность устройств Интернета вещей.

Ожидаемыми научными результатами проекта «Разработка метода обнаружения вторжений с использованием сценариев многовекторных атак в децентрализованной IoT среде» являются:

1. Математическая модель реализации многовекторных атак на IoT системы на основе анализа потока сетевого трафика.
2. Модель угроз нарушения информационной безопасности процесса доверенного взаимодействия устройств IoT системы, формализующая сценарии многовекторных атак.
3. Масштабируемый метод обнаружения многовекторных атак на скомпрометированные устройства IoT системы с использованием алгоритмов машинного обучения.
4. Методика обнаружения и противодействия многовекторным угрозам нарушения информационной безопасности децентрализованной IoT системы.

5. Имитационная модель масштабируемого метода многовекторных атак с учетом ограничений вычислительных и информационных ресурсов IoT устройств.

Разработанные в рамках проекта модели, методы и алгоритмы соответствуют задачам программы развития цифровой экономики Российской Федерации, так как их использование позволит повысить уровень кибербезопасности в различных сферах, включая государственные и коммерческие организации.

Полученные научные результаты могут быть использованы в учебном процессе для обучения специалистов в области информационной безопасности и кибербезопасности. Кроме того, научные результаты могут быть использованы для участия в научных конференциях и семинарах, что позволит представить их широкой научной аудитории.

СПИСОК ЛИТЕРАТУРЫ

1. Аль-Джабир А. Аномалия обнаружения в системах IoT на основе анализа многовекторных атак // IEEE Access — 2021 — 9 — 331-342.
2. Salim M.M. Distributed denial of service attacks and its defenses in IoT: a survey / S. Rathore, J.H. Park // Supercomput — 2022 — 76 — 5320-5363.
3. Yu F. A multi-vector attack detection scheme for industrial IoT systems based on deep learning and fuzzy logic / Q. Zhang, H. Liu // IEEE Access — 2021 — 9 — 15602-15615.
4. Zahid S. Threat modeling in smart firefighting systems: Aligning MITRE ATT&CK matrix and NIST security controls / M. S. Mazhar, S. G. Abbas, Z. Hanif, S. Hina, G. A. Shah // Internet of Things — 2023 — 22.
5. Chen S. A Survey of Federated Learning for Edge IoT / P. Jiang, M. Xue // IEEE Access — 2021 — 9 — 45592-45605.
6. Gao S. Decentralized Federated Learning for Privacy-Preserving / X. Zhang, M. Ma // IEEE Internet of Things Journal Access — 2021 — 8(18) — 14606-14619.
7. Ahmetoglu H. A comprehensive review on detection of cyber-attacks: Data sets, methods, challenges, and future research directions / R. Das // Internet of Things — 2022 — 20.
8. Dey A. K. A metaheuristic-based ensemble feature selection framework for cyber threat detection in IoT-enabled networks / G. P. Gupta, S. P. Sahu // Decision Analytics Journal — 2023 — 7.
9. Ahakonye L. A. C. SCADA intrusion detection scheme exploiting the fusion of modified decision tree and Chi-square feature selection / C. I. Nwakanma, J.-M. Lee, D.-S. Kim // Internet of Things — 2023 — 21.
10. El-Ghamry A. An optimized CNN-based intrusion detection system for reducing risks in smart farming / A. Darwish, A. E. Hassanien // Internet of Things — 2023 — 22.
11. Santosh K. Deep malware detection framework for IoT-based smart agriculture / G. P. Gupta, S. Kumar // Computers and Electrical Engineering — 2022 — 104.
12. Dina A. S. A deep learning approach for intrusion detection in Internet of Things using focal loss function / A.B. Siddique, D. Manivannan // Internet of Things — 2023 — 22.
13. Sezer B. B. PPFchain: A novel framework privacy-preserving blockchain-based federated learning method for sensor networks / H. Turkmen, U. Nuriyev // Internet of Things — 2023 — 22.
14. Каженова Ж. С. Безопасность в протоколах и технологиях iot: Обзор / Ж.Е. Кенжебаева // International Journal of Open Information Technologies — 2022 — 3.

Панфилова И.Е.
ФГБОУ ВО «Самарский государственный технический университет»,
инженер-электроник II категории,
panfilova_2015@bk.ru

МЕТОДЫ И АЛГОРИТМЫ ПОВЫШЕНИЯ НАДЕЖНОСТИ НЕЙРОСЕТЕВОЙ БИОМЕТРИЧЕСКОЙ АУТЕНТИФИКАЦИИ

Аннотация: Быстрое развитие технологий искусственного интеллекта позволяет внедрять различные системы на их основе во все сферы деятельности человека. Тем не менее, подавляющее большинство современных систем искусственного интеллекта оказываются уязвимы с точки зрения конфиденциальности своих решающих параметров и данных, которыми оперируют. В этой связи оказывается нарушенной концепция доверенного искусственного интеллекта, и система перестает отвечать требованиям надёжности. Особенно актуальной указанная проблема становится для систем биометрической аутентификации, основанных на алгоритмах машинного обучения (в том числе на искусственных нейронных сетях): в этом случае в качестве данных выступают персональные биометрические характеристики пользователей. С целью повышения надежности нейросетевой биометрической аутентификации необходимо использовать алгоритмы защиты биометрических шаблонов, позволяющие обеспечивать сокрытие своих решающих правил и самих биометрических данных. В рамках данного исследования продемонстрированно, что указанным требованиям в полной мере соответствуют отечественные реализации нейросетевых преобразователей биометрия-код. Однако его модификаций оказывается недостаточно для обеспечения защиты системы биометрической аутентификации от класса атак на биометрическое предъявление. В связи с этим в работе предлагаются новые подходы повышения надежности нейросетевой биометрической аутентификации, основанные на методах объяснимого искусственного интеллекта и использующие технологии альтернативных модификаций нейросетевых преобразователей биометрия-код.

Ключевые слова: биометрическая аутентификация, автоматическое обучение, преобразователи «биометрия-код», доверенный искусственный интеллект, машинное обучение, искусственные нейронные сети, извлечение признаков, аутентификация по лицу.

В виду активного развития систем искусственного интеллекта (ИИ) и их практического применения к различным сферам деятельности человека, особенно актуальным становится вопрос проектирования и разработки таких алгоритмов ИИ, которым пользователь смог бы в полной мере доверять. В данном контексте понятие доверия восходит к определению концепции доверенного искусственного интеллекта, сформулированной сообществом владельцев, разработчиков и пользователей ИИ [1] с целью решения новых, ранее не прорабатываемых, задач, таких как злонамеренные атаки на ИИ или его неправомерное использование. Однако, среди прочих критериев доверенного ИИ (например, робастности и прозрачности (объяснимости)), особое место занимает вопрос безопасности систем искусственного интеллекта с точки зрения конфиденциальности процессов его функционирования и данных. В этой связи особенно пристальное внимание необходимо уделять системам ИИ, принимающим ответственные решения или оперирующим критически важными данными. В полной мере к указанной группе могут быть отнесены биометрические

системы (БС) аутентификации и/или идентификации на основе алгоритмов машинного обучения (в том числе на искусственных нейронных сетях): подобные системы не только используют биометрические параметры человека, то есть его персональные данные, но и сами являются сервисами реализации информационной безопасности.

Одной из распространенных практик обеспечения конфиденциальности биометрических данных является хранение таковых в виде биометрических шаблонов (БШ) [2], получаемых путем тех или иных преобразований исходного образа. Однако недавние исследования показывают, что исходные биометрические данные могут быть восстановлены из открыто хранящихся биометрических шаблонов [3], а затем использованы с целью доступа к системе. В связи с этим, особенно актуальными становятся задачи защиты биометрических шаблонов от компрометации путем реализации такого процесса преобразования биометрического образа в его шаблон, при котором невозможно раскрытие параметров работы преобразующей системы, а также самих биометрических данных. Именно такая задача, отдельно от области развития технологий биометрической аутентификации, на протяжении последних десятилетий решается в контексте направления защиты биометрических шаблонов (ЗБШ).

Область исследований ЗБШ представляет собой довольно широкий спектр подходов к сокрытию, шифрованию, изменению и преобразованию биометрических образов людей. В общем случае все перечисленные подходы позволяют обеспечивать защиту биометрических систем от атак, связанных с их программным обеспечением. К таким атакам могут относиться попытки получения контроля над управлением алгоритмом ИИ, лежащим в основе БС, с целью получения доступа к системе и персональным данным пользователей. В таком случае, одним из наиболее простых способов защиты биометрических шаблонов является использование стандартных шифров [4], таких как SHA-3. Однако из-за изменчивости биометрических шаблонов их необходимо расшифровывать перед сравнением, что снижает их эффективность по сравнению с традиционными паролями, которые можно сравнить в зашифрованной (хешированной) форме. Поэтому другим возможным шифром для защиты биометрических шаблонов на сегодняшний день представляется гомоморфное шифрование [5]. Такой подход к шифрованию позволяет сравнивать шаблоны в их зашифрованной форме, чтобы получить зашифрованные результаты, которые затем расшифровываются, чтобы получить решение. Однако гомоморфное шифрование требует больших вычислительных ресурсов, особенно для многомерных биометрических шаблонов. Оно также страдает от той же проблемы управления ключами, что и большинство гомоморфных конструкций шифрования [5], в которых ключ дешифрования зашифрованных результатов может использоваться для дешифрования зашифрованных шаблонов.

Кроме методов на основе шифрования, современные исследователи выделяют также подходы по защите биометрических шаблонов на основе биокриптографических систем и на основе методов отменяемой биометрии. Отменяемая биометрия (ОБ) использует функции необратимого преобразования и секретный ключ, специфичные для пользователя с целью создания псевдобиометрических шаблонов в качестве защищенных версий исходных БШ. Измененный шаблон и пользовательский ключ сохраняются для целей проверки. Чтобы изменить биометрические шаблоны, функцию преобразования можно реализовать либо с помощью функции «многие к одному» (необратимые преобразования), где безопасность схем зависит от необратимости функции преобразования, либо с помощью подхода смешивания (соление), где безопасность схемы зависит от безопасности ключа. Однако, такие защищенные

псевдошаблоны также могут быть уязвимы для атак в зависимости от установленного механизма безопасности [6].

В случае подходов, основанных на криптографическом шифровании биометрических шаблонов, в основе всегда находится биометрическая криптосистема (БКС). В общем случае, под этим термином понимается любая схема шифрования, которая позволяет безопасно привязывать цифровой ключ к биометрическому шаблону или генерировать цифровой ключ из биометрического шаблона. При этом, как видно из определения, БКС делятся на два класса в зависимости от принципа функционирования: генерирующие ключи из биометрического шаблона и связывающие ключ с БШ. В случае генерации ключей в основу работы БКС закладывается принцип квантования биометрических данных: векторы признаков нескольких биометрических образцов раскладываются на интервалы элементов признаков, затем полученные интервалы кодируются и сохраняются в виде вспомогательных данных [7].

Альтернативным подходом является использование схем защиты биометрических шаблонов на основе БКС, которые позволяют связывать исходные биометрические данные с определенным извне криптографическим ключом. Хорошо известным примером такого подхода является схема нечеткого обязательства, в соответствии с которой случайное, специфичное для пользователя кодовое слово «связывается» с биометрическим шаблоном пользователя. Другим известным типом «привязки» метода ЗБШ является схема нечеткого контейнера, где случайно выбранное, специфическое для пользователя кодовое слово служит набором коэффициентов, определяющих секретный полином, а элементы биометрического шаблона пользователя являются входными данными полинома. Указанные подходы могут быть классифицированы как "нечёткие экстракторы", которые обеспечивают надёжную защиту биометрических данных путём создания хэшей, не раскрывающих информацию об исходных шаблонах [7]. Однако существующие нечеткие экстракторы не поддерживают эффективную идентификацию пользователя.

В отечественной практике наибольшую популярность среди подобных технологий приобрела разработанная в нашей стране и закрепленная в серии стандартов ГОСТ Р 52633 технология нейросетевых преобразователей биометрия-код (НПБК), представляющая собой биометрическую криптосистему перехода от открытого биометрического шаблона к защищенному ключу путем связывания первого с последним. В общем случае такой алгоритм направлен на преобразование вектора нечетких, неоднозначных биометрических параметров "Свой" в четкий однозначный код ключа (пароля) (на воздействие случайного входного вектора, не принадлежащего множеству образов "Свой", такой преобразователь откликается случайным выходным кодом). Наряду с этим, нейросетевое исполнение ПБК (НПБК) предоставило еще больше возможностей для формирования длинных ключей, устойчивых к атакам подбора, а также для повышения точности распознавания биометрических образов. Такие показатели во многом стали возможны за счет использования специфических реализаций как самой нейронной сети («широкие сети») [8], так и отдельных нейронов (квадратичные [9], корреляционные [10] и др.).

Также важным условием функционирования НПБК является тот факт, что все параметры обученных нейронов (параметры связей и значения весов) нейросетевого преобразователя биометрия-код, называемые «нейросетевым контейнером», подвергаются дополнительной защите с целью невозможности осуществления атак извлечения знаний. Для реализации такого подхода к таблицам нейросетевых функционалов применяется механизм защищенного нейросетевого контейнера (ЗНК), отраженный в [11]. В общем виде защита

биометрического шаблона в соответствии с указанной спецификацией достигается путем применения использования обратимого или необратимого преобразования.

Использование нейросетевых преобразователей биометрия-код для различного рода биометрических модальностей остается открытой исследовательской областью, особенно с учетом того факта, что схема НПБК не является абсолютным решением вопроса защиты биометрического шаблона и решающих правил самой системы. НПБК по-прежнему обладает рядом ограничений, не позволяющих в полной мере реализовывать абсолютно безопасный и удобный процесс аутентификации пользователя, основываясь на его биометрических данных. В случае использования в качестве биометрического образа лица человека, являющегося открытым образом (то есть образом, общедоступным для наблюдения), НПБК не способен точно определить присутствие перед системой аутентификации реального человека. Таким образом, НПБК становится уязвим к другому типу атак, носящему название атак на биометрическое предъявление [12]. Чаще для определения подобного типа атак используется термин спуфинг (spoofing attack), применяемый в контексте биометрической аутентификации как попытка обхода такой системы посредством предъявления ей поддельного биометрического образа. Данная особенность НПБК связана с тем, что на его вход поступают только векторы признаков биометрических образов, которые могут быть получены как путем предварительной обработки образа, так и в ходе процесса извлечения признаков в реальном времени. В связи с этим, главной целью представленного исследования является разработка методов и алгоритмов повышения надежности процесса нейросетевой биометрической аутентификации на основе открытого образа лица человека с учетом существующих недостатков функционирования нейросетевых преобразователей «биометрия-код». Для достижения поставленной цели в рамках проекта необходимо решить следующие задачи:

1. Разработать метод определения подлинности аутентифицируемых лиц, учитывающий защищенный режим исполнения биометрической системы на основе БКС.
2. Разработать отличный от существующих (учитывающий недостатки предыдущих решений) математический аппарат построения нейросетевого преобразователя биометрия-код (как варианта БКС), осуществляющего процедуру биометрической аутентификации по лицу с обеспечением защиты от атак и компрометации знаний.
3. Разработать алгоритм автоматического синтеза и обучения нового типа нейросетевого преобразователя биометрических образов лица в код на малых выборках с предварительным получением верно классифицированных изображений (подлинное или поддельное).

Для решения поставленных задач, а также достижения главной цели исследования, могут быть применены следующие методы:

1. Реализация метода определения подлинности аутентифицируемых лиц, учитывающего защищенный режим исполнения биометрической системы на основе БКС, возможно осуществить путем добавления в процесс аутентификации пользователей новых функциональных элементов, основанных на алгоритмах глубокого обучения. Одним из перспективных направлений реализации такого рода элементов, наряду с классическими архитектурными решениями, учитывающими особенности входного изображения, является объяснимый искусственный интеллект. В таком случае использование стандартных библиотек для объяснения решений алгоритмов машинного обучения может использоваться для задачи определения подлинности входного изображения. Как видно из рисунка 1, при принятии решения в случае бинарной классификации алгоритм ИИ может «обращать» внимание на разные значимые для него пиксели изображения в зависимости от его качества.

Предварительные исследования показывают [13-14], что для плоских (поддельных) изображений такое изображение значимых пикселей может существенно отличаться от реального изображения. На основе подобного рода информации относительно подлинности изображения можно принимать то или иное решение.

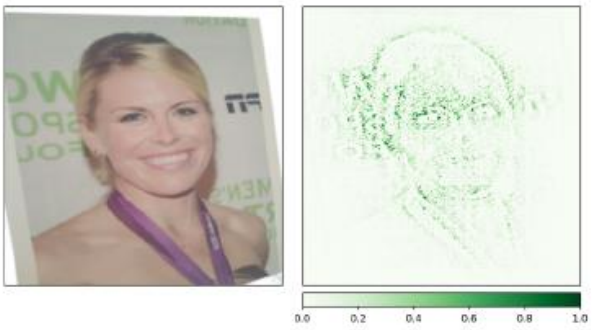


Рис.1. «Значимые» пиксели входного поддельного изображения

В рамках исследования также имеет смысл осуществить сравнительный анализ такого подхода со стандартными решениями на базе бинарных классификаторов, принимающих решение о подлинности или поддельности входного изображения. Такой подход позволит выборочно осуществить внедрение подходящего нейросетевого модуля извлечения признаков, обученного работать с реальным изображением лица человека. Реализация направления осуществима путем применения технологий глубокого обучения, в особенности сверточных нейронных сетей, широко применяемых для задач извлечения информативных признаков из поступающих на вход изображений.

2. Получение отличного от существующих структур НПБК возможно путем применения альтернативных метрик работы с входными признаками. Одним из перспективных направлений в таком случае становится применение математического аппарата усреднения входного потока группы признаков с целью стабилизации вычислений. Процедура осуществляется до попадания суммы признаков в функцию активации, что позволяет анализировать весь допустимый входной поток. Альтернативным подходом в реализации новой структуры НПБК может также стать метрика, учитывающая расположение признаков друг относительно друга. Впервые подобные исследования производились [15] в рамках исследования мета-пространства признаков, порождаемого зависимостью двух признаков между собой.

3. Разработка алгоритма автоматического синтеза и обучения нейросетевого преобразователя биометрических образов лица в код на малых выборках с предварительным получением верно классифицированных изображений (подлинное или поддельное) возможна путем разработки и анализа предыдущих шагов и их синтеза.

Предложенная группа подходов позволяет не только учитывать защищенное исполнение искусственного интеллекта, лежачего в основе системы аутентификации пользователя по лицу, но и значительно повышает устойчивость всей системы к возможным атакам на биометрическое предъявление и атакам, ориентированным на манипуляции с программным обеспечением БКС. Предполагается, что разработанная группа подходов будет применена для реализации защищенного исполнения систем биометрической аутентификации субъектов по лицу. Научные результаты исследования могут быть применены для задачах проектирования и разработки новых технологий защиты биометрических данных в системах аутентификации по лицу.

СПИСОК ЛИТЕРАТУРЫ

1. Li Bo. Trustworthy AI: From Principles to Practices / Bo Li, Peng Qi, Bo Liu, Shuai Di, Jingen Liu, Jiquan Pei, Jinfeng Yi, And Bowen Zhou // 2021.— P 1-11. URL: https://doi.org/10.48550/arXiv.2110.01167
2. Mai G. SecureFace: Face Template Protection / G. Mai, K. Cao, X. Lan, P. C. Yuen // IEEE Transactions on Information Forensics and Security. — 2020. — P 1–1
3. Mai G. On the reconstruction of face images from deep face templates / G. Mai, K. Cao, P. C. Yuen, and A. K. Jain // IEEE Transactions on Pattern Analysis and Machine Intelligence. — 2019.
4. Stallings W. Cryptography and network security: principles and practice // Pearson. — vol. 7. — 2016.
5. Gentry C. A fully homomorphic encryption scheme // Stanford University. — 2009.
6. Abdullahi Sani M. Biometric Template Attacks and Recent Protection Mechanisms: A Survey / Sani M. Abdullahi, Sun Shuifa, Wang Beng, Wei Ning, Wang Hongxia // 2021. URL: http://dx.doi.org/10.2139/ssrn.4543001
7. Панфилова И.Е., Иниватов Д.П.. Обзор методов защиты данных биометрических шаблонов / И.Е. Панфилова, Д.П. Иниватов // Сборник научных статей по материалам V Всероссийской научно-технической конференции «Безопасность информационных технологий». — Том 1.— 2023.
8. ГОСТ Р 52633.5-2011. Защита информации. Техника защиты информации. Автоматическое обучение нейросетевых преобразователей биометрия-код доступа. – Москва: Стандартинформ, 2013.
9. Малыгина, Е. А. Биометрико-нейросетевая аутентификация: перспективы применения сетей квадратичных нейронов с много-уровневым квантованием биометрических данных : пре-принт / Е. А. Малыгина. – Пенза : Изд-во ПГУ, 2020. – 114 с.
10. Иванов, А. И. Использование сетей корреляционных нейронов с многоуровневым квантованием: защита от извлечения знаний из параметров решающего правила : препринт / А. И. Иванов, А. Е. Сулавко. – Пенза : Изд-во ПГУ, 2020. – 48 с.
11. ТС 26.2.002-2020 «Защита нейросетевых контейнеров с использованием криптографических алгоритмов»
12. ГОСТ Р 58624.3-2019. Информационные технологии. БИОМЕТРИЯ. Обнаружение атаки на биометрическое предъявление. Часть 3. Испытания и протоколы испытаний. – Москва: Стандартинформ, 2019.
13. Selvaraju R. R. Grad-cam: Visual explanations from deep networks via gradient-based localization / R. R. Selvaraju, M. Cogswell, A. Das, R. Vedantam, D. Parikh, and D. Batra // ICCV. – 2017.
14. Silva Wilson. Artificial Intelligence for Face Presentation Attack Detection / Wilson Silva, Tiago Filipe Sousa Gonçalves, Ana Sequeira, João Ribeiro Pinto. Explainable // 26th Portuguese Conference in Pattern Recognition (RECPAD). – 2020.
15. Sulavko, A. Biometric-Based Key Generation and User Authentication Using Acoustic Characteristics of the Outer Ear and a Network of Correlation Neurons // Sensors. – 22, 9551. – 2022.

Петренко А.С.
СПбГЭТУ «ЛЭТИ», аспирант,
A.Petrenko1999@rambler.ru

МЕТОД ОБЕСПЕЧЕНИЯ КВАНТОВОЙ УСТОЙЧИВОСТИ БЛОКЧЕЙН ЦИФРОВОЙ ЭКОНОМИКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Аннотация: показано, что ключевые блокчейн-экосистемы и платформы Цифровой экономики Российской Федерации уже не обладают требуемой устойчивостью для целевого функционирования в условиях ранее неизвестных (и соответственно слабо изученных) атак злоумышленников с применением квантового компьютера. Достижения *IBM*, а также ряда других высокотехнологичных производителей квантовых компьютеров, убедительно свидетельствуют о реалистичности так называемой «*квантовой угрозы*». По этой причине в ряде технологических стран мира уже начали подготовку к противодействию будущим квантовым кибератакам. Предложен новый метод обеспечения квантовой устойчивости блокчейн, который в отличие от других известных методов информационной безопасности позволяет упреждать приведение упомянутых систем к существенным или катастрофическим последствиям в условиях роста угроз безопасности. Здесь под *квантовой устойчивостью* понимается способность блокчейн достигать цели функционирования в условиях квантовых атак злоумышленников.

Ключевые слова: цифровая экономика, технология блокчейн, квантовая угроза, криптопримитивы, постквантовая криптография, квантово-устойчивый блокчейн.

Состояние вопроса. В настоящее время квантовые технологии и вычисления активно развиваются. При этом мы находимся в так называемой эре шумных квантовых устройств промежуточного размера (NISQ) [1,9,10]. Это означает, что те компоненты квантового компьютера (см. Рис. 1), которые можно реализовать на практике, несовершенны в плане точности, сильно подвержены помехам и ошибкам. Тем не менее, если эти компоненты использовать в сочетании с классическими компьютерами и супер-ЭВМ пятого поколения архитектуры *фон Неймана*, оказывается возможным достичь существенного ускорения в вычислениях в области решения широкого класса задач многомерной оптимизации, в том числе, задачи дешифрования известных криптопримитивов блокчейн [1-4,10].

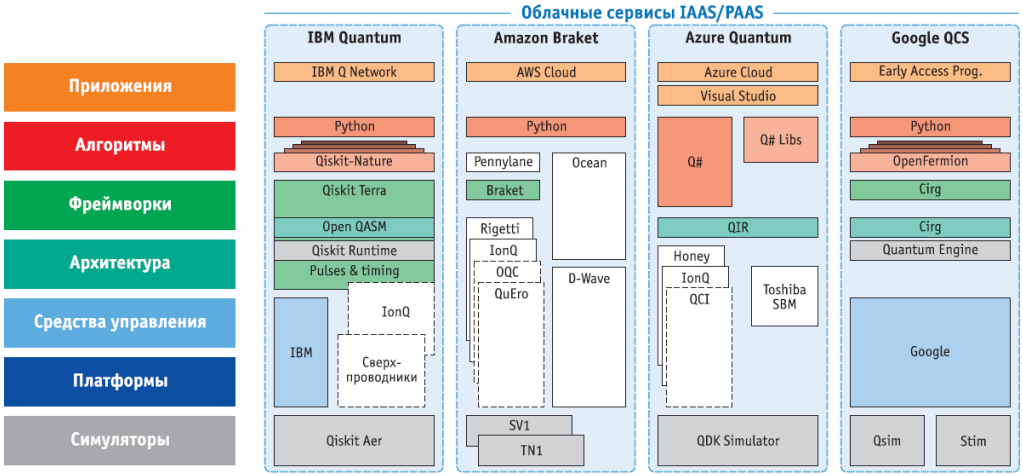


Рис. 1. Инструментальные средства для квантового криптоанализа криптопримитивов блокчейн

В настоящее время исследователи во всем мире работают над созданием квантовых компьютеров на четырех основных платформах: *сверхпроводниках, ионах, нейтральных атомах и фотонах*. Рассмотрим основные особенности этих платформ.

Первый тип платформ, на сверхпроводниках, развивают компании *IBM, Google, Rigetti, Intel, Alibaba*. К достоинствам этих платформ относятся: хорошая масштабируемость, стабильность во времени и относительная легкость в управлении. К недостаткам - необходимость использования сверхнизких температур и низкая когерентность.

Второй тип платформ, на ионах, развивают и совершенствуют компании *Honeywell, IonQ, AQT*. Упомянутые платформы характеризуются лучшей стабильностью и точностью вычислительных операций. Недостатком этого типа платформ считается технологическое ограничение максимального размера квантового регистра.

Третий тип платформ, на нейтральных атомах, развивают компания *Pasqal (Франция), Гарвардский университет и Университет Париж-Сакле*. Платформы этого типа допускают хорошее масштабирование. Вместе с тем они отличаются высокой сложностью управления квантовыми системами.

Четвертый тип, на фотонах, развивают компании *Xanadu, Quix, Psi Quantum* и др. Этот тип платформы отличают компактные размеры, возможность работы при комнатных температурах, а также возможность относительно легкого сопряжения с волоконно-оптическими линиями связи. Вместе с тем в таких платформах сложнее реализовать логические цепи из-за слабого взаимодействия фотонов.

Если говорить о конкретных моделях квантовых компьютеров, то большее распространение получили вычислительные устройства на *сверхпроводниках.* В частности, *Zuchongzhi* — 66 кубитов (USTC, Китай); *Hummingbird* — 65 кубитов (IBM, США); *Sycamore* — 54 кубита (Google, США); *Tangle Lake* — 49 кубитов (Intel, США) и др. Здесь следует отметить событие, происшедшее 14 ноября 2022 года, когда на мероприятии *IBM «Quantum Summit 2022»* был представлен квантовый процессор *Osprey* с рекордными 433 кубитами, https://www.youtube.com/watch?v=8ySjHqfioJM. В планах IBM создание квантового процессора *Condor* с 1121 кубитами, а также модульного процессора *Heron*, объединяющего сразу несколько 133-кубитных блоков. К концу 2023 года ожидается появление квантовой системы второго поколения *Quantum System Two*, которая станет основой для создания гибридных квантовых суперкомпьютеров. В планах *IBM* разработать квантовую систему с более чем 4 000 кубитами к 2025 году. Конкурирующая компания *Google* планирует представить квантовый облачный вычислитель с 1 млн. кубитов к 2029 году. Для сравнения, сейчас лидирует облачный вычислитель канадской компании *D-Wave* с процессором *D-Wave Advantage 2* на 7 000 кубитов, основанный на технологии квантового отжига. Для работы с этим вычислителем разработан открытый облачный сервис *Leap*, который и позволяет создавать и исполнять различные квантовые приложения.

Активно развиваются и соответствующие квантовые алгоритмы (более 40), старт которым был положен в 1980 году известным советским и российским математиком Ю.И. Маниным (1937-2023), член-корреспондентом РАН (1990). Затем Дойч в 1985 году, обратив внимание на аналогию между квантовыми вентилями и логическими вентилями в цифровых схемах, формально описал квантовую машину Тьюринга (англ. quantum Turing machine; иногда — универсальный квантовый компьютер) [4-8,10].

В 1994 году американский математик Питер Шор (Peter Shor) разработал алгоритм, который показал, что с помощью квантовых вычислений можно эффективно решать задачу

факторизации числа, то есть разложения числа на произведение простых сомножителей. При этом за полиномиальное время (стало быть, полиномиальное количество гейтов) и на полиномиальном количестве кубитов. Т.е.., квантовый алгоритм Шора может быть использован для криптоанализа большинства известных криптопримитивов блокчейн [10].

Существенно, что развитие алгоритмической базы может сократить сроки появления эффективных квантовых вычислителей. Более того, перспективы появления «практического» квантового компьютера, способного выполнять поставленные задачи криптоанализа, становятся еще ближе, если учитывать текущие результаты компании *IBM* - *433*-кубитный квантовый процессор *Osprey*. В планах *IBM* к 2025 году разработать квантовый процессор на *4000* кубитов, а рубеж в *1000* кубитов преодолеть до конца 2023 года, https://www.ibm.com/quantum/roadmap.

В конце 2022 года китайские ученые представили новый метод факторизации чисел на основе *алгоритма Шнорра*, https://eprint.iacr.org/2021/933.pdf, в котором было использовано квантовое ускорение для приближенного получения результатов одного из его этапов – решения задачи поиска короткого вектора в решетке (*SVP*) небольшой размерности. Была выдвинута гипотеза о том, что для факторизации числа требуется меньше кубитов, чем его длина, а также квантовые схемы меньшей глубины, чем считалось ранее, https://arxiv.org/abs/1905.09749. Работоспособность этого метода была продемонстрирована на примере факторизации *48*-битового числа *RSA* с помощью квантового компьютера на сверхпроводниках всего с *10*-кубитами. В итоге был сделан вывод о том, что для факторизации *2048*-битового числа *RSA* достаточно всего *372* физических кубитов, https://arxiv.org/pdf/2212.12372.pdf (вместо ранее озвученных *20* млн. физических кубитов). В основе нового подхода лежит комбинация *алгоритма Шнорра*, https://eprint.iacr.org/2021/933.pdf с дополнительным этапом «квантовой оптимизации» (*Quantum Approximate Optimization Algorithm, QAOA),* https://arxiv.org/pdf/2212.12372.pdf. Однако, полученные результаты китайских ученых нуждаются в тщательной проверке. Так как *алгоритм Шнорра* не имеет корректной оценки сложности (см. Рис. 2).

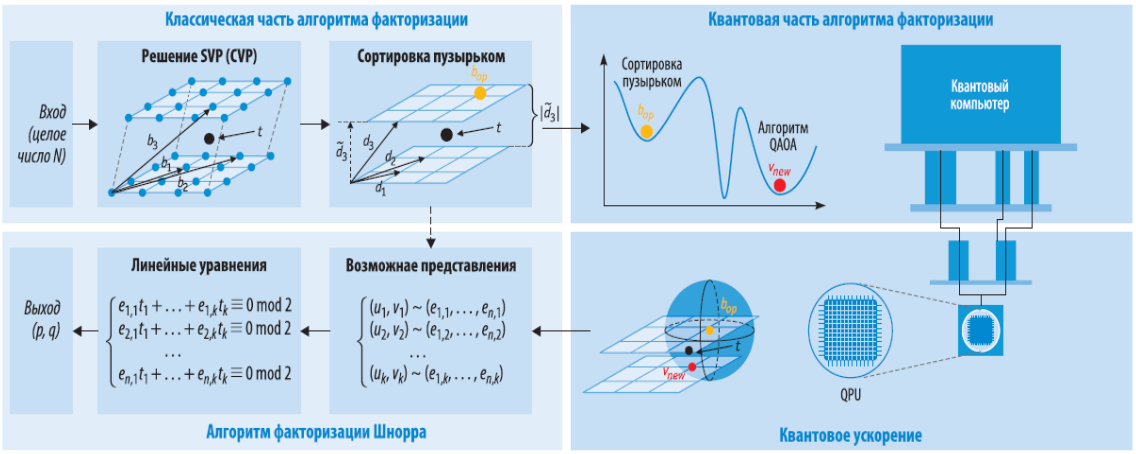


Рис. 2. Возможная схема гибридного алгоритма факторизации

Цели и задачи научного проекта в рамках реализации гранта. Главной целью проекта является разработка метода обеспечения требуемой устойчивости блокчейн-экосистем и платформ Цифровой экономики Российской Федерации в условиях ранее

неизвестных атак злоумышленников с применением квантового компьютера. К основным *задачам проекта* относятся:

1) Создание и развитие алгоритмов анализа квантовой устойчивости блокчейн на основе модифицированных *квантовых алгоритмов Шора и Гровера*, позволяющих получить реальные оценки теоретической и практической стойкости криптопримитивов *Enterprise Ethereum Alliance (Эфириум 2.0), Waves Enterprise (Waves, Vostok), Мастерчейн 2.0* и др. Создание соответствующих метрик и мер квантовой устойчивости блокчейн Цифровой экономики Российской Федерации. Выработка рекомендаций по обеспечения требуемой квантовой устойчивости упомянутых блокчейн.

2) Разработка алгоритмов синтеза постквантовых криптопримитивов для блокчейн *Enterprise Ethereum Alliance (Эфириум 2.0), Waves Enterprise (Waves, Vostok), Мастерчейн 2.0* на основе разделов математики, потенциально содержащих сложные вычислительные задачи, для которых не известны эффективные алгоритмы решения. В том числе, на основе *теории решеток, многочленов от многих переменных, теории кодирования, изогений на эллиптических кривых, алгебры октонионов, многочленов Чебышева, теории Кос* и др.

3) Разработка алгоритмов решения задач выбора оптимальных технологий и программ обеспечения квантовой устойчивости блокчейн *Enterprise Ethereum Alliance (Эфириум 2.0), Waves Enterprise (Waves, Vostok), Мастерчейн 2.0* в детерминированных условиях.

4) Разработка архитектуры, инструментальных средств и программного обеспечения синтеза технологий и комплексных планов обеспечения квантовой устойчивости блокчейн *Enterprise Ethereum Alliance (Эфириум 2.0), Waves Enterprise (Waves, Vostok), Мастерчейн 2.0* в условиях классических и квантовых атак злоумышленников. Многокритериальное оценивание, анализ и выбор базовой архитектуры информационной платформы обеспечения квантовой устойчивости упомянутых блокчейн. Определение состава и структуры возможного аналитико-имитационного программного комплекса синтеза технологии обеспечения квантовой устойчивости блокчейн Цифровой экономики Российской Федерации. Разработка новых и модификация существующих инструментальных средств автоматизации решения задач синтеза технологий и программ обеспечения квантовой устойчивости названных блокчейн.

Все перечисленные задачи проекта увязаны с диссертационной работой автора настоящего доклада. Для решения поставленных задач предлагаются следующие методы и подходы: теоретический и системный анализ требований нормативно-правовых актов, научных публикаций, технологий квантовой и постквантовой защиты, а также средств их реализации в ключевых блокчейн-экосистемах и платформах Цифровой экономики Российской Федерации.

Научная новизна проекта заключается в проведенном всестороннем анализе необходимости построения нового метода обеспечения квантовой устойчивости блокчейн Цифровой экономики Российской Федерации в условиях роста квантовой угрозы, анализе требований к упомянутому подходу и соответствующей технологии, ее составных моделей, методов и средств реализации. Предложен новый метод обеспечения квантовой устойчивости блокчейн, который в отличие от других известных методов информационной безопасности позволяет упреждать приведение упомянутых блокчейн к существенным или катастрофическим последствиям в условиях атак злоумышленников с применением квантового компьютера.

К ожидаемым результатам научного проекта относятся.

1. Алгоритмы анализа квантовой устойчивости блокчейн Цифровой экономики Российской Федерации на основе перспективных квантовых алгоритмов. Создание соответствующих метрик и мер квантовой устойчивости блокчейн Enterprise Ethereum Alliance (Эфириум 2.0), Waves Enterprise (Waves, Vostok), Мастерчейн 2.0.

2. Алгоритмы синтеза постквантовых криптопримитивов для блокчейн Цифровой экономики Российской Федерации на основе разделов математики, потенциально содержащих сложные вычислительные задачи, для которых в настоящее время не известны эффективные алгоритмы решения на классических и квантовых вычислителях. В том числе, на основе *теории решеток, многочленов от многих переменных, теории кодирования, изогений на эллиптических кривых, алгебры октонионов, многочленов Чебышева, теории Кос* и др.

3. Методика решения задачи выбора оптимальных технологий и программ обеспечения квантовой устойчивости блокчейн Enterprise Ethereum Alliance (Эфириум 2.0), Waves Enterprise (Waves, Vostok), Мастерчейн 2.0 в детерминированных условиях. Определение содержания и особенностей реализации основных этапов решения задач синтеза технологий и комплексного планирования обеспечения квантовой устойчивости упомянутых блокчейн в условиях классических и квантовых атак злоумышленников.

4. Типовая архитектура инструментальных средств и программного обеспечения для синтеза технологий и комплексных планов обеспечения квантовой устойчивости блокчейн Enterprise Ethereum Alliance (Эфириум 2.0), Waves Enterprise (Waves, Vostok), Мастерчейн 2.0. в условиях классических и квантовых атак злоумышленников.

5. Математическое и программное обеспечение решения задач синтеза технологий и комплексных планов обеспечения квантовой устойчивости блокчейн Enterprise Ethereum Alliance (Эфириум 2.0), Waves Enterprise (Waves, Vostok), Мастерчейн 2.0. в условиях классических и квантовых атак злоумышленников.

СПИСОК ЛИТЕРАТУРЫ

1. Петренко А.С. Динамическая модель квантово-устойчивого блокчейна / А.С. Петренко, С.А. Петренко, М.И. Ожиганова // Журнал «Защита информации. Инсайд». — 2023. — № 2 (110). — с. 44-52.
2. Петренко А.С. Инновационная платформа для квантового криптоанализа известных криптопримитивов блокчейна / А.С. Петренко, С.А. Петренко, А.А. Бучнев // Журнал «Защита информации. Инсайд». — 2023. — № 2 (110). — с. 58-67.
3. Петренко А.С. Метод оценивания квантовой устойчивости блокчейн-платформ / А.С. Петренко, С.А. Петренко // Журнал «Вопросы кибербезопасности». — 2022. — № 3 (49). — с. 2-22.
4. Петренко А.С. Basic Algorithms Quantum Cryptanalysis (Основные алгоритмы квантового криптоанализа) / А.С. Петренко, С.А. Петренко // Журнал «Вопросы кибербезопасности». — 2023. — № 1 (53). — с. 100-115.
5. Петренко А.С. Модель квантовых угроз безопасности для современных блокчейн-платформ / А.С. Петренко, С.А. Петренко, А.Д. Костюков, М.И. Ожиганова // Журнал «Защита информации. Инсайд». — 2022. — № 3 (105). — с. 10-20.
6. Петренко А.С. Метод параметрического выбора криптопримитивов для квантово-устойчивой блокчейн-платформы. Часть I / А.С. Петренко, С.А. Петренко, А.О.

Антонова-Дружинина, М.И. Ожиганова // Журнал «Защита информации. Инсайд». — 2022. — № 4 (106). — с. 24-33.
7. Петренко А.С. Эталонная модель блокчейн-платформы / А.С. Петренко, С.А. Петренко, А.Д. Костюков // Журнал «Защита информации. Инсайд». — 2023. — № 2 (110). — с. 44-52. Журнал «Защита информации. Инсайд». 2022. № 4. (106). с. 34-44.
8. Петренко А.С. Метод параметрического выбора криптопримитивов для квантово-устойчивой блокчейн-платформы. Часть II / А.С. Петренко, С.А. Петренко, А.О. Антонова-Дружинина, М.И. Ожиганова // Журнал «Защита информации. Инсайд». — 2022. — № 5 (107). — с. 20-27.
9. Петренко А.С. Модель угроз безопасности по аналитике зарубежных национальных квантовых программ / А.С. Петренко, С.А. Петренко, М.И. Ожиганова // Журнал «Защита информации. Инсайд». — 2021. — № 4 (100). — с. 50-59.
10. Петренко А.С. Перспективный метод криптоанализа на основе алгоритма Шора / А.С. Петренко, А.М. Романченко // Журнал «Защита информации. Инсайд». — 2020. — № 2 (92). — с. 17-23.

Подтопельный В. В.
Институт цифровых технологий ФГБОУ ВО «КГТУ»,
ст. преподаватель
ionpvv@mail.ru

РАЗРАБОТКА ГИБРИДНОЙ СИСТЕМЫ ПОИСКА, АНАЛИЗА И ПРОГНОЗИРОВАНИЯ СОБЫТИЙ БЕЗОПАСНОСТИ В РАСПРЕДЕЛЁННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ ПРИ НЕОДНОЗНАЧНО ИНТЕРПРЕТИРУЕМЫХ ВХОДНЫХ ДАННЫХ ОБ ИНЦИДЕНТАХ БЕЗОПАСНОСТИ

***Аннотация*:** Изучаются аспекты создания вектора атаки информационных систем. Рассматриваются методики, используемые при построении вектора атаки, характеризуются их особенности, специфика использования Марковских цепей для моделирования атакующих действий нарушителя. Определяется пригодность этих методик для определения параметров вектора с учетом применения элементов искусственного интеллекта при выявлении признаков событий безопасности различных типов. При создании вектора атаки учитываются особенности определения вероятностей переходов системы в различные состояния компрометации сети. Для решения задач поиска атак и формирования их векторов предлагается гибридная система на основе модульной архитектуры. Рассматривается формирование вектора атаки в контексте эксплуатации многоуровневой корпоративной информационной системы. Рассматриваются особенности создания упрощенного вектора атаки с учетом связей между тактиками (состояниями) предложенными в методических документа ФСТЭК.

***Ключевые слова*:** вектор атаки, информационная система, корпоративная сеть, уязвимость, марковские процессы, злоумышленник, тактики, сетевые атаки, угроза

При анализе информационной безопасности (ИБ) автоматизированных систем требуется формировать векторы атак злоумышленников. Для этого в Российской Федерации применяются несколько руководящих документов, последний из которых принят в 2021 году («Методика оценки угроз безопасности информации» (далее – Методика)) [1]. В соответствии с Методикой определение векторов атак производится на основании экспертного мнении специалистов ИБ. При этом использование формальных способов не предусматривается. Марковские цепи позволяют учесть вероятности переходов системы в различные состояния компрометации сети, что может быть полезным при создании вектора атаки.

Для более точного построения вектора атаки и определения его параметров, нужно учесть специфику классификации признакового пространства сетевых аномалий и использовать формальные методы определения последовательности тактик, приведенных в методическом документе. Эти методы должны быть простыми и применимыми на практике при построении модели угроз. Кроме того, требуется учитывать неоднозначность признаков атакующих воздействий, на основе которых выстраивается вектор. Соответственно, необходима разработка технического (программного), математического и алгоритмического обеспечения поиска, анализа и прогнозирования событий безопасности в распределённых информационных системах при неоднозначно интерпретируемых входных данных об

инцидентах безопасности. Для достижения указанных целей требуется решить следующие задачи (задачи научного исследования):

1. Произвести анализ существующих подходов, инструментов поиска и анализа событий безопасности в распределённых информационных системах (ИС) при неоднозначно интерпретируемых входных данных о потенциально опасных, деструктивных воздействиях на ресурсы информационных систем.
2. Определить возможности использования доступных наборов данных для разработки модели анализа и прогнозирования неоднозначно интерпретируемых входных данных. Определить признаки и параметры используемых событий безопасности.
3. Разработать модели поиска, анализа и прогнозирования событий безопасности в распределённых информационных системах.
4. Разработать инструментарий поиска, анализа и прогнозирования событий безопасности в распределённых информационных системах и сравнительный анализ точности разработанных моделей.

Реализация приведенных задач позволит создать гибридную систему поиска, анализа и прогнозирования событий безопасности в распределённых информационных системах при неоднозначно интерпретируемых входных данных об инцидентах безопасности, что является предметом исследования диссертационной работы.

Вектор атаки должен учитывать возможность появления новых сценариев реализации угрозы. При построении такого вектора необходимо учесть факторы, которые могут изменить направление атаки. Кроме того, вектор может состоять из нескольких сегментов, описывающих состояния объектов системы с явными и неявными признаками компрометации. Такой подход особенно полезен при аудите многоуровневых систем, так как он учитывает особенности используемых технологий передачи данных и средств защиты. Продолжение вектора или определение нового направления зависит от успешности предыдущих атакующих последовательностей.

Известны многочисленные методы поиска и анализа вредоносных воздействии, однако в них не учитывается ряд особенностей, свойственных реальным процессам обеспечения ИБ, связанных с прогнозированием вредоносных воздействий при недостаточности сведений о развертывании атак. Существуют следующие методы анализа, применимые к выявлению инцидентов безопасности: статистический анализ, вейвлет-анализ, кластерный анализ, фрактальный анализ, метод опорных векторов, генетические алгоритмы, иммунные системы, нейронные сети, деревья решений, байесовские сети, экспертные системы.

Статистические методы без дополнительной обработки их результатов из-за неверного выбора набора наблюдаемых параметров или неверных размеров обобщения наборов исходных данных могут привести к тому, что модель описания потока сетевого трафика окажется слишком привязанной к конкретному промежутку времени либо слишком обобщенной. Это вызовет ложные тревоги системы или неспособность обнаружения вторжений. Преимущества систем, работающих на основе группы статистических методов, — относительная ясность результатов, их адаптивность к изменению поведения пользователей сети, а также способность к обнаружению модифицированных атак.

Веивлет-анализ помогает в большом объеме данных выделить наиболее весомые области, сгладив незначимые шумы [2]. Суть его состоит в подборе коэффициентов данных о признаках инцидентов, описанного наборами данных, по базисным функциям. В качестве сигнала можно рассматривать объем сетевого трафика в единицу времени [3]. Фрактальный

анализ помогает выявить в сетевом трафике самоподобные интервалы данных на отрезках времени различного масштаба, удовлетворяющие свойству самоподобия [4]. При этом установлено, что аномальный и нормальный трафики характеризуются разными значениями результирующего показателя фрактального анализа (показатель Херста). Это обстоятельство — очевидное преимущество данного метода анализа сетевого трафика, поскольку упрощает принятие решения о наличии вторжения при выявлении аномального трафика.

Кластерный анализ (КА) сетевого трафика помогает выявить в сетевом трафике такие характеристики, с помощью которых его можно будет разбить на отдельные, однозначно разделяемые группы, среди которых будут выделены группы нормального и аномального состояния. Нейронные сети часто применяются как способ обнаружения аномалий. Однако, они требуют большое количество вычислительных ресурсов и время на обучение [5].

Подходы к применению Марковских моделей в задачах оценки и прогнозирования состояния сложных технических объектов в том числе ЗОКИИ рассматриваются в работах Артеменкова С. Л., Алхимова В. И., Баранова С. Н., Беляевой О. Б., Кубарева А.В., Лапсаря А.П., Думина П.Н. Работа (диссертация) Марковой О. С. посвящена рассмотрению вектора атаки в зависимости от психологических склонностей нарушителя (пригодна для внутренних нарушителей) с учетом применения теории вероятности [6]. Особенностью данного исследования является совмещение аспектов психологии нарушителя, которые автор пытается параметризировать, и аспектов процесса атаки. Отдельно следует рассмотреть способы формирования векторов, в том числе, с применением Марковских сетей для определения специфики атакующих воздействий. Обоснование мер защиты информации с применением Марковских цепей в своей работе приводит Носаль И.А.[7]. В других работах проводится попытка рассмотрения этапов сетевых атак с учетом специфики уязвимостей [8,9].

При анализе приведенных исследований нужно отметить:

1. Все рассматриваемые атакующие воздействия предполагают некое начальное состояние (совокупность вероятностей), которое в большинстве случаев совпадает с начальным этапом вектора атаки (разведкой). Однако необходимо отметить, что обнаружение атаки может произойти в момент реализации любого из её этапов. Эти этапы хорошо изложены в Методике ФСТЭК. Соответственно, существует необходимость выстраивать вектор атаки, учитывая:

- специфику динамики негативных воздействий на информационную систему;
- момент обнаружения, сопоставленный с определённым этапом ее продвижения.

Подобный подход позволит использовать вектор для прогнозирования действий злоумышленника, а также определить возможные негативные и скрытые последствия уже реализованных ранее этапов.

2. Следует отметить то, что уязвимость (точнее, факт ее присутствия в каком-либо сегменте ИС, мера ее применимости) эксплуатируется при реализации одной угрозы или множества угроз. Это указывает на то, что последовательность атаки, а также одновременное применение нескольких атак, можно определять, используя вектор уязвимостей, для составления которого можно использовать Марковские цепи. Для этого предварительно нужно параметризировать существующие уязвимости. Это позволит упростить вычисление рисков рассматриваемых систем.

Некоторые сетевые параметры атаки, указывающие на активное использование уязвимостей, могут определяться как маркеры угроз только тогда, когда они используются совместно с другими маркерами или при определенных условиях их (маркеров) проявления.

При этом их фиксация может указывать на простую ошибку передачи данных в сети. Таким образом, само выявление сигнатурных маркеров в некоторых случаях не гарантирует того, что выстроенный вектор атаки соответствует реалиям атакующих воздействий. Более того, повышается вероятность неправильного формирования вектора при получении ошибочных сетевых пакетов в сетях большого масштаба, а также при некорректной настройке маршрутизирующих устройств. Соответственно, вектор атаки, сформированный с учетом вектора уязвимостей, вероятностного характера маркеров атак, будет более точным, а также поможет определить возможные ранее незамеченные уязвимости.

Для восстановления незамеченных ранее, но уже реализованных этапов атаки при использовании векторов, созданных на основе Марковских процессов, можно применять алгоритм Витерби. Это позволит не только прогнозировать атакующие воздействия за счёт уточнения типа атакующих воздействий, но и расследовать инциденты безопасности.

3. В большинстве приведенных работ не рассматривается типология атак, которая влияет на определение вектора атаки, а, соответственно, на параметры вероятности реализации и проявления признаков атаки на различных узлах в сети.

4. Необходимо отметить, что большую проблему представляет определение начального состояния вектора атаки (вектора начальных состояний). Соответственно, для определения входящих вероятностей можно применять различные средства интеллектуального анализа, фиксирующие событие безопасности и использующие методы машинного обучения, нейросетевого анализа, иные вероятностные модели. Подход, позволяющий совместить различные способы определения признаков атакующих воздействий, Марковские цепи для определения вектора атаки, прогнозирования ее развития, может использоваться при построении системы поиска и определения специфики различных угроз. Такая система будет иметь гибридный характер. Она может включать несколько функциональных блоков:

1. Модуль сбора данных о параметрах атак.
2. Модуль анализа данных и сохранения результатов анализа.
3. Анализатор для сетевых или других параметров.
4. Консультационный модуль, использующий Марковские сети, интегрированный в общую подсистему консультации.

Таким образом, учитывая специфику приведённых ранее исследований, можно привести наиболее перспективные методы и способы определения векторов атак, позволяющие решить поставленные в исследовании построения векторов атаки и их прогнозирования задачи. Используются две группы методов. Первая группа включает в свой состав методы искусственного интеллекта, позволяющие определять признаки присутствия реализуемой угрозы в информационной системе. Особо следует отметить то, что искомые угрозы могут не иметь признаков, которые их однозначно идентифицируют. К первой группе методов относится следующее:

1. Методы вычислительного интеллекта. Нейронная сеть. Карты Кохонена, ART-сети, LSTM-сети, Нейронная сеть кластерного типа (позволяет решать противоречивые задачи чувствительности к новым данным и сохранения полученных знаний).

2. Методы машинного обучения. Классификаторы машинного обучения. Байесовская сеть доверия позволяет проводить вероятностный анализ процессов обеспечения безопасности.

3. Методы на основе знаний. Экспертные технологии. Продукционные правила. Они используются для определения последовательности регистрируемых операций.

Ко второй группе относятся методы, позволяющие определять вектор потенциальной или действующей атаки с учетом топологии сети, восстанавливать вектор при расследовании инцидента безопасности

4. Статистические методы. Цепи Маркова для прогнозирования состояний безопасности ЛВС, формирования вектора. Алгоритм Витерби для восстановления вектора атаки. Фильтр Калмана для уточнения данных при формировании вероятностных показателей вектора.

Таким образом, перспективность (новизна исследования) заключается в том, чтобы использовать совмещение нескольких методов анализа признаков событий безопасности с экспертными методами контроля анализа, ориентируясь на вычислительные методы, основанные на Марковских процессах. Комплекс Марковских моделей с учетом формализации типовых атукающих последовательностей (техник и тактик) позволит прогнозировать и выявлять раннее необнаруженные этапы развития вредоносного воздействия на информационные системы.

При построении вектора атаки создается последовательность связанных состояний, которые реализуются в виде череды фиксируемых в определённый период времени событий, маркирующих состояние компрометации на сетевых узлах. Последовательность состояний (маркируемых событий) с учетом периода фиксации и очередности событий, классифицируемых по принадлежности к тактикам, формируется с учетом возможного наличия других векторов атак. Для этого необходимо ассоциировать тактики и состояния, которые будут являться вершинами графа, описывающего Марковские процессы. Это означает что методика ФСТЭК, применяемая на предприятиях получит формализацию, что приведет к меньшей зависимости процессов формирования векторов атак от человеческого фактора (экспертного мнения). Таким образом, при определении вектора атаки в дополнение к методикам ФСТЭК, видам машинного обучения можно использовать векторные Марковские последовательности.

Практическая значимость результатов исследований в области применения гибридного подхода к формированию вектора атаки заключается в возможности, повысить уровень ИБ ресурсов информационных систем, осуществлять оперативное выявление угроз ИБ. Помимо повышения общего уровня безопасности ИБ инфраструктуры предприятия, предложенные решения могут найти применение при проектировании новых информационных инфраструктур и при управлении информационной безопасностью.

В управление информационной безопасностью организаций оперативное реагирование предложено осуществлять на основе нового комплекса моделей прогнозирования, ориентированных на широкий круг возможных ситуации. При этом учитываются: топология сети предприятия, ценность защищаемых информационных ресурсов, потенциальная информированность злоумышленников на текущий момент времени, ограничения на имеемые ресурсы и другие факторы.

СПИСОК ЛИТЕРАТУРЫ

1. Методика оценки угроз безопасности информации Методический документ ФСТЭК России: утв. ФСТЭК России России 5 февраля 2021 г. [Электронный ресурс]. – Режим доступа: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-5-fevralya-2021-g (дата обращения: 02.07.2023)

2. Амосов. О.С., Баена, СГ. Вейвлет-алгоритмы оценивания нестационарных процессов с фрактальной структурой, имеющих неоднородности и нарушения Н Информатика и системы управления. — 2017. — № 2 (52) - С. 85-99.
3. De Castro, L.N., Von Zuben, F.J. Arti6cial Immune Systems: Pай I — Basic Theory and Applications // Universidade Estadual de Campinas, Dezembro de, Technical Report. — 1999. — 95 p.
4. Громов, Ю.Ю., Земской, Н.А., Иванова, О.Г., Лагутин, А.В., Тютюнник, В.М. Фрактальный анализ и процессы в компьютерных сетях: учеб. пособие. — Изд. 2-е, стереотип. — Тамбов: Изд-во Тамб. гос. техн. ун-та, 2007. – 108 с.
5. Jiang, H., Ruan, J. The Application of Genetic Neural Network in Network Intrusion Detection H Journal of computers. — 2009. — Vol. C-4, № 12. - P. 1223-1230.
6. Макарова О. С. Разработка методики прогнозирования динамики изменения вектора компьютерной атаки с точки зрения нарушителя: диссертация на соискание ученой степени кандидата технических наук: 2.3.6 / О. С. Макарова — Екатеринбург, 2021. — 218 с.
7. Носаль И.А. Автор в диссертации «Обоснование мероприятий информационной безопасности социально-важных объектов: диссертация на соискание ученой степени уч. степени канд. техн. наук: 05.13.19: защищена 24.03 2016 г. / Носаль И.А. – СПб., 2015 – 159 с.
8. Петров М.Ю., Фаткиева Р.Р. Модель синтеза распределенных атакующих элементов в компьютерной сети / Петров М.Ю., Фаткиева Р.Р. // Труды учебных заведений связи. – СПб.,2020. – Т. 6, № 2 – С.113 – 120
9. Токарев В.Л., Сычугов А.А. Метод оценки уровня рисков безопасности узлов сети для повышения эффективности размещения иммунных детекторов / Токарев В.Л., Сычугов А.А. // Моделирование, оптимизация и информационные технологии – 2020. – Т. 8, №3 – С. 1-11 [Электронный ресурс]. – Режим доступа: https: //moitvivt.ru/ru/journal/pdf?id=840 (дата обращения: 02.07.2023).

Раковский Д.И.
МТУСИ, ассистент, аспирант кафедры ИБ,
Prophet_alpha@mail.ru

ОБНАРУЖЕНИЕ КОМПЬЮТЕРНЫХ АТАК И ПРЕДУПРЕЖДЕНИЕ НАРУШЕНИЙ ФУНКЦИОНИРОВАНИЯ КОМПЬЮТЕРНЫХ СЕТЕЙ НА ОСНОВЕ МНОГОЗНАЧНЫХ ЗАКОНОМЕРНОСТЕЙ

Аннотация: Обоснована актуальность многозначного подхода к решению задач информационной безопасности. Разработан алгоритм прогнозирования нарушения свойств доступности и целостности компьютерной сети и циркулирующей в ней информации на основе анализа многомерных многозначных временных последовательностей системных журналов, при помощи математического аппарата многозначных зависимостей. Разработан алгоритм классификации многозначных компьютерных атак и нарушений функционирования КС на базе искусственной нейронной сети с множественным выходом. Разработан многозначный алгоритм обнаружения многозначных компьютерных атак на базе архитектуры искусственной нейронной сети типа «автокодировщик». Разработаны и программно реализованы стенды для поддержки диссертационного исследования.

Ключевые слова: компьютерная сеть, многозначная классификация, информационная безопасность, компьютерная атака, классификация компьютерных атак, состояние компьютерной сети, многозначная закономерность.

Актуальность работы.

Современные компьютерные сети (КС) порождают многомерные наборы данных, ассоциированные элементами, входящими в их состав: хосты, поддерживающая инфраструктура, циркулирующая в сети информация [1–4]. Данные могут агрегироваться с системных журналов, сетевых карт, системных датчиков, установленных на каждом из хостов; собираться на уровне маршрутизаторов и коммутаторов, ассоциированных с КС; порождаться исполняемыми программами и приложениями, осуществляющими взаимодействие между собой.

При анализе наборов данных, собранных с таких КС для решения задач информационной безопасности (ИБ), обнаруживаются многозначные записи – обладающие одновременно несколькими классовыми метками. Многозначная классификация в задаче ИБ данных является актуальной задачей, поскольку большая часть исследований в области многозначности сконцентрировано в рамках анализа текста и изображений. Наиболее релевантный репозиторий многозначных наборов данных UCO.ES [5], содержащий более 80 наборов данных, не содержит наборов данных, ассоциированных с ИБ или КС.

Отдельными авторскими коллективами предлагаются собственные, сравнительно небольшие (до 1 ГБ), многозначные наборы данных. Примером является многозначный набор данных web-атак SR-BH 2020 [6], впервые представленный в [7].

Тем не менее, некоторые крупные и широко известные наборы данных, релевантные для задач ИБ, помеченные как однозначные, обладают свойствами многозначности. Например, в наборе данных UNSW-NB15 [8] имеется около 0.1% многозначных записей [9]. Как правило, исследователями таких наборов данных многозначность игнорируется.

Наиболее существенными недостатками известных методов работы с многозначными данными являются[10]: игнорирование корреляционных связей между метками, ассоциированными с многозначными экспериментальными данными (ЭД), что ухудшает эффективность решения задачи классификации (часть алгоритмов, ассоциированных с подходом адаптации алгоритмов; некоторые методы, ассоциированные с подходом преобразования многозначности в «классическую» однозначность); экспоненциальный рост необходимых экспериментальных данных в зависимости от размерности пространства классовых меток; либо игнорирование многозначности данных.

Степень разработанности темы.

Вопросам применения многозначного анализа для решения задач информационной безопасности посвящен ряд работ отечественных и зарубежных авторов.

Областью исследования является разработка научных методов, алгоритмов и программ, направленных на повышение эффективности алгоритмов обнаружения компьютерных атак и предупреждения нарушений функционирования компьютерных сетей на основе учета многозначности экспериментальных данных.

Целью проекта, а также диссертации, является повышение эффективности алгоритмов обнаружения компьютерных атак и предупреждения нарушений функционирования компьютерных сетей на основе учета многозначности экспериментальных данных.

Задачами исследования являются:

1. Обоснование актуальности многозначного подхода к решению задач информационной безопасности (обнаружения компьютерных атак и предупреждения нарушений функционирования КС) методами многозначного анализа временных рядов системных журналов и телеметрии КС.

2. Разработка нового алгоритма прогнозирования состояний КС на основе многозначных зависимостей, позволяющего повысить эффективность предупреждения нарушений функционирования КС за счет прогнозирования категориального временного ряда.

3. Разработка нового алгоритма ***классификации*** многозначных *компьютерных атак* на базе многозначных зависимостей, ассоциированных как с нарушением профиля нормального функционирования, так и с проведением компьютерных атак.

4. Разработка нового многозначного алгоритма ***обнаружения*** многозначных *компьютерных атак* на базе архитектуры искусственной нейронной сети типа «автокодировщик».

5. Разработка стенда для моделирования многозначных компьютерных атак в контролируемых условиях.

Объект исследования: классификация и прогнозирование компьютерных атак нарушений функционирования (состояний) КС.

Исторические данные, преобразованные к табличному виду посредством ряда манипуляций [11], могут быть представлены в виде таблицы размером *M* столбцов на *N* строк:

$$\boldsymbol{D}_{NM} = \left\{ \left(\boldsymbol{A}(n,\ ), set_n \right); \boldsymbol{A} = \left(a_{nm} \right), m = \overline{1,M}, n = \overline{1,N} \right\}, \quad (1)$$

где *n*-ной строке значений атрибутов записи $\boldsymbol{A}(n,\ )$ ставится в соответствие множество меток set_n. Множество меток set_n ассоциируется с решающими правилами и контекстом решаемой задачи.

В исследуемом случае рассматривается многозначность классовых меток, соответствующих наличию (отсутствию) компьютерной атаки. Предполагается возможность одновременного возникновения нескольких классовых меток.

Извлечение таких множеств в отдельное упорядоченное множество осуществляется по правилу:

$$f : \boldsymbol{D}_{NM} \to \boldsymbol{L}_n; \boldsymbol{L}_n = \left(set_n; n = \overline{1, N} \right), \quad (2)$$

где $\boldsymbol{D}_{NM}$ – табличное представление размеченных экспериментальных данных, а $\boldsymbol{L}_n$ является множеством меток set_n. «Алфавит», образованный уникальными элементами множества L_n сведем в отдельное множество S:

$$S = \bigcup_{n=1}^{N} set_n , \quad (3)$$

в котором объединены все элементы $\boldsymbol{L}_n$. Поскольку S не является мультимножеством, повторяющиеся элементы исключаются, что позволяет получить все уникальные классовые метки, содержащиеся в «исторических данных».

Немаркированные, «новые» данные одинаковой размерности с «историческими данными» (2), представляются в виде:

$$\hat{\boldsymbol{D}}_{\hat{N}M} = \left\{ \hat{\boldsymbol{A}}(\hat{n},); \hat{\boldsymbol{A}} = \left(\hat{a}_{\hat{n}m} \right), m = \overline{1, M}, \hat{n} = \overline{1, \hat{N}} \right\}, \quad (4)$$

где $\hat{N} \in \mathbb{N}$ - количество неразмеченных данных, $\hat{\boldsymbol{A}}(\hat{n},)$ - $\hat{n}$-я строка в наборе неразмеченных экспериментальных данных.

Под классификацией немаркированной записи понимается процесс отображения немаркированной $\hat{n}$-той записи (вектора-строки) $\hat{\boldsymbol{A}}(\hat{n},)$ в соответствующий набор классовых меток $set_{\hat{n}}$.

Методами исследования поставленной задачи классификации являются системный анализ, теория графов, теория множеств, теория мягких множеств, математическая статистика, методы синтеза искусственных нейронных сетей, методы машинного обучения и интеллектуального анализа данных.

Решение поставленной задачи осуществлено за счет учета многозначности как классовых меток, так и нелинейных взаимосвязей между атрибутами данных, поступающих на вход разработанным алгоритмам.

Научная новизна исследования состоит в следующем:

1. Разработан новый алгоритм прогнозирования нарушения свойств *доступности и целостности* компьютерной сети и циркулирующей в ней информации на основе анализа многомерных многозначных временных последовательностей системных журналов, при помощи математического аппарата многозначных зависимостей.

2. Разработан новый, более эффективный, алгоритм ***классификации*** многозначных *компьютерных атак* и нарушений функционирования КС на базе искусственной нейронной сети с множественным выходом.

3. Разработан новый, более эффективный, многозначный алгоритм ***обнаружения*** многозначных *компьютерных атак* на базе архитектуры искусственной нейронной сети типа «автокодировщик».

Научные результаты соответствуют соответствует пункту №6 паспорта научной специальности 2.3.6. «Методы и системы защиты информации, информационная

безопасность» - «Методы, **модели** и средства **мониторинга**, **предупреждения**, **обнаружения** и противодействия **нарушениям и компьютерным атакам в компьютерных сетях**».

Практическая ценность полученных результатов состоит в следующем:

1. Программно реализован новый алгоритм прогнозирования нарушения свойств *доступности и целостности* компьютерной сети и циркулирующей в ней информации на основании анализа многомерных временных последовательностей «исторических данных» и выявления на их основе многозначных зависимостей при помощи математического аппарата точечно-множественных отображений [12,13].

2. Программно реализован алгоритм ***классификации*** многозначных *компьютерных атак* на базе многозначных зависимостей, ассоциированных как с нарушением профиля нормального функционирования, так и с проведением компьютерных атак [14].

3. Программно реализован многозначный алгоритм ***обнаружения*** многозначных *компьютерных атак* на базе архитектуры искусственной нейронной сети типа «автокодировщик».

4. Разработан стенд для моделирования многозначных компьютерных атак в контролируемых условиях.

5. Разработан и программно реализован исследовательский фреймворк для решения задач информационной безопасности - обнаружения компьютерных атак и мониторинга нарушений функционирования КС методами машинного обучения, реализующий концепцию многозначной, многоклассовой классификации.

6. Разработан и программно реализован исследовательский фреймворк для исследования гиперпараметров ИНС с множественным выходом в рамках концепции многозначной классификации.

СПИСОК ЛИТЕРАТУРЫ

1. Шелухин О.И., Раковский Д.И. Бинарная классификация многоатрибутных размеченных аномальных событий компьютерных систем с помощью алгоритма SVDD // Наукоемкие Технологии В Космических Исследованиях Земли. 2021. Т. 13, № 2. С. 74–84с. DOI: 10.36724/2409-5419-2021-13-2-74-84.
2. Шелухин О.И., Раковский Д.И. Выбор метрических атрибутов редких аномальных событий компьютерной системы методами интеллектуального анализа данных // T-Comm: Телекоммуникации И Транспорт. 2021. Т. 15, № 6. С. 40–47с. DOI: 10.36724/2072-8735-2021-15-6-40-47.
3. Rakovskiy D.I. Analysis of the problem of multivalued of class labels on the security of computer networks // Synchroinfo Journal. 2022. Т. 8, № 6. С. 10–17с. DOI: 10.36724/2664-066X-2022-8-6-10-17.
4. Sheluhin O.I., Rakovskiy D.I. Multi-Label Learning in Computer Networks // 2023 Systems of Signals Generating and Processing in the Field of on Board Communications. Moscow, Russian Federation: IEEE, 2023. С. 1–5с. DOI: 10.1109/IEEECONF56737.2023.10092157.
5. Multi-Label Classification Dataset Repository – Knowledge Discovery and Intelligent Systems – KDIS – University of Córdoba [Электронный ресурс]. URL: http://www.uco.es/kdis/mllresources/ (дата обращения: 03.09.2023).
6. Sureda Riera T., Bermejo Higuera J.R., Bermejo Higuera J., Sicilia Montalvo J.A., Martínez Herráiz J.J. SR-BH 2020 multi-label dataset. Harvard Dataverse, 2022. с. DOI: 10.7910/DVN/OGOIXX.

7. Riera T.S., Higuera J.-R.B., Higuera J.B., Herraiz J.-J.M., Montalvo J.-A.S. A new multi-label dataset for Web attacks CAPEC classification using machine learning techniques // Computers & Security. 2022. Т. 120. С. 102788c. DOI: 10.1016/j.cose.2022.102788.
8. ADFA | UNSW Canberra [Электронный ресурс] // UNSW Sites. URL: https://www.unsw.edu.au/canberra (дата обращения: 20.08.2023).
9. Иванникова В.П., Шелухин О.И. Бинарная классификация компьютерных атак на примере базы данных UNSW-NB15 // Телекоммуникации И Информационные Технологии. 2020. Т. 7, № 1. С. 10–18.
10. Раковский Д.И. Влияние проблемы многозначности меток классов системных журналов на защищенность компьютерных сетей // Наукоемкие Технологии В Космических Исследованиях Земли. 2023. Т. 15, № 1. С. 48–56с. DOI: 10.36724/2409-5419-2023-15-1-48-56.
11. Шелухин О.И., Раковский Д.И. Многозначная классификация меток классов системных журналов компьютерных сетей. Сравнительный анализ эффективности классификаторов // Вопросы кибербезопасности. 2023. Т. 55, № 3. С. 62–77с. DOI: 10.21681/2311-3456-3-62-77.
12. Шелухин О.И., Раковский Д.И. Прогнозирование профиля функционирования компьютерной системы на основе многозначных закономерностей // Вопросы Кибербезопасности. 2022. № 6 (52). С. 53–70с. DOI: 10.21681/2311-3456-2022-6-53-70.
13. Sheluhin O.I., Osin A.V., Rakovsky D.I. New Algorithm for Predicting the States of a Computer Network Using Multivalued Dependencies // Aut. Control Comp. Sci. 2023. Т. 57, № 1. С. 48–60с. DOI: 10.3103/S0146411623010091.
14. Шелухин О.И., Раковский Д.И. Многозначная классификация компьютерных атак с использованием искусственных нейронных сетей с множественным выходом // Труды учебных заведений связи. Т. 9, № 4. С. 95–111с. DOI: 10.31854/1813-324X-2023-9-4-95-111.

Рыбкина О.В.
Дальневосточный государственный университет путей сообщения,
старший преподаватель кафедры «Информационные технологии и системы»,
itis_dvgups@mail.ru

ПОСТРОЕНИЕ ДИНАМИЧЕСКОЙ МОДЕЛИ ЗАЩИТЫ ИНФОРМАЦИОННОЙ СИСТЕМЫ ОТ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ОСНОВЕ ТЕОРИИ СТОХАСТИЧЕСКИХ ДИФФЕРЕНЦИАЛЬНЫХ УРАВНЕНИЙ

Аннотация: предлагается математическая динамическая модель защиты информационной системы от угроз информационной безопасности, учитывающая случайные процессы: винеровские возмущения и скачки пуассоновского процесса. При разработке моделей безопасности угроз использование данной теории является новым направлением исследований и ранее не рассматривалось. Внесение в модель защиты информационной системы от угроз ИБ случайных возмущений в виде непрерывных (винеровский процесс) и скачкообразных (пуассоновский процесс) компонент, позволяет строить модель исследуемого явления, более приближенную к реальности. Введение же в систему программного управления с вероятностью 1 позволит в свою очередь, практически мгновенно, реагировать на поступающие угрозы. В результате полученная модель позволит поддерживать информационную систему в работоспособном состоянии, отслеживать поступающие угрозы и своевременно на них реагировать.

Ключевые слова: математическая модель защиты информации, математическое моделирование, система стохастических дифференциальных уравнений, динамическая модель угроз информационной безопасности.

Основной целью исследования является построение динамической модели защиты информационной системы от угроз ИБ на основе теории стохастических дифференциальных уравнений. Данное исследование строится на уже рассмотренной ранее детерминированной модели и является логическим продолжением исследований, проводимых в рамках диссертационной работы на тему «Разработка динамической модели защиты информационной безопасности на основе теории инвариантов».

Для реализации данной цели необходимо решить следующие задачи:

- Построение стохастической модели защиты информационной системы от угроз ИБ с управлением, позволяющим с вероятностью 1 сохранять наиболее важные инварианты системы.
- Исследование стохастической модели защиты информационной системы от угроз ИБ в зависимости от показателей входящих информационных потоков.
- Проверка построенной стохастической модели на адекватность с помощью компьютерного моделирования.

На сегодняшний день актуальной проблемой является разработка моделей, которые учитывают динамику изменения данных. Наибольший интерес представляют разработки, основанные на применении математического аппарата [1].

К моделям, учитывающим динамику изменения данных, можно отнести работы, основанные на марковских случайных процессах, учитывающих состояния системы и переход системы из одного состояния в другое.

Росенко А.П. и Бордак И.В. [2] беря за основу применение марковского случайного процесса к информационной системе, рассматривают модель определения вероятности последствий от реализации угрозы, что позволило в дальнейшем дать количественную оценку безопасности информации и применить полученные данные для возможного повышения уровня защищенности информации.

Обоснование применимости марковских процессов при моделировании угроз безопасности было рассмотрено в работе Щеглова К.А., Щеглова А.Ю. [3], а также моделирование системы с отказами и восстановлениями [4].

Вопросы моделирования обеспечения целостности данных, а также эффективность процессов противодействия такого рода угрозам затрагиваются в работе Душкина А.В., Демченкова А.В. [5]. Для комплексной оценки эффективности защиты данных от угроз искажения строится аналитическая модель. Принимая условие, при котором злоумышленнику удается реализовать угрозу и учитывая случайный характер временных величин и теории вероятностей строятся показатели эффективности обеспечения защиты данных от угроз преднамеренного и непреднамеренного характера, что позволяет количественно оценить необходимые направления совершенствования защиты данных от угроз их целостности.

Горбылев А.Л., и Горбылева Е.Л. [6] рассматривают линейную динамическую модель угроз безопасности информации, где вводятся динамические характеристики, такие как конфиденциальность, доступность, целостность и строится динамическая система уравнений. Предлагается способ моделирования, позволяющий дать объективную оценку баланса между угрозами безопасности информации, мероприятиями по защите и объемом защищаемой информации.

Антипов А.Л. и Труфанов А.И. [7] предлагают модель динамической адаптивной защиты, выступающей аналогом иммунной системы биологического организма. При создании модели системы ИБ используется концепция построения иммунного ответа биологического организма на вводимый антиген. В основе модели лежит динамическое развертывание активной защиты в момент защиты информации.

В работе Варлатой С.К., Шаханова М.В. [8] рассматривается математическая модель динамики возникновения и реализации угроз, в которой предлагаются вероятностные показатели, позволяющие оценить вероятность возникновения угроз в заданные промежутки времени. Метод основан на теории стохастических систем массового обслуживания.

Коллектива авторов Геворкян М.Н., Демидова А.В., Демидова Т.С., Соболев А.А. [9] рассматривают модель распространения сетевых червей с помощью стохастических дифференциальных уравнений. За основу берется SIR модель, описывающая затухающие сетевые эпидемии.

Непосредственно SIR-модель и ее применение к вопросам распространения эпидемий компьютерных вирусов, рассматриваются в работах Давыдова В.В. [10], Семенова С.Г. [11], Качалина А.И. [12], Минаева В.А., Сычева М.П., Вайц Е.В. и Киракосяна А.Э. [13]. Давыдов В.В. и Семенов С.Г. рассматривают сравнительную характеристику существующих разновидностей SIR-модели и приводят их усовершенствованные версии применимые при распространении эпидемий компьютерных вирусов. В работе Качалина А.И. рассматривается обобщенная модель распространения сетевых червей, с подробным рассмотрением этапов развития эпидемии и возможные решения проблемы на каждом из этапов. Рассмотрение SIR-модели с точки зрения имитационного моделирования предлагается в работе коллектива

авторов Минаева В.А., Сычева М.П., Вайц Е.В. и Киракосяна А.Э., что позволяет управлять эпидемией, прогнозировать ее течение, подбирать методы противодействия.

Таким образом, проведя анализ современного состояния исследований в данной области были определены актуальные проблемы и определены основные методы, которые будут служить инструментом для дальнейших исследований.

Для решения поставленных задач будет использована теория случайных процессов, теория стохастических дифференциальных уравнений Ито, математическая теория управления.

В качестве основного метода исследования будет применен метод построения систем стохастических дифференциальных уравнений с винеровскими и пуассоновскими возмущениями, имеющий заданный набор гладких функций в качестве первых интегралов (глобальных инвариантов), предложенный Карачанской Е.В. [14-16]. Предложенный метод построения основан на существовании для системы стохастических дифференциальных уравнений с винеровскими и пуассоновским возмущениями инварианта – первого интеграла и применении метода программного управления с вероятностью 1.

Рассматривая защиту информационной системы от угроз информационной безопасности, как динамическую систему, можно предположить, что существуют инварианты, позволяющие данной системе оставаться в защищенном состоянии. Исходя из множества таких инвариантов, строится множество систем стохастических дифференциальных уравнений с помощью подбора дополнительных функций, из которых выбирается тот набор систем, вид которых позволяет провести адекватную трактовку коэффициентов системы и начальных условий. В случае добавления стохастических слагаемых в уравнения уже существующей детерминированной модели, сохранение инвариантов будет гарантировано внесением в стохастическую систему компенсатора – программного управления с вероятностью 1. Таким образом, учитывая сохранение наиболее важных инвариантов, можно построить математическую динамическую модель защиты информационной системы от угроз информационной безопасности с инвариантным управлением. Полученная модель позволит в режиме реального времени отражать (блокировать) опасный входящий информационный поток. В такой постановке задача построения модели защиты информационной системы от угроз информационной безопасности не рассматривалась. Построение математической модели защиты информационной системы от угроз информационной безопасности с учетом сохранения заданных инвариантов ранее не рассматривалось. Введение программного управления с вероятностью 1 позволит построить управляемую математическую модель с мгновенной обратной связью, что означает возможность оперативно реагировать на поступающие угрозы.

Для построения математической модели, ее исследования и адаптации к реальным условиям будет использован математический пакет MathCad.

В ходе исследований будет получена математическая динамическая модель защиты информационной системы от угроз информационной безопасности, позволяющая поддерживать информационную систему в работоспособном состоянии, отслеживать поступающие угрозы и своевременно на них реагировать. Результаты данного исследования в рамках программы развития цифровой экономики Российской Федерации соответствуют базовому направлению «Информационная безопасности» и могут служить одним из средств для достижения цели обеспечения состояния защищенности личности, общества и государства от внутренних и внешних информационных угроз. Результаты данных

исследований могут быть взяты за основу при подготовке новых публикаций, создании программного обеспечения в области защиты информации, внедрены в учебный процесс при подготовке специалистов направления 10.05.03 «Информационная безопасность автоматизированных систем», а также магистров направления 10.04.01 «Информационная безопасность».

СПИСОК ЛИТЕРАТУРЫ

1. Дорогинина (Рыбкина) О.В. О математических моделях угроз безопасности информации / О.В. Дорогинина, Е.В. Карачанская, // Информационные системы и технологии. – 2020. – № 3 (119). – С. 113-123.
2. Росенко А. П. Математическая модель определения вероятности последствий от реализации злоумышленником угроз безопасности информации ограниченного распространения / А. П. Росенко, И. В. Бордак // Известия ЮФУ. Технические науки. – 2015. – № 7 (168). – С. 6-19.
3. Щеглов К. А. Марковские модели угрозы безопасности информационной системы / К. А. Щеглов, А. Ю. Щеглов // Изв. Вузов. Приборостроение. – 2015. – Т. 58, № 12. – С. 957-965.
4. Щеглов К. А. Моделирование угрозы безопасности информационной системы с использованием аппроксимирующих функций / К. А. Щеглов, А. Ю. Щеглов // Изв. Вузов. Приборостроение. – 2016. – Т. 59, № 1. – С. 50-59.
5. Душкин А. В. Аналитическая модель оценки эффективности обеспечения защиты данных от угроз нарушения целостности в информационных системах / А. В. Душкин, А. В. Демченков // ВЕСТНИК ВВИ МВД России. – 2015. – № 1.
6. Горбылев А. Л. Линейная динамическая модель угроз безопасности информации / А. Л. Горбылев, Е. Л. Горбылева // Безопасность информационных технологий. – 2018. – Том 26, № 3. – С. 53-66.
7. Антипов А. Л. Модель динамической адаптивной иерархической системы информационной безопасности / А. Л. Антипов, А. И. Труфанов // Безопасность информационных технологий. – 2008. – Т. 15, № 3. – С. 76-82.
8. Варлатая С. К. Математические модели динамики возникновения и реализации угроз / С. К. Варлатая, М. В. Шаханова // Доклады ТУСУРа. – 2012. – № 1(25), часть 2. – С. 7-11.
9. Геворкян М. Н. Моделирование распространения сетевых червей с помощью стохастических дифференциальных уравнений / М. Н. Геворкян, А.В. Демидова, Т.С. Демидова, А.А. Соболев // Информационно-телекоммуникационные технологии и математическое моделирование высокотехнологических систем: материалы Всероссийской конференции с международным участием. – Москва: РУДН, 2018. – С. 314-317.
10. Давыдов В. В. Сравнительный анализ моделей распространения компьютерных вирусов в автоматизированных системах управления технологическим процессом / Системи обробки інформації. – Харків: ХУПС, 2012. – Вип. 3 (101). – Том 2. – С. 147 – 151.
11. Давыдов В. В. Математическая модель распространения компьютерных вирусов в гетерогенных компьютерных сетях автоматизированных систем управления технологическим процессом / В. В. Давыдов, С.Г. Семенов // Вестник НТУ ХПИ. – Харьков: – 2012. – № 38. – С. 163 – 171.

12. Качалин А.И. Моделирование процесса распространения сетевых червей для оптимизации защиты корпоративной сети // Искусственный интеллект. – 2006. – № 2, 2006. – С. 84-87.
13. Минаев В.А. Имитационное моделирование эпидемий компьютерных вирусов / В.А. Минаев, М.П. Сычев, Е.В. Вайц, А.Э. Киракосян // Вестник Российского нового университета. – 2019. – № 3. – С. 3-12.
14. Карачанская Е. В. Обобщенная формула Ито–Вентцеля для случая нецентрированной пуассоновской меры, стохастический первый интеграл и первый интеграл // Математические труды. – 2014. – Т.17. № 1, – С. 99-122.
15. Карачанская Е. В. Построение программных управлений с вероятностью 1 для динамической системы с пуассоновскими возмущениями // Вестник Тихоокеанского госуниверситета. –2011. – № 2(21). – С.51-60.
16. Карачанская Е. В. Моделирование систем дифференциальных уравнений с динамическими инвариантами. // Математическое моделирование и численные методы. – 2019. – № 1. – С. 98-117.

Салманов В.Д.
Кафедра Безопасности информационных технологий
им. О.Б. Макаревича, ИКТИБ ИТА ЮФУ, ассистент
vsalmanov@sfedu.ru

МЕТОДИКА ОЦЕНКИ НАДЕЖНОСТИ СОВРЕМЕННЫХ СИСТЕМ РАСПРЕДЕЛЕННОГО РЕЕСТРА

Аннотация: Системы распределенного реестра стали занимать отдельную нишу в современном стеке информационных технологий. Перед разработчиком приложений на базе блокчейн технологий стоит сложный выбор – он заключается в выборе платформы, на которой будет строиться взаимодействие пользователей его приложения. За последние пять лет появилось более ста платформ и для пользователей, а иногда и для разработчиков, сложно сориентироваться в этом разнообразии, понять какая из платформ подходит для него, и разумеется, какая из них будет соответствовать заявляемым требованиям, в том числе обеспечивать необходимый уровень безопасности данных.

Данный проект направлен на формирование методики оценки надежности современных систем распределенного реестра. В ходе работы над проектом будет проведен сравнительный анализ платформ и выявлены их ключевые характеристики, после чего будет сформирован универсальный эмулятор блокчейн платформы. Он позволит спрогнозировать поведение системы при различной степени нагрузки, удостоверившись тем самым в устойчивости сети.

Достигнув критического состояния системы, будут сделаны выводы о надежности работы системы, в том числе стоимости и сложности проведения атаки на уязвимые компоненты системы. Исходя из полученных результатов, будет представлена методика, которая позволит разработчику самостоятельно оценить надежность платформы, с которой ему предстоит работать.

Ключевые слова: блокчейн, распределенные реестры, эмулятор, модель блокчейн сети, одноранговая сеть, децентрализация.

Цели и задачи научного проекта в рамках реализации гранта

Основной целью проекта является составление методики определения надежности работы с различными блокчейн платформами.

Для выполнения поставленной цели формулируются следующие задачи необходимые к выполнению:

- изучить существующие блокчейн платформы на предмет их характеристик, текущего числа пользователей, свойств масштабируемости, частоты обновлений программного кода, частоты атак на платформу и т.д.;
- выделить основные функциональные недостатки для каждой сети или группы однотипных сетей;
- реализовать алгоритм моделирования работы блокчейн сети при различных параметрах нагрузки, в том числе количестве пользователей, количестве транзакций в секунду, объеме транзакции;
- экспериментально выявить наиболее эффективные параметры функционирования сети в критическом состоянии;

- оценить вероятность наступления условий для каждой из рассматриваемых сетей, оценить потенциальную стоимость атаки с целью выведения сети или ее компонентов из строя;

- разработать методику выбора наименее уязвимой системы при постановке конкретной задачи для работы с системой распределенного реестра.

Анализ современного состояния исследований в данной области

В ходе анализа технической литературы выявлено небольшое количество источников по сравнению с другими предметными областями. Конечно, это связано с новизной технологии, ее стремительным развитием. В русскоязычном сегменте основную часть научных работ составляют мнения специалистов о применении блокчейна в финансовой индустрии, госсекторе и других отраслях, рассматриваются ведущие мировые и российские блокчейн-стартапы [1]. Появляются описания тех или иных разработок, базирующихся на существующих платформах распределенного реестра [2][3]. Эти решения применяются как в частном секторе между пользователями платформ, так и используются юридическими лицами.

В основном все исследования и дискуссии в научном сообществе направлены на оценку перспектив технологии, оценивается ее развитие в ближайшем будущем [4]. Ведутся споры о необходимости использования и внедрения в различные сферы жизни общества. Чаще всего системы распределенного реестра упоминаются в контексте цифровой экономики, тем или иным образом связывая технологию с денежным обращением [5].

Что касается англоязычной литературы, то уже существует достаточный объем достоверных источников информации, на которые можно опираться в своих исследованиях. Некоторые авторы описывают разработку новых гибридных протоколов взаимодействия пользователей [6], ими приводятся преимущества и недостатки объединенной модели двух алгоритмов консенсуса, рассматриваются проблемы информационной безопасности, которые этим могут быть вызваны. В работе [7] описываются варианты взаимодействия систем распределенного реестра с технологиями облачных вычислений. Новый подход к построению инфраструктуры по информации авторов позволил им обеспечить гораздо более высокий уровень целостности системы, усилить контроль доступа к данным и защитить конфиденциальную информацию, устранить недостатки современных протоколов аутентификации. Доклад [8] посвящен непосредственно возможным уязвимостям в работе протокола обработки транзакций в блокчейн-системе, которые могут стать причиной проблемы двойной траты, описаны возможные последствия реализации этой уязвимости, указаны методы, которыми можно добиться как практической, так и теоретической стойкости в работе платформ.

Профессиональное сообщество постоянно обсуждает вопросы масштабируемости той или иной сети [9]. Рост самых популярных платформ-гигантов, таких как Ethereum и BitCoin, удивляет как скоростью появления новых пользователей, так и новых продуктов на платформах. Систем достаточно сбалансированы и автоматически подстраиваются под текущие условия существования, сохраняя уровень надежности работы. Крупнейшие биржи, обменники, мосты между сетями, различные токенизированные активы, модули игровых приложений – все находит место на платформах и получает заявленную скорость и безопасность. Однако еще больше удивляет экстенсивный рост платформ – базируясь на открытом коде первоисточника, многие старт-апы запускают свои платформы. Не получив должного внимания и проработки, такие программные решения накапливают в себе большое количество уязвимостей и не имеют возможности к дальнейшему развитию, формируя целый

ряд потенциальных рисков для своего, пусть и не многочисленного, количества пользователей.

В статье [10] опубликованы примеры уязвимостей смарт-контрактов на Solidity на примере атак на опубликованные контракты. Известно, что в ходе использования уязвимости в смарт-контракте, который использовался инвесторским фондом было похищено ⅓ активов - $50 млн [11]. Так, из-за уязвимости контракта Ethereum к обратному вызову платформа кредитования DeFi потеряла $25 млн, так как пользователи могли рекурсивно вызывать получение средств от смарт-контракта, тем самым увеличивая свой капитал. В статье [12] показано, как мелкие ошибки в компиляторе Vyper для платформы Ethereum привели к тому, что создатели Ethereum отказались от использования Vyper как официального языка для написания смарт-контрактов. Известны случаи, когда ошибки,совершенные в контракте, приводили к большим финансовым потерям. В статье [13] описан сценарий, пользуясь которым злоумышленники использовали статус hard_fail и задержки в транзакций для проведения атаки ложного пополнения. Помимо ошибок в смарт-контрактах, при реализации приложений разработчики часто допускают ошибки в протоколах формирования и распространения ключей. Так, злоумышленникам удалось получить ключи большого количества кошельков и некоторые коды двухфакторной авторизации из-за ненадежного ресурса генерации ключей [14].

Сегодня одним из важных направлений обеспечения безопасности блокчейн решений является предварительный аудит кода смарт-контрактов. Эта процедура позволяет авторам системы получить квалифицированное мнение специалиста относительно уязвимостей в программном коде и своевременно их устранить. Для этого используются новые подходы к анализу кода, чаще это методы статического анализа, которые позволяют изучить с точки зрения определенных паттернов программирования, привычных последовательностей команд, а также оптимизировать код, обеспечив к тому же его более стабильную работу и сократить расходы на его выполнение в блокчейн сети [15].

Подводя итог обзора, можно сказать, что это всего лишь обобщенная картина из нескольких категорий уязвимостей. Относительно достаточно комплексного анализа работы протоколов и сетей пока не существует полноценных работ, которые содержали бы в себе достаточное количество исследовательского опыта. Разработчикам проектов остается ориентироваться только на заверения создателей используемых платформ и отсутствие известных инцидентов безопасности.

Предлагаемые методы и подходы к решению поставленных задач

Для выполнения задач, описанных в пункте 1, изначально необходимо сформировать пул рассматриваемых сетей. На сегодняшний день существует более ста различных блокчейн платформ, определенным образом отличающихся друг от друга. Необходимо определить критерии, по которым будут отобраны платформы, которые станут объектами исследования. После этого необходимо полноценно овладеть технической информацией относительно рассматриваемых платформ и определить перечень характеристик и параметров систем как предметов исследования.

Выделив необходимые для изучения критерии, необходимо определить значимость каждого критерия на работу сети, способы его изменения, взаимозависимость критериев друг от друга, порядки значений каждого критерия. На базе полученных значений необходимо сформулировать определенную модель влияния параметра на работоспособность сети.

Получив теоретические выводы, будет спроектирован и разработан эмулятор состояния блокчейн сети, работающей при различных параметрах нагрузки – это позволит экспериментально определить критические параметры, после чего предположить причины их возникновения в реальных обстоятельствах. Для разработки основной логической части эмулятора предполагается использовать язык программирования C/C++, для визуальной части эмулятора предполагается использовать средства фреймворка Qt. Также предполагается создать библиотеку для основных логических функций эмулятора, которая будет доступна и полезна всем разработчикам блокчейн-систем. При разработке эмулятора важно учитывать различные параметры системы. Поэтому обязательно надо реализовать функции по учету влияния на систему следующих параметров:

- Структура транзакции
- Механизмы подписи и проверки транзакций
- Структура блока
- Скорость создания блока
- Механизмы проверки блока
- Механизм консенсуса
- Нагрузка сети
- Используемые механизмы криптографии
- Количество узлов сети/количество активных узлов сети
- Размер базы блокчейн

Отталкиваясь от сведений о системе и зная необходимую степень вредоносного воздействия на сеть будут сделаны выводы о стоимости реализации возможной атаки – под стоимостью понимается сочетание затрат финансовых, вычислительных и временных ресурсов злоумышленника.

Исходя из полученных данных будут сделаны выводы о потенциальных рисках для продуктов различной направленности, будут сформированы рекомендации относительно выбора блокчейн платформы под нужды автора проекта с учетом возможных рисков.

Новизна исследования, заявленного в проекте

Новизна проекта обусловлена рядом факторов. Однако ключевой из них – инновационность технологии. Первая блокчейн система BitCoin была запущена только в 2009 году, вторая платформа Ethereum – в 2015 году, впервые популярность и известность технология получила в 2017-2018 году на пике популярности майнинга. В результате – внимание вокруг технологии сосредоточено лишь последние пять лет, в том числе и внимание широкого научного сообщества. Ведется большое количество исследований вокруг темы сетевого взаимодействия пользователей, безопасности узлов в сети, безопасности клиентских приложений, а также безопасности децентрализованных приложений, построенных на базе платформ. Широкая популярность технологии и неуспевающие за ней исследования приводят профессиональное сообщество к формированию огромного рынка продуктов, а разница между ними понятна далеко не всем пользователям и даже разработчикам.

Так разработчик получает огромное количество вариантов сети с абсолютно различными параметрами – структурой транзакций и блоков, размером транзакций и блоков, скоростью передачи и обработки данных, определенным влиянием конкретного механизма консенсуса на работу сети. Все эти параметры могут отразиться на работе децентрализованных приложений, в определенный момент поставив под угрозу обеспечение обрабатываемых конфиденциальных данных или работоспособность сети в целом.

Обширный комплексный анализ, построенный на сравнении используемых в разных платформах технологий, позволит систематизировать средства как минимум на текущем этапе развития технологии, а в ряде случаев будет применим и спустя годы. Разработчик получит универсальный инструмент, который предоставит экспертную оценку выбранной платформе, оценит то, на сколько она приемлема для решения конкретной поставленной задачи.

Ожидаемые по окончании проекта научные результаты

В результате работы над проектом будет:

1. Разработан и реализован программный комплекс, предназначенный для эмуляции работы современных блокчейн систем с возможностью задавать различные параметры системы, такие как количество узлов сети, нагрузка сети, скорость сетевого взаимодействия, архитектура блокчейн (включая структуру транзакций, структуру блоков, используемые механизмы консенсуса) и др. Данный программный комплекс будет предназначен для исследования надежности и работоспособности различных блокчейн систем, как уже существующих, так и только проектируемых.

2. На основе данных, полученных с использованием эмулятора, будет проведен анализ и предложен комплекс мер по выявлению и предотвращению возможных угроз для блокчейн систем, связанных с техническими аспектами реализации таких систем.

3. Будут сформированы методики по работе с блокчейн платформами, в частности рекомендации по выбору платформы для выполнения конкретных задач.

4. Будет получено Свидетельство о регистрации программы для ЭВМ.

5. Будет опубликовано не менее 2 статей в рецензируемых изданиях.

6. Основные значимые результаты будут представлены как минимум на двух научных конференциях.

СПИСОК ЛИТЕРАТУРЫ

1. Блокчейн: как это работает и что ждет нас завтра. Генкин А.С., Михеев А.А., Москва, 2018.
2. Перспективы использования технологии блокчейн в медицинских информационных системах, Л. А. Шевчук, О. В. Ниссенбаум, Математическое и информационное моделирование: сборник научных трудов, Министерство науки и высшего образования РФ, ТГУ – Тюмень : Изд-во Тюм. гос. ун-та, 2018. – Вып. 16. – С. 369-375.
3. Перспективы использования технологии распределенных реестров для автоматизации государственного аудита Варнавский А.В., Бурякова А.О., Управленческие науки. 2018. Т. 8. № 3. С. 88-107.
4. Перспективы внедрения технологии блокчейн, Арефьева А.С., Гогохия Г.Г., Молодой ученый. 2017. № 15 (149). С. 326-330.
5. Блокчейн как коммуникационная основа формирования цифровой экономики: преимущества и проблемы, Пряников М.М., Чугунов А.В., International Journal of Open Information Technologies. 2017. Т. 5. № 6. С. 49-55.
6. Hybrid Consensus: Efficient Consensus in the Permissionless Model, Rafael Pass and Elaine Shi, Cryptology ePrint Archive, 2016.
7. Security through block vault in a blockchain enabled federated cloud framework, Malomo O., Rawat D., Garuba M., Department of Electrical Engineering and Computer Science College of Engineering and Architecture Howard University, Washington, DC, United States

8. Detecting multi-block double spent transaction based on b-tree indexing, Murugan A., Vijayalakshmi J., Department of Computer Science, Dr. Ambedkar Government Arts College, Affiliated to University of Madras, Chennai, India
9. Blockchain scalability and distributed ledger technologies — Sezer Bora Buğra1, Nuriyev Urfat, Informasiya Sistemləri Vətexnologiyalar: Nailiyyətlər Və Perspektivlər, Сумгаитский государственный университет, Азербайджан, 2020.
10. Уязвимости смарт-контрактов блокчейн-платформы Ethereum. – Алиев И.А., Научные записки молодых исследователей, 2019 // https://cyberleninka.ru/article/n/uyazvimosti-smart-kontraktov-blokcheyn-platformy-ethereum/viewer
11. Methods of protecting decentralized autonomous organizations from crashes and attacks – Andryukhin A.A., Proceedings of the institute for system programming of the RAS, pp. 149-164, 2018.
12. Overview of the languages for safe smart contract programming – Tyurin A.V., Tyulyandin I.V., Maltsev V.S., Kirilenko J.A., Berezun D.A., Proceedings of the institute for system programming of the RAS, pp. 157-176, 2019.
13. Analysis on functionalities and security features of internet of things related protocols – Rizzardi A., Sicari S., Coen-Porisini A., Wireless networks 28.7, pp. 2857-2887, 2022.
14. Децентрализованные финансы (defi): риски, перспективы и регулирование – Алешина А.В., Булгаков А.Л., Финансовые рынки и банки №12, сс. 23-28, 2022.
15. Smartcheck: static analysis of ethereum smart contracts – Tikhomirov S., Voskresenskaya E., Ivanitskiy I., Takhaviev R., Marchenko E., Alexandrov Y., Proceedings - 2018 ACM/IEEE 1st International Workshop on Emerging Trends in Software Engineering for Blockchain, pp. 9-16, 2018.

Синадский А.Н.
Исследователь, CyberLympha,
Ассистент, ФГАОУ ВО «УрФУ имени первого Президента России Б.Н. Ельцина»
alexsin@e1.ru

КОМПЛЕКС АЛГОРИТМОВ ВЫЯВЛЕНИЯ АНОМАЛИЙ В КОМПЬЮТЕРНЫХ СЕТЯХ, ИСПОЛЬЗУЮЩИЙ МЕТОДЫ МАШИННОГО ОБУЧЕНИЯ И ОТЛИЧАЮЩИЙСЯ ОТСУТСТВИЕМ ВОЗДЕЙСТВИЯ НА СЕТЕВУЮ ИНФРАСТРУКТУРУ

Аннотация: В статье рассмотрены цели и задачи исследования, направленного на создание комплекса алгоритмов выявления аномалий в компьютерных сетях, использующего методы машинного обучения и отличающегося отсутствием воздействия на сетевую инфраструктуру. Приведён краткий анализ современного состояния исследований в данной области. Описаны новизна исследования и ожидаемые по окончании проекта научные результаты.

Ключевые слова: выявление аномалий, машинное обучение, восстановление структуры сетевого трафика.

Цель исследования заключается в повышении качества работы систем обнаружения атак путём разработки алгоритма выявления аномалий с возможностью интерпретации принятых решений на основе классификации сетевых узлов по генерируемому ими сетевому трафику без априорной информации о его структуре.

Научная задача диссертационного исследования заключается в совершенствовании алгоритмов восстановления структуры сетевых протоколов, определения классификационных характеристик сетевых узлов без активного воздействия на них и интерпретируемого выявления аномальной активности сетевых узлов без применения сигнатурного анализа в компьютерных сетях АСУ ТП.

Практическая цель исследования заключается в повышении качества работы систем обнаружения атак путём разработки алгоритма выявления аномалий с возможностью интерпретации принятых решений на основе классификации сетевых узлов по генерируемому ими сетевому трафику без априорной информации о его структуре.

Теоретическая цель исследования заключается в развитии алгоритмического аппарата восстановления структуры сетевого трафика, определения классификационных признаков сетевых узлов, выявления аномальной активности сетевых узлов.

Цель диссертационной работы достигается последовательным решением следующих частных задач:

1. Систематизация и анализ современного состояния теории и практики, технологий, методов и средств восстановления структуры сетевого трафика, определения классификационных характеристик сетевых узлов и выявления аномальной активности сетевых узлов.
2. Разработка комплекса алгоритмов, в т.ч. восстановления структуры сетевого трафика, определения классов сетевых узлов по генерируемому ими сетевому трафику без воздействия на них, выявления аномалий в активности сетевых узлов по генерируемому ими трафику.

3. Анализ степени достижения цели исследования путём разработки и тестирования прототипа программного обеспечения, реализующего алгоритмы восстановления структуры сетевого трафика, определения классификационных характеристик сетевых узлов и выявления аномальной активности сетевых узлов.

В результате выполнения исследования будет развит научно-методический аппарат восстановления структуры сетевого трафика, определения классификационных признаков сетевых узлов, выявления аномальной сетевой активности, имеющий существенное значение для развития средств обеспечения информационной безопасности.

Также будет предложено новое техническое решение, позволяющее повысить качество работы систем обнаружения атак, что вносит значительный вклад в повышение информационной безопасности компьютерных сетей. Результаты исследования могут быть использованы при подготовке диссертационной работы по соответствующей теме, при создании систем анализа сетевого трафика в составе систем обнаружения атак, а также систем защиты информации в сетях, где состав сетевых узлов, подлежащих защите, априорно не известен.

Методы разделения и классификации информационных потоков исследовались такими учёными, как А.И. Гетьман, Е.Ф. Евстропов, Ю.В. Маркин, Ш. Войт, К. Говард, Д. Филип, К. Пенни. Некоторые методы поиска границ полей на основе анализа последовательностей байт предложены Д. Антюнес, Н. Невес, П. Вериссимо.

Китайская школа исследователей (Р. Ли, Х. Хао, С. Ни, Х. Женг, С, Хиа, Ф. Сун, С. Вонг, С. Жанг, Х. Жанг) подходит к задаче с другой стороны и предлагает оценивать границы адресных полей на основе изменения значений информационной энтропии отдельных байт. Но предлагаемые ими методы используют не все доступные статистические характеристики и задают детерминированный набор условий, что не позволяет получить достаточную точность решения. В исследовании будет предложена доработка алгоритма, заключающаяся в использовании дополнительных статистических свойств сетевого трафика и определении алгоритма создания набора правил с помощью методов машинного обучения.

Учёные, относящиеся к китайской школе, предлагают выделять группы протоколов с помощью оценки расстояния между форматами протоколов. Но у предложенного ими алгоритма есть принципиальная проблема: квадратичная сложность и квадратичный расход памяти, что не позволяет обрабатывать большие объёмы трафика. В исследовании будет предложена доработка алгоритма, позволяющая снизить требования к вычислительной мощности и решить проблему анализа больших объёмов трафика.

Проблема определения устройства-источника по характерным признакам генерируемого сетевого трафика изучалась А.Ж. Пинейро, Ж.М. Безерра, К.А. Бургарт, Д.Р. Кампело. Есть реализованное решение от Kasperskiy, позволяющее определять типы узлов, но оно имеет ограничение в виде фиксированного списка возможных типов, что ограничивает его применимость в сетях АСУ ТП и возможности по адаптации к особенностям защищаемой сети.

В результате, для каждого положения можно сделать следующие выводы.

Существующие на данный момент прототипы и модели систем восстановления структуры сетевых протоколов не всегда эффективны в случае обработки сетевого трафика, пакеты которого могут принадлежать к разным наборам протоколов, поскольку, в основном, основаны на анализе последовательностей байт как непрерывных слов и оценке символьных совпадений [1]. Методы, позволяющие определять структуру пакетов сложного трафика,

используют не все доступные статистические характеристики, поэтому в некоторых случаях их точность оказывается недостаточно высокой [2].

Существующие на данный момент прототипы и модели систем определения классов сетевых узлов основаны на активном взаимодействии с сетевым узлом [3], что не всегда допустимо в сетях АСУ ТП. Системы, позволяющие определять класс узла в пассивном режиме, могут работать исключительно с заложенным на этапе разработки системы списком классов [4, 5, 6], что не позволяет задавать пользовательские классы и адаптировать системы к работе в заданных сетях в режиме реального времени – например, при обнаружении в сети новых, ранее не описанных, протоколов.

Существующие на данный момент прототипы и модели систем выявления аномалий в сетевом трафике часто основаны на сигнатурном анализе, для корректной работы которого необходима сложная предварительная настройка СЗИ [7, 8, 9], а прототипы и модели, основанные на отслеживании статистических характеристик, не всегда могут объяснить причину признания поведения узла аномальным [4].

Для реализации проекта предлагается использовать следующие методы исследования: теория вероятностей, математическая статистика, теория матриц, методы машинного обучения, эволюционно-генетический аппарат, теория алгоритмов.

Общий план проводимых исследований представлен в таблице (Табл. 1).

Табл. 1. План проводимых исследований

№ п/п	Наименование этапа	Основные результаты
1	Систематизация и анализ современного состояния теории и практики, технологий, методов и средств восстановления структуры сетевого трафика, определения классификационных характеристик сетевых узлов и выявления аномальной активности сетевых узлов	Глава диссертации
2	Разработка алгоритма восстановления структуры сетевого трафика, обеспечивающего восстановление структуры пакетов сетевого трафика, содержащего поля переменной длины	Статья ВАК/Scopus Алгоритм
3	Разработка алгоритма определения классификационных характеристик сетевых узлов по генерируемому ими сетевому трафику без воздействия на них	Статья ВАК/Scopus Алгоритм
4	Разработка алгоритма выявления аномалий в активности сетевых узлов	Статья ВАК/Scopus Алгоритм
5	Разработка прототипа программного обеспечения, реализующего разработанные алгоритмы	Свидетельство о регистрации ПО Акт о внедрении
6	Подготовка диссертации на тему «Комплекс алгоритмов выявления аномалий в компьютерных сетях, использующий методы машинного обучения и отличающийся отсутствием воздействия на сетевую инфраструктуру»	Автореферат Диссертация на соискание ученой степени кандидата наук

В рамках исследования впервые будут предложены алгоритмы в виде комплексного решения, впервые использующего:

— оценку близости форматов сообщений для разделения многопротокольного трафика на кластеры;

— статистические характеристики трафика для определения границ полей заголовков сетевых пакетов;

— методы формирования характеристических векторов узлов из сетевого трафика для определения класса узла;

— контроль изменения во времени и многомерном пространстве профиля сетевого трафика узла для выявления аномальной активности;

— иерархическую кластеризацию векторных представлений сетевых узлов для интерпретации принятых решений о наличии аномальной активности.

По окончании проекта планируется получить следующие научные результаты, соответствующие задаче развития основных инфраструктурных элементов цифровой экономики (информационная инфраструктура, информационная безопасность) программы развития цифровой экономики Российской Федерации:

1. Алгоритм восстановления структуры сетевого трафика, впервые использующий статистические характеристики трафика для определения границ полей заголовков сетевых пакетов, обеспечивает анализ сетевого трафика при наличии в нем нескольких протоколов неизвестной структуры.

2. Алгоритм определения классификационных признаков сетевых узлов, отличается использованием методов формирования характеристических векторов из сетевого трафика и обеспечивает автоматизированное определение типа сетевого узла при сохранении целостности исследуемой сети.

3. Алгоритм выявления аномальной сетевой активности сетевого узла впервые использует методы формирования профиля сетевого трафика узла и иерархической кластеризации векторных представлений сетевых узлов и обеспечивает контроль изменения во времени и многомерном пространстве профиля сетевого трафика узла при выявлении аномальной сетевой активности с интерпретацией результатов.

Научные результаты планируется представлять на тематических научно-практических конференциях по информационной безопасности, в частности:

– Всероссийская научно-практическая конференция студентов, аспирантов и молодых ученых «Безопасность информационного пространства»;

– Ural-Siberian Conference on Biomedical Engineering, Radio Electronics and Information Technologies (USBEREIT);

– Международная молодежная научно-техническая конференция «Современные проблемы радиоэлектроники и телекоммуникаций».

Также планируется серия публикаций в рецензируемых изданиях, в частности:

– Вестник УрФО. Безопасность в информационной сфере

– Защита информации. Инсайд

Разработанный комплекс алгоритмов планируется реализовать в программном обеспечении, предназначенном для дополнения существующих систем обнаружения компьютерных атак новым функционалом, востребованным при практической реализации систем обнаружения компьютерных атак в сетях объектов автоматизированных систем управления технологическим процессом.

Программное обеспечение планируется зарегистрировать в Едином реестре российских программ для электронных вычислительных машин и баз данных, а также осуществить его внедрение в ООО «Сайберлимфа». Полученные научные результаты планируется использовать при подготовке патента на изобретение.

СПИСОК ЛИТЕРАТУРЫ

1. Cui Weidong, Jayanthkumar Kannan, Helen J. Wang. Discoverer: Automatic Protocol Reverse Engineering from Network Traces. // USENIX Security Symposium. 2007.
2. Fanghui Sun, Shen Wang, Chunrui Zhang, Hongli Zhang. Unsupervised field segmentation of unknown protocol messages. // Computer Communications, Volume 146, 15 October 2019, pp. 121-130.
3. Chapter 8. Remote OS Detection // Официальный сайт компании «NMAP» [Электронный ресурс] URL: https://nmap.org/book/osdetect.html (дата обращения: 15.09.2023).
4. Kaspersky Machine Learning for Anomaly Detection // Официальный сайт компании «Лаборатория Касперского» [Электронный ресурс] URL: https://mlad.kaspersky.ru/ (дата обращения: 15.09.2023).
5. Responder: a familiar HTTP Service Framework for Python // Репо-зиторий компании «Responder» на веб-сервисе для хостинга IT-проектов «GitHub» [Электронный ресурс] URL: https://github.com/taoufik07/responder (дата обращения: 15.09.2023).
6. Antônio J.Pinheiro, Jeandrode M. Bezerra, Caio A.P.Burgardt, Divanilson R.Campelo “Identifying IoT devices and events based on packet length from encrypted traffic”, Computer Communications, Volume 144, 15 August 2019, Pages 8-17, DOI: 10.1016/j.comcom.2019.05.012.
7. Industrial Strength OT and IoT Security and Visibility. // Официальный сайт компании «NOZOMI networks» [Электронный ресурс] URL: https://www.nozominetworks.com/products/guardian/ (дата обращения: 27.03.2023).
8. Шадрин А.В., Дякин П.В., Кулагин Д.А. Система и способ противодействия аномалиям в технологической системе. Патент №2747461 РФ, МПК G06F 21/53. Заявл. 17.07.2019. Опубл. 05.05.2021.
9. Репин Д.С., Краснов А.Е., Надеждин Е.Н., Никольский Д.Н., Галяев В.С. Способ обнаружения сетевых атак на основе анализа временной структуры трафика. Патент №2680756 РФ, МПК G06F 21/55, H04L 12/70. Заявл. 14.12.2017. Опубл. 26.02.2019.
10. Зуйков А.В., Душа И.Ф., Зулькарнаев Р.Ф. Способ обработки сетевого трафика с использованием межсетевого экранирования. Патент №2697698 РФ, МПК H04L 12/66, H04L 12/70. Заявл. 27.12.2017. Опубл. 16.08.2019.

Стародубов М.И.
Дальневосточный Федеральный Университет, ассистент
Starodubov.mi@dvfu.ru

МЕТОДЫ И ТЕХНОЛОГИИ В ЗАДАЧЕ ОБНАРУЖЕНИЯ ВРЕДОНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Аннотация: В данной работе рассматриваются методы обнаружения вредоносного программного обеспечения: метод сигнатурного обнаружения, метод эвристического анализа и метод обнаружения, основанный на анализе аномалий. Описываются их положительные и отрицательные стороны. Особое внимание уделяется использованию технологий интеллектуального анализа в задаче обнаружения вредоносного программного обеспечения.

Ключевые слова: вредоносное программное обеспечение, межпрограммное взаимодействие, интеллектуальные системы.

Компьютерные технологии стремительно проникли в нашу жизнь. Просмотр любимого фильма, поход в магазин, проезд на автобусе, поход в банк, взаимодействие с государством, всё это сферы, которые стали проще, удобнее и быстрее благодаря компьютерным технологиям. С каждым днём компьютерные технологии обрабатывают всё больше и больше личной информации, обрабатывают больше платёжных транзакций, обрабатывают не только пользовательские и коммерческие данные, но и государственную информацию. В связи с этим, компьютерная техника представляет особый интерес для злоумышленника.

Одним из наиболее используемых злоумышленниками инструментов является вредоносное программное обеспечение (ВПО, вредоносное ПО). Доля атак с его использованием превышает 55% и постоянно растёт [1]. При этом увеличивается как количество атак, так и их сложность [2]. Злоумышленники становятся более квалифицированными и используют более сложные и изощрённые методы проникновения. По этой причине возрастает и сложность вредоносных программ, а также их количество. Согласно статистике «Лаборатории Касперского» в течение 2022 года атакам подверглось 15% от общего количества устройств, подключённых к интернету [3].

Существует немало определений вредоносного программного обеспечения, согласно наиболее широкому определению, вредоносное программное обеспечение – понятие, обозначающее часть программного кода, программного средства или специальный модуль, сознательно созданные в целях нанесения ущерба компьютерной системе, перехвата информации, проникновения в систему, получения полного или частичного контроля над системой. ГОСТ Р 53113.1-2008 даёт более узкое определение вредоносной программы, как программы, предназначенной для осуществления несанкционированного доступа и (или) воздействия на информацию или ресурсы информационной системы [4]. В дальнейшем, под вредоносным программным обеспечением будем подразумевать любую программную составляющую или самостоятельную программу, предназначенную для исполнения любого несанкционированного действия на пользовательском устройстве.

Целью исследования является разработка алгоритма обнаружения вредоносного программного обеспечения с использованием методов интеллектуального анализа.

В рамках данного исследования ставятся следующие задачи:

– теоретическая оценка эффективности алгоритмов и систем обнаружения вредоносного программного обеспечения;

– разработка алгоритма интеллектуального анализа межпрограммного взаимодействия;

– разработка алгоритма обнаружения вредоносного обеспечения на основе алгоритма интеллектуального анализа межпрограммного взаимодействия;

– оценка эффективности и возможностей разработанного алгоритма.

Связь исследования с диссертационной работой прослеживается в задаче 3 диссертационного исследования (Разработка алгоритма обнаружения вредоносного обеспечения на основе алгоритма интеллектуального анализа межпрограммного взаимодействия).

Задача обнаружения вредоносного программного обеспечения известна с 1970-х годов и нашла не мало вариантов её решения. На данный момент обнаружение вредоносного ПО заключается главным образом в обнаружении характерного вредоносного кода. Среди классических методов обнаружения вредоносных объектов можно выделить сигнатурный анализ, эвристический анализ и метод обнаружения на основе аномалий.

Сигнатурный анализ в своей основе используется обнаружение сигнатур (определённых последовательностей), хранимых в базе данных анализатора, для идентификации вредоносного ПО и его типа. База данных содержит широкий спектр сигнатур уже известных вредоносных объектов. В случае совпадения сигнатуры объекта с любой сигнатурой из базы данных анализатор определяет объект как вредоносный. В качестве сигнатур для исполняемых файлов могут выступать строки, последовательности байт, последовательности опкодов и другие извлекаемые из файла объекты. Данный метод обнаружения может быть построен на трёх техниках анализа: статической, динамической или смешанной [5].

Сигнатурный анализ имеет ряд положительных черт: широкая применимость, простота работы, быстрая скорость работы и поиск исчерпывающей информации о вредоносном ПО. Несмотря на это, метод не лишён недостатков: неспособность обнаруживать полиморфное ВПО, зависимость размера базы сигнатур от числа обнаруживаемых объектов, необходимость постоянного обновления баз и невозможность обнаружения ранее не неизвестных вредоносных объектов [5 – 7].

Другим известным методом обнаружения является эвристический анализ – метод обнаружения и различению нормального и ненормального поведения системы для выявления уже известных и ранее неизвестных вредоносных атаках и поиска подходящего решения. Основанные на весах правила или системы используются для определения вреда, который вредоносный объект может нанести. Если вес этих правил превышает заданный предел, предпринимаются превентивные действия, например помещение файла в карантин [5].

Метод эвристического анализа является более сложным, по сравнению с методом сигнатурного анализа и получил ещё ряд дополнительных положительных черт, главные из которых возможность обнаружения полиморфного вредоносного ПО и возможность обнаруживать новое ВПО, похожее на уже известные вредоносные объекты. Однако, вредоносные объекты, ранее никем не обнаруженные и не похожие на другие вредоносные объекты, остались без внимания [8].

Совершенно другим подходом, является метод обнаружения, основанный на аномалиях, который заключается в проверке вредоносности программы путем обнаружения разницы между поведением аномальной программы и поведением нормальной программы.

Как правило, траектория поведения вредоносного ПО отличается от траектории поведения обычного программного обеспечения. После полного понимания поведения обычной программы будет сформирован набор стандартов и спецификаций. Если траектория поведения обнаруживаемой программы является ненормальной и нарушает этот набор спецификаций, она может быть определена как вредоносная. Существует три различных метода обнаружения на основе аномалий: статическое обнаружение, динамическое обнаружение и гибридное обнаружение [9].

На абстрактном уровне аномалия определяется как паттерн, которые не соответствует ожидаемому нормальному поведению. Таким образом, простой подход в обнаружении аномалий заключается в определении области, представляющей нормальное поведение, и объявления аномалией любого наблюдения, не соответствующего области нормального поведения. Этот подход кажется достаточно простым, однако, существует несколько факторов, значительно его усложняющих [9]:

1. Определить нормальную область, которая охватывает все возможные варианты нормального поведения, очень сложно. Кроме того, граница между нормальным и аномальным поведением часто не является точной. Таким образом, аномальное наблюдение, лежащее близко к границе, на самом деле может быть нормальным, и наоборот.

2. В случае, когда аномалии являются результатом вредоносных действий, злоумышленники часто приспосабливаются, чтобы аномальные наблюдения выглядели нормальными, тем самым усложняя задачу определения нормального поведения.

3. Во многих областях нормальное поведение объекта постоянно изменяется и развивается. В связи с этим, нынешнее представление о нормальном поведении может оказаться недостаточно репрезентативным в будущем.

4. Доступность помеченных данных для обучения/валидации моделей, используемых методами обнаружения аномалий, обычно является серьезной проблемой.

5. Часто данные содержат шум, который, как правило, похож на фактические аномалии и, следовательно, его трудно различить и удалить.

Из-за этих проблем задачу обнаружения аномалий в ее самом общем виде решить непросто. На самом деле, большинство существующих методов обнаружения аномалий решают конкретную постановку проблемы. Формулировка определяется различными факторами, такими как характер данных, доступность помеченных данных, тип аномалий, которые необходимо обнаружить, и так далее. Часто эти факторы определяются областью применения, в которой необходимо обнаружить аномалии. Исследователи взяли на вооружение концепции из различных дисциплин, таких как статистика, машинное обучение, интеллектуальный анализ данных, теория информации, спектральная теория, и применили их к конкретным постановкам задач.

Одним из способов борьбы с вредоносным программным обеспечением является применение технологий интеллектуального анализа. Существует множество методов и алгоритмов интеллектуального анализа, которые используются для обнаружения вредоносного программного обеспечения. Рассмотрим основные из них более подробно:

1. Методы анализа поведения – основаны на изучении поведения программы во время работы. Используются для обнаружения неизвестных вредоносных программ и распознавания новых видов вредоносной активности. Для этого анализируются все действия, выполняемые программой, и сравниваются с известными алгоритмами вредоносных программ.

2. Методы статического анализа – основаны на анализе исходного кода программы. Для обнаружения вредоносных программ используются алгоритмы статического анализа, которые выявляют уязвимости, которые могут быть использованы злоумышленниками для внедрения вредоносного ПО.

3. Очень близким к методу анализа поведения является метод динамического анализа – метод, основанный на анализе программы во время выполнения в контролируемой среде. Он позволяет выявлять новые виды вредоносных программ и обходить защиту от статического анализа. Данный метод отличается от метода анализа поведения средой исполнения: при динамическом анализе поведение образца изучается в контролируемой изолированной среде, в то время при методе анализа поведения образец изучается в реальных условиях на реальных системах.

4. Методы машинного обучения – методы, основанные на обучении алгоритмов распознавания вредоносных программ. Для этого используются нейронные сети, алгоритмы классификации и другие методы машинного обучения. Алгоритмы обучаются на множестве известных вредоносных объектов и затем применяются для распознавания новых видов ВПО.

Все представленные выше методы не являются взаимоисключающими и могут использоваться совместно. В таком случае часто говорят о применение «Гибридного метода обнаружения» – метода, включающего в себя несколько других методов обнаружения.

Помимо классических методов машинного обучения, таких как алгоритмы кластеризации и классификации, в анализе вредоносного программного обеспечения также активно применяются нейронные сети различных архитектур и методы глубокого обучения. В задаче обнаружения ВПО уже применяются следующие архитектуры нейронных сетей: MLP, CNN, RNN, GAN и GNN. При этом наименее изученными, в рамках решения задачи обнаружения вредоносного ПО, являются GNN, что обусловливается тем, что они появились не так давно [10], но несмотря на это с точки зрения анализа межпрограммного взаимодействия являются наиболее перспективными.

Как видно из приведённых выше исследований, методы интеллектуального анализа являются важным инструментом при обнаружении вредоносного программного обеспечения (ВПО). Использование методов интеллектуального анализа:

1. Повышает точность обнаружения. Методы интеллектуального анализа позволяют выявлять скрытые связи и закономерности в данных, что может помочь повысить точность обнаружения ВПО.

2. Ускоряет процесс обнаружения. Методы интеллектуального анализа могут автоматизировать процесс обнаружения ВПО, что позволяет ускорить процесс и снизить количество ложных срабатываний.

3. Помогает в анализе больших объемов данных. Обнаружение ВПО требует анализа больших объемов данных, включая файлы, сетевой трафик и действия пользователей. Методы интеллектуального анализа позволяют автоматически анализировать такие данные и выявлять угрозы.

4. Позволяет обнаруживать новые угрозы. ВПО постоянно эволюционирует и появляются новые виды угроз. Методы интеллектуального анализа могут помочь выявить новые угрозы, которые не были обнаружены ранее.

Несмотря на то, что методы обнаружения, представленные выше, играют очень важную роль, разработчики вредоносного кода часто используют различные средства для их обхода. Также они создают некоторые новые типы вредоносного кода или варианты вредоносного

кода, в связи с чем точность любой системы обнаружения в этих случаях будет значительно снижена. В связи с этим, необходимо постоянно развивать уже существующие методы обнаружения вредоносного ПО и создавать новые.

В рамках планируемого исследования предлагается использовать графовые нейронные сети для анализа межпрограммного взаимодействия программного обеспечения, с применением положений теории графов.

Межпрограммным взаимодействием называют механизм, предоставляемый операционной системой, который позволяет процессам (программам) взаимодействовать друг с другом. Это взаимодействие может включать в себя процесс, сообщающий другому процессу о том, что произошло какое-то событие, или передачу данных от одного процесса к другому.

Межпрограммное взаимодействие включает в себя различные методы, реализованные по-разному в различных операционных системах: файл, сигнал, сокет, канал, именованный канал, неименованный канал, семафор, разделяемая память, обмен сообщениями (без разделения), проецируемый в память файл, очередь сообщений, почтовый ящик.

Анализируя межпрограммное взаимодействие конкретного программного объекта, можно составить его «слепок», по которому его, и его другие версии, можно однозначно идентифицировать в компьютерной системе.

СПИСОК ЛИТЕРАТУРЫ

1. Актуальные киберугрозы: IV квартал 2022 года [Электронный ресурс]. — Режим доступа : https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2022-q4/
2. Кибербезопасность в 2022–2023. Тренды и прогнозы [Электронный ресурс]. — Режим доступа : https://www.ptsecurity.com/ru-ru/research/analytics/ogo-kakaya-ib/
3. Kaspersky Security Bulletin 2022. Статистика [Электронный ресурс]. — Режим доступа : https://securelist.ru/ksb-2022-statistics/106227/
4. ГОСТ Р 53113.1-2008. Национальный стандарт Российской Федерации. Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения" [Электронный ресурс]. — Режим доступа : https://data.1000gost.ru/catalog/Data/484/48435.pdf .
5. Tahir R. A study on malware and malware detection techniques / Tahir R. //International Journal of Education and Management Engineering. – 2018. – Т. 8. – №. 2. – С. 20.
6. Souri A. A state-of-the-art survey of malware detection approaches using data mining techniques / Souri A., Hosseini R //Human-centric Computing and Information Sciences. – 2018. – Т. 8. – №. 1. – С. 1-22.
7. Moser A. Limits of static analysis for malware detection / Moser A., Kruegel C., Kirda E. //Twenty-third annual computer security applications conference (ACSAC 2007). – IEEE, 2007. – С. 421-430.
8. Zahra Bazrafshan A survey on heuristic malware detection techniques / Zahra Bazrafshan, Hashem Hashemi, Seyed Mehdi Hazrati Fard, Ali Hamzeh //The 5th Conference on Information and Knowledge Technology. – IEEE, 2013. – С. 113-120.
9. Chandola V. Anomaly detection: A survey / Chandola V., Banerjee A., Kumar V //ACM computing surveys (CSUR). – 2009. – Т. 41. – №. 3. – С. 1-58.
10. F. Scarselli The graph neural network model / F. Scarselli, M. Gori, A. C. Tsoi, M. Hagenbuchner, G. Monfardini // IEEE transactions on neural networks. – 2008. – Т. 20. – №. 1. – С. 61-80.

МТУСИ

ФУМО ВО ИБ