ВОПРОСЫ КИБЕРБЕЗОПАСНОСТИ

№4 2024 (62)

DOI: 10.21681/2311-3456

Безопасный искусственный интеллект

Прогнозирование размера исходного кода бинарной программы

Цифровые двойники для обеспечение информационной безопасности

ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ ДЛЯ ГЛОБАЛЬНОГО МИРА

致力于全球和平的信息通信技术

ICTs FOR GLOBAL PEACE

ВОПРОСЫ КИБЕРБЕЗОПАСНОСТИ

НАУЧНЫЙ РЕЦЕНЗИРУЕМЫЙ ЖУРНАЛ

№4 (62) 2024 г.

Выходит 6 раз в год

Журнал выходит с 2013 г. (Свидетельство о регистрации ПИ № ФС77-75239). Перерегистрировано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций 07.03.2019.

Журнал входит в рейтинг научных изданий ВАК в категории К1, индексируется в RSCI, публикует статьи по специальностям 1.2.4 и 2.3.6 – физ-мат. науки; 2.2.15, 2.3.1, 2.3.5, 2.3.6 – техн.науки

Учредитель и издатель

АО «Научно-производственное объединение «Эшелон»

Над номером работали:

Г. И. Макаренко – *шеф-редактор*, И. Ю. Шахалов – *отв. секретарь*, С. С. Игнатов – *верстка*, Н. С. Рождественская – *маркетинг и подписка*

Подписано к печати 19.07.2024 г.
Общий тираж 120 экз. Цена свободная

Адрес: 107023, Москва, ул. Электрозаводская, д. 24, стр. 1.
E-mail: editor@cyberrus.info, тел.: +7 (985) 939-75-01.
Требования, предъявляемые к рукописям, размещены на сайте: **https://cyberrus.info/**

СОДЕРЖАНИЕ

БЕЗОПАСНЫЙ ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ

ПЕРСПЕКТИВНЫЕ НАПРАВЛЕНИЯ ПРИМЕНЕНИЯ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ПРИ ЗАЩИТЕ ИНФОРМАЦИИ
Мещеряков Р. В., Мельников С. Ю., Пересыпкин В. А., Хорев А. А. 2

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ИНФОРМАТИКИ

ПРОГНОЗИРОВАНИЕ РАЗМЕРА ИСХОДНОГО КОДА БИНАРНОЙ ПРОГРАММЫ В ИНТЕРЕСАХ ЕЕ ИНТЕЛЛЕКТУАЛЬНОГО РЕВЕРС-ИНЖИНИРИНГА
Израилов К. Е. 13

ПРИМЕНЕНИЕ ЛОГИКО-ВЕРОЯТНОСТНОГО МЕТОДА В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. Часть 5
Калашников А. О., Аникина Е. В., Бугайский К. А., Бирин Д. С., Дерябин Б. О., Цепенда С. О., Табаков К. В. 26

ТЕСТИРОВАНИЕ И МОНИТОРИНГ КИБЕРБЕЗОПАСНОСТИ

ОБЕСПЕЧЕНИЕ СОВМЕСТИМОСТИ ТЕХНИЧЕСКИХ КОМПОНЕНТОВ ПРИ СОЗДАНИИ СИСТЕМЫ МОНИТОРИНГА ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
Девицына С. Н., Пилькевич П. В. 38

МЕТОДЫ И СРЕДСТВА КОДИРОВАНИЯ

АНАЛИЗ ТРЕБОВАНИЙ ПРИМЕНЕНИЯ И ТЕХНОЛОГИЧЕСКИХ ВОЗМОЖНОСТЕЙ РАДИОСИГНАЛОВ, ПЕРСПЕКТИВНЫХ ДЛЯ СЕТЕЙ 6G
Барабошин А. Ю., Лучин Д. В., Маслов Е. Н. 45

КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ

АНАЛИЗ СУЩЕСТВУЮЩИХ ПОДХОДОВ К СИНТЕЗУ ПСЕВДО-ДИНАМИЧЕСКИХ SBOX
Прудников В. А. 57

ВЫЧИСЛЕНИЯ НАД ПОЛИНОМАМИ В ПОСТКВАНТОВЫХ СХЕМАХ ПОДПИСИ
Иваненко В. Г., Иванова И. Д., Иванова Н. Д. 65

ПРИЛОЖЕНИЕ МЕТОДОВ КОДИРОВАНИЯ И КРИПТОГРАФИИ

СПОСОБ УСИЛЕНИЯ РАНДОМИЗАЦИИ ПОДПИСИ В АЛГОРИТМАХ ЭЦП НА НЕКОММУТАТИВНЫХ АЛГЕБРАХ
Молдовян Д. Н., Костина А. А. 71

БЕЗОПАСНОСТЬ МЕТА-СЕТИ ИНТЕРНЕТ

СТРУКТУРНО-ФУНКЦИОНАЛЬНЫЙ АНАЛИЗ КОНФЛИКТНОЙ СИТУАЦИИ МЕЖДУ ГОСУДАРСТВЕННОЙ СИСТЕМОЙ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ИНОСТРАННОЙ СИСТЕМОЙ ДЕСТРУКТИВНЫХ ВОЗДЕЙСТВИЙ
Стародубцев Ю. И., Закалкин П. В. 82

УПРАВЛЕНИЕ РИСКАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ПРИМЕНЕНИЕ ТЕХНОЛОГИЙ МАШИННОГО ОБУЧЕНИЯ ДЛЯ ОБНАРУЖЕНИЯ ВЕБ-АТАК
Лапина М. А., Мовзалевская В. В., Токмакова М. Е., Бабенко М. Г., Саджид М. 92

БЕЗОПАСНОСТЬ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

АЛГОРИТМ ИМИТАЦИИ ДИНАМИЧЕСКИХ ХАРАКТЕРИСТИК ТРАФИКА ВЕБ-СЕРВИСА
Горбачёв А. А., Лысенко Д. Э. 104

МЕТОДЫ МАТЕМАТИЧЕСКОГО МОДЕЛИРОВАНИЯ

РАЗРАБОТКА ПРОГРАММНО-АППАРАТНОГО КОМПЛЕКСА МОДЕЛИРОВАНИЯ МНОГОЗНАЧНЫХ КОМПЬЮТЕРНЫХ АТАК
Шелухин О. И., Раковский Д. И. 116

АЛГОРИТМ ОЦЕНКИ УРОВНЯ ЦИФРОВОЙ АВТОНОМИИ КОМПОНЕНТОВ ИНФРАСТРУКТУРЫ ЦИФРОВОГО ПРОСТРАНСТВА
Рыженко А. А., Селезнёв В. М. 131

БЕЗОПАСНОСТЬ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

ИСПОЛЬЗОВАНИЕ ЦИФРОВЫХ ДВОЙНИКОВ С ЦЕЛЬЮ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КИБЕРФИЗИЧЕСКИХ СИСТЕМ
Водопьянов А. С. 140

РЕЦЕНЗИИ

ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ ДЛЯ ГЛОБАЛЬНОГО МИРА
Стрельцов А. А. 145

Подписка на журнал осуществляется в почтовых отделениях по каталогу «Пресса России». Подписной индекс 40707

ПЕРСПЕКТИВНЫЕ НАПРАВЛЕНИЯ ПРИМЕНЕНИЯ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ПРИ ЗАЩИТЕ ИНФОРМАЦИИ

Мещеряков Р. В.[1], Мельников С. Ю.[2], Пересыпкин В. А.[3], Хорев А. А.[4]

DOI: 10.21681/2311-3456-2024-4-02-12

Цель работы: *выявление актуальных направлений реализации угроз информационной безопасности различных систем с использованием технологий искусственного интеллекта и основных задач по защите информации, в которых применяются технологии искусственного интеллекта.*

Метод исследования: *системный анализ открытых источников о состоянии развития современных технологий искусственного интеллекта, которые создают новые угрозы безопасности информации, и возможности применения технологий искусственного интеллекта для повышения эффективности системы защиты информации.*

Полученный результат: *приведены результаты анализа основных задач защиты информации в различных направлениях информационной безопасности, в том числе использование искусственного интеллекта в компьютерных системах и сетях: обнаружение компьютерных атак; обнаружение вредоносных программ; обнаружение модификации и подмены данных и сообщений; обнаружение и предотвращение утечек конфиденциальных данных в корпоративных сетях; оценка рисков информационной безопасности; повышение надежности и киберустойчивости компьютерных систем и сетей, в вычислительных и технических системах.*

Научная новизна: *систематизированы методы защиты информации с точки зрения применения технологий и систем искусственного интеллекта применительно к задаче защиты информации. Классифицированы угрозы, реализуемые с использованием технологий искусственного интеллекта: «подделка» биометрических идентификационных признаков с целью получения доступа на объект или в систему путем формирования идентификационных признаков, принадлежащих доверенному субъекту; формирование ложных речевых сообщений, имитирующих речь конкретного человека; создание ложных фото и видео с участием конкретных лиц; «подделка» текстов, имитирующих стиль определенных авторов и других.*

Вклад авторов: *Мещеряков Р. В. исследовал направление по телекоммуникационным системам, Мельников С. Ю. исследовал направление по текстовым и речевым системам, Пересыпкин В. А. исследовал направление по системам аутентификации и рискориентированному подходу, Хорев А. А. исследовал направление по технической защите информации.*

Ключевые слова: *информационная безопасность, защита информации, технологии искусственного интеллекта, угрозы безопасности информации, кибербезопасность.*

PROMISING DIRECTIONS FOR APPLYING ARTIFICIAL INTELLIGENCE TECHNOLOGIES IN INFORMATION PROTECTION

Meshcheryakov R. V.[5], Melnikov S. Yu.[6], Peresypkin V. A.[7], Horev A. A.[8]

1 Мещеряков Роман Валерьевич, доктор технических наук, профессор, главный научный сотрудник ИПУ РАН, Москва, Россия. ORCID: 0000-0002-1129-8434. E-mail: mrv@ieee.org

2 Мельников Сергей Юрьевич, доктор физико-математических наук, кафедра теории вероятностей и кибербезопасности института компьютерных наук и телекоммуникаций факультета физико-математических и естественных наук Российского университета дружбы народов имени Патриса Лумумбы, Москва, Россия. ORCID :0000-0002-9023-9896. E-mail: melnikov-syu@rudn.ru

3 Пересыпкин Владимир Анатольевич, доктор технических наук, действительный член Академии криптографии Российской Федерации, научный сотрудник Академии криптографии Российской Федерации, Москва, Россия. E-mail: info@cryptoacademy.gov.ru

4 Хорев Анатолий Анатольевич, доктор технических наук, профессор заведующий кафедрой информационной безопасности, МИЭТ, Москва, Россия. ORCID: 0000-0001-9074-385X. E-mail: horev@miee.ru

5 Roman V. Meshcheryakov, Dr.Sc. (of Tech.), Professor, Chief Researcher, ICS RAS, Moscow, Russia. ORCID: 0000-0002-1129-8434. E-mail: mrv@ieee.org

6 Sergey I. Melnikov, Dr.Sc. (in Physics and Math.), Department of Probability Theory and Cybersecurity, Institute of Computer Science and Telecommunications, Faculty of Physics, Mathematics and Natural Sciences, Patrice Lumumba Peoples' Friendship University of Russia, Moscow, Russia. ORCID :0000-0002-9023-9896. E-mail: melnikov-syu@rudn.ru

7 Vladimir A. Peresypkin, Dr. Sc. (of Tech.), Academician of the Academy of Cryptography of the Russian Federation, Researche, ACoRF Moscow, Russia. E-mail: info@cryptoacademy.gov.ru

8 Khorev Anatoly Anatolyevich, Dr.Sc.(of Tech.), Professor, Head of the Department of Information Security, MIET, Moscow, Russia. ORCID: 0000-0001-9074-385X. E mail: horev@miee.ru

Purpose of the work: *identifying current areas of threats implementation to information security of various systems using artificial intelligence technologies and the main tasks of information protection, in which artificial intelligence technologies are used.*

Research method: *system analysis of open sources and publication on the state of development of modern artificial intelligence technologies that create new threats to information security and privacy, and the possibility of using artificial intelligence technologies to improve the efficiency of the information security system.*

Result: *the results of the analysis of the main tasks of information protection in various areas of information security are presented, including the use of artificial intelligence in computer systems and networks: detection of computer attacks; detection of malware; detection of modification and substitution of data and messages; detection and prevention of leaks of confidential data in corporate networks; assessment of information security risks; increasing the reliability and cyber stability of computer systems and networks, in computing and technical systems.*

Scientific novelty: *the methods of information protection are systematized from the point of view of the application of artificial intelligence technologies and systems in relation to the task of information protection. The threats implemented using artificial intelligence technologies are classified: «forgery» of biometric identification features in order to gain access to an object or system by forming identification features belonging to a trusted subject; formation of false speech messages imitating the speech of a specific person; creation of false photos and videos involving specific persons; «forgery» of texts imitating the style of certain authors and others.*

Keywords: *information security, information protection, artificial intelligence technologies, threats to information security, cybersecurity.*

Введение

Развитие современных информационных технологий, с одной стороны, создает новые угрозы безопасности информации, а с другой – позволяет повысить эффективность мер защиты информации [1–3]. Технологии искусственного интеллекта являются одной из наиболее динамично развивающихся современных технологий обработки информации.

В соответствии с Национальной стратегией развития искусственного интеллекта[9] под искусственным интеллектом (ИИ) понимается комплекс технологических решений, позволяющий имитировать когнитивные функции человека (включая поиск решений без заранее заданного алгоритма) и получать при выполнении конкретных задач результаты, сопоставимые с результатами интеллектуальной деятельности человека или превосходящие их. Технологии искусственного интеллекта (ТИИ) включают в себя компьютерное зрение, обработку естественного языка, распознавание и синтез речи, интеллектуальную поддержку принятия решений и др.

Отметим важные изменения, внесенные в Национальную стратегию развития ИИ в 2024 году[10]. Стратегия определяет доверенные технологии ИИ как технологии, отвечающие стандартам безопасности <...>, исключающие при их использовании возможность нанесения ущерба интересам общества и государства. Обязательное внедрение доверенных технологий ИИ в тех областях его использования, в которых может быть нанесен ущерб безопасности Российской Федерации, отнесено к основным задачам развития ИИ в нашей стране. Безопасность является одним из основных принципов развития и использования ТИИ. Отмечается недопустимость использования ИИ в целях умышленного причинения вреда гражданам и организациям. Отдельно к принципам развития и использования ИИ отнесено использование ИИ в целях обеспечения информационной безопасности.

Одно из наиболее распространенных направлений использования искусственного интеллекта – это машинное обучение, которое основано на получении знаний интеллектуальной системой в процессе ее работы. Перечислим основные, широко используемые алгоритмы машинного обучения: логистическая регрессия, линейная регрессия, решающие деревья, случайный лес, градиентный бустинг, методы ближайших соседей, k-средних, опорных векторов, разновидности байесовских классификаторов, искусственные нейронные сети.

К характеристикам оценки решений с использованием технологий искусственного интеллекта относят не только ошибки первого (False Rejection Rate, «ложная тревога») и второго (False Acceptance Rate, «пропуск цели») рода. Следует использовать и обобщенные оценки, например, как в работе [4], для оценки эффективности коррекции искаженных слов в распознанных речевых сигналах используется точность и полнота (F1 мера). F1 мера – гармоническое среднее точности A и полноты R коррекций искажённого текста с одинаковым весом.

Основные задачи, которые могут решаться с использованием алгоритмов искусственного

9 Национальная стратегия развития искусственного интеллекта на период до 2030 года, утверждена Указом Президента Российской Федерации от 10 октября 2019 г. № 490.

10 Указ Президента Российской Федерации от 15.02.2024 № 124 «О внесении изменений в Указ Президента Российской Федерации от 10 октября 2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации" и в Национальную стратегию, утвержденную этим Указом».

интеллекта: классификация, кластеризация, регрессия, обнаружение аномалий, распознавание образов, поиск ассоциативных правил, прогнозирование, моделирование рассуждений, обработка естественного языка, инженерия знаний, создание экспертных систем и пр.

Множество алгоритмов искусственного интеллекта применяется как для реализации атак, так и для обеспечения защиты. Вместе с тем необходимо учитывать, что системы искусственного интеллекта могут содержать уязвимости и быть подвержены атакам различного класса, в том числе и специализированным. Одним из наиболее известных подходов к построению ландшафта угроз и поверхности атаки является база знаний MITRE ATT&CK[11].

Целью данной работы является выявление актуальных направлений реализации угроз информационной безопасности различных систем с использованием технологий искусственного интеллекта и основных задач по защите информации, в которых применяются технологии искусственного интеллекта. Указанная цель разбивается на две составные части: первая – обеспечение защиты от атак, которые реализуются с использованием технологий искусственного интеллекта, вторая – использование технологий искусственного интеллекта для защиты от угроз информационной безопасности.

1.Анализ возможных угроз безопасности информации, создаваемых с использованием технологий искусственного интеллекта

Исторически первые методы ИИ применялись в задачах идентификации, связанных с обработкой речи, текста и изображений. В настоящее время идентификация по биометрическим признакам уже широко используется в системах управления доступа на объектах информатизации, в автоматизированных и информационных системах различного назначения. Сегодня биометрические системы используются в большинстве смартфонов.

Особенностью использования ТИИ является возможность сбора и обработки огромного объема биометрических идентификационных признаков, таких как: изображения лица, формы кисти, отпечатков пальцев, особенностей голоса, клавиатурного почерка или почерка на графическом планшете и т.д. [5–10].

К возможным угрозам, реализуемым с использованием ТИИ по обработке биометрических идентификационных признаков, можно отнести следующие:

- «подделка» биометрических идентификационных признаков с целью получения прав доступа на объект или в систему путем формирования идентификационных признаков другого лица, как, например, это сделано с отпечатками пальцев[12] или речевыми сообщениями [11–13];
- формирование ложных речевых сообщений, имитирующих речь конкретного человека [8];
- создание ложных фото и видео с участием конкретных лиц [11];
- «подделка» текстов, имитирующих стиль определенных авторов [9] и т.д.

Указанные угрозы биометрических систем с использованием подходов на базе ИИ потенциально нарушают не только конфиденциальность и доступность информации, но и ее целостность, т.к. в ходе реализации угрозы может производиться подмена информации. Известны случаи подделки не только внешних, наглядно различимых идентификационных признаков, но и тех признаков, которые являются «внутренними» и связаны с личностными, социальными и иными поведенческими реакциями. Это существенно усложняет противодействие такого рода атакам.

Следовательно, возникают задачи противодействия новым угрозам безопасности информации, которые возникают в результате использования технологий искусственного интеллекта. В частности, следует отметить:

- выявление, локализация источника угроз, который использует технологии искусственного интеллекта;
- классификация вида угроз для конкретного объекта и технологии защиты, против которого направлена угроза и формируется новое признаковое пространство угрозы (включая вектор атаки);
- моделирование действий конкретного типа злоумышленника, под действия которого моделируется проведение атаки, реализующая конкретную угрозу и происходит мимикрия под конкретный источник угроз;
- переход от статического к динамическому обнаружению угроз (например, как используется биометрическая технология liveness), однако и это направление в настоящее время отрабатывается злоумышленниками на высоком уровне;
- информационное противоборство с учетом ретроспективных и прогнозных моделей для формирования целевой линии поведения системы защиты для выявления аномалий, генерируемых системами с искусственным интеллектом, обученными на моделях подыгрывающей стороны;
- возможности реализации новых угроз с использованием генеративных моделей ИИ при формировании открытого признакового пространства

11 MITRE ATT&CK https://attack.mitre.org/

12 Универсальные отпечатки» для взлома смартфонов https://sysblok.ru/futurology/universalnye-otpechatki-dlja-vzloma-smartfonov/

сигнальных последовательностей на входе в информационную систему и систему защиты информации;
- угроза генерации «отложенного» внутреннего нарушителя, который запускается при возникновении определенных событий.

Таким образом, отмеченные задачи требуют проработки не только на уровне построения моделей нарушителей и моделей угроз, но и с учетом динамики развития потенциально возможных злоумышленных действий, которые необходимо учитывать при формировании обучающих выборок сценариев деятельности системы защиты информации.

2. Анализ возможных направлений использования технологий искусственного интеллекта при решении задач защиты информации

Наиболее распространенной областью применения технологий искусственного интеллекта в целях защиты информации являются автоматизированные, информационные, киберфизические и телекоммуникационные системы, включая компьютерные сети различной архитектуры (далее компьютерные системы и сети).

К основным задачам защиты информации в компьютерных системах и сетях с использованием искусственного интеллекта можно отнести:

- обнаружение компьютерных атак;
- обнаружение вредоносных программ;
- обнаружение модификации и подмены данных и сообщений;
- обнаружение и предотвращение утечек конфиденциальных данных в корпоративных сетях;
- оценка рисков информационной безопасности;
- повышение надежности и киберустойчивости компьютерных систем и сетей.

Недостатки традиционных систем информационной безопасности во многом связаны с тем, что они основаны на правилах. Используются заранее определенные методы выявления угроз и реагирования на них. Это влечет за собой ограничения, в частности неспособность реагировать на новые угрозы. С появлением новых угроз правила обновляют вручную. Другим таким ограничением является объем данных. Существующие системы безопасности могут генерировать огромные объемы данных, которые сложно анализировать в реальном времени. Кроме того, системы, основанные на правилах, могут оказаться неэффективными при обнаружении более сложных атак, например использующих ИИ для имитации обычного поведения пользователя.

Преимущества технологий искусственного интеллекта

Возможность быстрой обработки больших массивов данных для «раннего предупреждения». Это одно из ключевых преимуществ ИИ. С помощью ИИ можно в режиме реального времени анализировать огромные объемы информации, прежде всего сетевого трафика.

Обнаружение аномалий и необычной активности. ИИ может анализировать данные из нескольких источников, включая сетевой трафик, системные журналы и данные о поведении пользователей, чтобы выявлять активности, выходящие за рамки нормы. Например, ИИ может обнаружить необычные модели поведения, которые могут указывать на кибератаку, например, передачу больших объемов данных во внешнюю систему или необычные попытки входа в систему. ИИ может провести анализ поведения пользователей, чтобы выявлять аномалии, которые могут указывать на внутреннюю угрозу, например, когда сотрудник получает доступ к данным в нерабочее время или получает доступ к данным, на доступ к которым у него обычно нет разрешения.

Автоматизация реагирования на угрозы. Еще одним преимуществом ИИ в информационной безопасности является его способность автоматизировать реагирование на угрозы. Например, если система искусственного интеллекта обнаруживает попытку кибератаки, она может автоматически заблокировать доступ к скомпрометированной системе, предотвращая дальнейший ущерб. Он также может отправлять оповещения сотрудникам службы безопасности, предоставляя им информацию об инциденте.

Новым, пока еще не сильно развитым направлением является использование методов ИИ для анализа систем шифрования и оценки качества генераторов псевдослучайных чисел (ГПСЧ). Существующие подходы с использованием нейросетей для анализа блочных шифров очень ограничены и представляют научный интерес для слабых шифров, у которых минимизированы число раундов и ослаблены другие важные криптографические параметры. Больший интерес представляет атака на ГСПЧ, которая может определять отклонения от случайности и прогнозировать следующие элементы выходной последовательности ГПСЧ, если известны несколько предшествующих. Так, подход с использованием глубоких нейросетей предложен в [15] для анализа модифицированного линейного конгруэнтного генератора.

Отметим, что в последние годы появляются работы, в которых методы ИИ применяются и для анализа квантовых генераторов случайных чисел ([16, 17] и др.).

При обнаружении компьютерных атак и вредоносных программ отметим направление UEBA (User and Entity Behavior Analytics) – системы поведенческого анализа пользователей и информационных сущностей. Основной сценарий применения ИИ-технологий в продуктах типа UEBA – это выявление аномалий в поведенческих моделях пользователей информационных систем. Выявленные аномалии могут классифицироваться с помощью тех или иных методов ИИ.

Оценка риска с использованием технологий искусственного интеллекта

Следует отразить особенность – это вероятностное описание объекта защиты, применительно к которому проводится оценка риска. Существующий арсенал моделей и подходов к оценке рисков позволяет использовать как вербальные описания, так и формализованные по стандартам менеджмента качества [18–30]. Очевидно, что расчет рисков очень важен для объектов критической информационной инфраструктуры (например, предприятий ТЭК), и беспилотных транспортных средств [31, 32].

С учетом большого количества данных, которые могут быть использованы для обучения, и наличия специализированных вычислителей распространенным решением является использование искусственных нейронных сетей [33–40]. Применению их в системах информационной безопасности посвящен ряд работ [41–44]. Для разных задач, разных обучающих выборок, разных конфигураций доступных вычислителей необходим творческий этап выбора подходящей нейросетевой архитектуры. В качестве обучающей выборки наиболее распространен датасет NSL-KDD Dataset[13].

Задачи информационной безопасности, характерные для новых типов сетей (киберфизические системы, сети интернета вещей и др.) [45–51], имеют свои особенности. Отметим расширяющееся использование биоинспирированных подходов для обеспечения безопасности сетей. В частности, идея иммунных подходов к безопасности сетей состоит в постоянном внутреннем мониторинге работы сети, идентификации зараженного сетевого узла и блокировке этого узла. Указанный подход использовался на заре развития интернета, но в то время не было надежных средств оценки рисков, что часто приводило к некорректным отключениям пользователей.

Анализ возможных направлений решения задач защиты информации для обеспечения безопасности технологий искусственного интеллекта

Отдельным направлением обеспечения информационной безопасности является обеспечение безопасности самих систем искусственного интеллекта, включая системы машинного обучения.

13 NSL-KDD Dataset https://www.unb.ca/cic/datasets/nsl.html

Национальной стратегией развития искусственного интеллекта к числу новых вызовов для государства отнесено, в том числе, «возникновение в сфере разработки, создания и использования ТИИ новых типов угроз информационной безопасности, нехарактерных для других сфер применения информационных технологий». Речь идет, в том числе, о специфических угрозах: атаки на обучающие данные, искажение разметки, атаки, направленные на установление принадлежности конкретных данных обучающей выборке, атаки, направленные на получение данных из обученной модели, и др.

Следовательно, для защиты систем искусственного интеллекта наряду с типовыми средствами защиты информации должны использоваться и специфические технологии, и средства защиты, к основным из которых можно отнести: повышение надежности обучающих выборок, оценка доверия к принимаемым решениям, интерпретируемость результатов, контроль процессов обучения и верификации, повторяемость, отсутствие галлюцинаций и другие.

Наиболее распространенные способы защиты от вредоносных воздействий на обучающие данные, обнаружения выбросов (аномалий) и проверки точности модели машинного обучения приведены в работах [53–60].

Известно, что архитектуры и принципы работы различных систем искусственного интеллекта существенно отличаются друг от друга, но для оценивания возможности атак на системы искусственного интеллекта надо учитывать следующие характеристики: точность (следует отличать работу на тестовых выборках и в реальных условиях), интерпретируемость (одна из наиболее важных характеристик, которая показывает, что система в состоянии объяснить принятое решение), параметрические или непараметрические модели (имеется ли заранее известные гипотезы и предположения), размерность данных для обработки, требуемая вычислительная архитектура (процессоры общего назначения, графические и нейроморфные).

Перечислим основные векторы атак на системы искусственного интеллекта, которые отражены в отчете по уязвимостям SonicWall[14]:

- искажение разметки;
- искажение обучающей выборки;
- атаки «белого ящика» и «черного ящика»;
- атаки на предобученные и аутсорсинговые ML-модели;
- утечки через обученные модели, атаки на уровне аппаратного обеспечения.

При рассмотрении различных систем следует

14 2022 SonicWall Cyber Threat Report https://www.infopoint-security.de/media/2022-sonicwall-cyber-threat-report.pdf

отметить, что возможны атаки на криптографические алгоритмы с использованием технологий ИИ, а также на стенографические алгоритмы для проведения стегоанализа [61].

В акустическом и радио каналах утечки информации следует уделять большое значение проведению моделирования свойств канала, поведению злоумышленника, работе средств перехвата и средств защиты. Технологии искусственного интеллекта используются как для «проигрывания» различных сценариев, так и для обработки сигналов, которые регистрируются в канале утечки. Очевидно, что с использованием искусственного интеллекта появляется возможность проведения анализа сигналов с учетом фоновой обстановки и последующей его интерпретации, поиска полезных сигналов [62–77].

Развитие средств физический защиты и нападения в настоящее время использует повышение интеллектуализации (читай искусственного интеллекта) для обеспечения периметровой охраны. Средства интеллектуализации позволяют провести моделирование различных угроз и поведения нарушителя, а также обеспечить на рубежах охраны контроль с использование средств распознавания. Следует учитывать, что даже использование воздушного зазора в критических системах не позволяет быть уверенными в безопасности всей системы.

Следует отметить, что алгоритмы искусственного интеллекта могут быть использованы и для исследования организационно-социальных и политических направлений [78]. Использование систем искусственного интеллекта с языковыми моделями типа ChatGPT для получения различной аналитической информации позволяет повысить эффективности деятельности аналитических подразделений. Спектр применения больших языковых моделей очень широк и позволяет не только проводить указанную аналитическую деятельность и конкурентную разведку, но и генерировать уникальный контент, в том числе вредоносный и ложный «человекоподобный», который используется для проведения атак социальной инженерии, например, фишинга с использованием телефонного канала.

Ряд систем генеративного искусственного интеллекта подвержены не только «переобучениям». Результатом запроса информации в таких системах может быть информация, которая отсутствует в обучающей выборке, может противоречить ей, однако по структуре соответствует реальной информации – этот результат называют «галлюцинацией». Указанная уязвимость может быть эксплуатируема злоумышленниками, а противодействие ей может быть осуществлено только путем создания доверенного искусственного интеллекта [79] за счет объяснимости и верификации выходных результатов работы.

Заключение

Актуальность использования технологий искусственного интеллекта в области обеспечения безопасности приобретает решающее значение. Тот, кто будет владеть технологиями, тот и будет превосходить противника вне зависимости от выполняемой атакующей или нападающий функции. Представляется важным нормативно регулировать деятельность систем искусственного интеллекта [80].

Рассмотренные в настоящей статье подходы систематизируют использование ИИ для обеспечения безопасности и защиты информации от утечек по различным техническим каналам, а также целостности и доступности. Развитие технологий искусственного интеллекта для обработки сигналов и данных различной природы будет ставить перед специалистами по защите информации новые задачи, формировать требования к средствам защиты и к разработке моделей каналов утечки информации.

Работа выполнена при финансовой поддержке гранта РНФ № 24-11-00340

Литература

1. *Марков А. С. Кибербезопасность и информационная безопасность как бифуркация номенклатуры научных специальностей // Вопросы кибербезопасности. 2022, № 1(47), с. 2–10.*
2. *Язов Ю. К. О научных специальностях «кибербезопасность» и «Методы и системы защиты информации. Информационная безопасность» // Вопросы кибербезопасности. 2022, № 2(48), с. 5-6.*
3. *Толстой А. И. Систематика понятий в области информационной безопасности. Безопасность информационных технологий, 2023, т. 30, № 1, с. 130–148.*
4. *Мельников С. Ю., Пересыпкин В. А. Об эволюции классических вероятностных моделей языка в естественно-языковых приложениях. Вестник современных цифровых технологий. 2023, № 16, с. 4–14.*
5. *Информационные измерения языка. Программная система оценки читаемости искаженных текстов / А. В. Германович, С. Ю. Мельников, В. А. Пересыпкин [и др.] // Известия ЮФУ. Технические науки. 2019, № 7 (209), с. 6–17.*
6. *Иванов А. И., Сулавко А. Е. Проект третьего национального стандарта России по быстрому автоматическому обучению больших сетей корреляционных нейронов на малых обучающих выборках биометрических данных // Вопросы кибербезопасности. 2021, № 3(43), с. 84–93.*

7. Машкина И. В., Белова Е. П. Разработка нейросетевой базы данных биометрических образов на основе нескольких параметров спектров гласных звуков для системы аутентификации и авторизации по голосу // Безопасность информационных технологий. 2019, т. 26, № 3, с. 90–102.
8. Костюченко Е. Ю., Мещеряков Р. В. Идентификация по биометрическим параметрам при использовании аппарата нейронных сетей // Нейрокомпьютеры: разработка, применение. 2007, № 7, с. 39–50.
9. Матвеев Ю. Н. Технологии биометрической идентификации личности по голосу и другим модальностям // Вестник Московского государственного технического университета им. Н.Э. Баумана. 2012, № 3 (3), с. 5–15.
10. Ziems N., Wu S. Security Vulnerability Detection Using Deep Learning Natural Language Processing, IEEE INFOCOM 2021-IEEE Conference on Computer Communications Workshops, 2021, pp. 1–6.
11. Morris J. X. et al. Textattack: A framework for adversarial attacks in natural language processing. 2020. DOI: https://doi.org/10.48550/arXiv.2005.05909.
12. Сидняев Н. И., Синева Е. Е. Построение составных критериев для оптимизации термов и обобщенного показателя баз знаний интеллектуальных систем // Вопросы кибербезопасности. 2023, № 2(54), с. 23–35.
13. Васильев В. И., Вульфин А. М., Кучкарова Н. В. Тематическое моделирование и суммаризация текстов в области кибербезопасности // Вопросы кибербезопасности. 2023, № 2(54), с. 2–22.
14. Baek S., Kim K. Recent advances of neural attacks against block ciphers //Proc. of SCIS. 2020.
15. Amigo G., Dong L., Ii R. J. M. Forecasting pseudo random numbers using deep learning // 2021 15th International Conference on Signal Processing and Communication Systems (ICSPCS). – IEEE, 2021. pp. 1–7.
16. Feng Y., Hao L. Testing randomness using artificial neural network //IEEE Access. 2020, Vol. 8, pp. 163685-163693.
17. Truong N. D. et al. Machine learning cryptanalysis of a quantum random number generator //IEEE Transactions on Information Forensics and Security. 2018, Т. 14, №. 2, с. 403–414.
18. Язов Ю. К., Соловьев С. В., Тарелкин М. А Логико-лингвистическое моделирование угроз безопасности информации в информационных системах // Вопросы кибербезопасности. 2022, № 4(50), с. 13–25.
19. Васильев В. И., Вульфин А. М., Герасимова И. Б., Картак В. М. Анализ рисков кибербезопасности с помощью нечетких когнитивных карт // Вопросы кибербезопасности. 2020, № 2(36), с. 11–21.
20. Васильев В. И., Вульфин А. М., Кучкарова Н. В. Оценка актуальных угроз безопасности информации с помощью технологии трансформеров // Вопросы кибербезопасности. 2022, № 2(48), с. 27–38.
21. Плугатарев А. В. и др. Применение нейронных сетей в системах обеспечения информационной безопасности // Безопасность информационных технологий, 2021, т. 28, № 3, с. 73–80.
22. Парьев С. Е., Правиков Д. И., Карантаев В. Г. Особенности применения риск-ориентированного подхода для обеспечения кибербезопасности промышленных объектов // Безопасность информационных технологий. 2020, т. 27, № 4, с. 37–52.
23. Воеводин В. А. Модель оценки функциональной устойчивости элементов информационной инфраструктуры для условий воздействия множества компьютерных атак. Информатика и автоматизация, 2023, 22(3), с. 691–715
24. Селифанов В. В., Солдатов А. Ю., Солдатов Е. Ю., Подлегаев А. П., Скориков В. С. Метод оценивания рисков в системах принятия решений с учетом защиты информации. Вестник СибГУТИ. 2023; 17(2). с. 84–92.
25. Ермаков С. А., Чурсин А. Г., Болгов А. А. Нечетко-множественная методика оценки рисков автоматизированной системы «Умный дом» с динамической топологией Информация и безопасность. 2022, Том: 25, № 4, с. 495–500.
26. Ермаков С. А., Болгов А. А. Оценка риска с использованием нейро-нечеткой системы // Информация и безопасность. 2022, Том: 25, № 4, с. 583–592.
27. Ермаков С. А., Гусарева Ю. А., Болгов А. А., Кострова В. Н. Повышение защищенности автоматизированной системы «умный дом»: алгоритм оценки рисков нарушения конфиденциальности информации // Информация и безопасность. 2022, Том: 25, № 3, с. 377–388.
28. Космачева И. М., Давидюк Н. В., Сибикина И. В., Кучин И. Ю. Модель оценки эффективности конфигурации системы защиты информации на базе генетических алгоритмов // Моделирование, оптимизация и информационные технологии. 2020; 8(3). Доступно по: https://moit.vivt.ru/wp-content/uploads/2020/08/KosmachevaSoavtors_3_20_1.pdf DOI: 10.26102/2310-6018/2020.30.3.022.
29. Семенов В. В. Оценивание состояния информационной безопасности на основе анализа временных рядов // Научно-технический вестник Поволжья. 2021, № 10, с. 127–129.
30. Рычкова А. А., Бурькова Е. В., Коннов А. Л. Анализ угроз информационной безопасности на основе метода кластеризации данных // Научно-технический вестник Поволжья. 2023, № 6, с. 307–310.
31. Промыслов В. Г., Акимов Н. Н., Абдулова Е. А., Голубев П. А., Жарко Е. Ф., Жмайлов В. В., Лепехин И. Ю., Лобанок О. И., Исхаков А. Ю., Мещеряков Р. В., Полетыкин А. Г., Мусихин А. М., Пронин В. В., Семенков К. В., Цыренов Д. В. Оценка риска и обеспечение кибербезопасности атомных электростанций. М.: ИПУ РАН, 2022. – 193 с.
32. Жарко Е. Ф., Промыслов В. Г., Исхаков А. Ю., Мещеряков Р. В., Семенков К. В., Абдулова Е. А., Байбулатов А. А., Исхаков С. Ю. Кибербезопасность беспилотных транспортных средств. Архитектура. Методы проектирования. М.: Радиотехника, 2021. – 160 с.
33. Ветров И. А., Подтопельный В.В. Особенности формирования вектора современных сетевых атак. Вестник СибГУТИ. 2022, № 3, с. 3–13.
34. Мещеряков Р. В., Исхаков А. Ю., Евсютин О. О. Современные методы обеспечения целостности данных в протоколах управления киберфизических систем. Информатика и автоматизация. 2020, 19(5), с. 1089–1122.
35. Букин А. В., Самонов А. В., Тихонов Э. И. Обнаружение инцидентов информационной безопасности на основе технологии нейронных сетей // Вопросы кибербезопасности. 2022, № 5(51), с. 61–73.
36. Саенко И. Б., Котенко И. В., Аль-Барри М. Х. Применение искусственных нейронных сетей для выявления аномального поведения пользователей центров обработки данных // Вопросы кибербезопасности. 2022, № 2(48), с. 87–97.
37. Меркальдо Ф., Мартинелли Ф., Сантоне А. Проверка модели для обнаружения атак в реальном времени в системах распределения воды. Информатика и автоматизация. 2022, 21(2), с. 219–242.
38. Штыркина А. А. Метод реконфигурации топологии киберфизической системы на основе графовой искусственной нейронной сети // Проблемы информационной безопасности. Компьютерные системы. 2023, 2 (54), с. 173–182.

39. *Сергадеева А. И., Лаврова Д. С. Применение модульной нейронной сети для обнаружения DDOS-атак // Проблемы информационной безопасности. Компьютерные системы 2023, № 1 (53), с. 111–118.*
40. *Александрова Е. Б., Штыркина А. А. Метод адаптивной нейтрализации структурных нарушений киберфизических систем на основе графовых искусственных нейронных сетей // Проблемы информационной безопасности. Компьютерные системы. 2023, № 4 (52), с. 89-100.*
41. *Царькова Е. Г. К вопросу применения искусственных нейронных сетей в системах обеспечения транспортной безопасности // Проблемы информационной безопасности. Компьютерные системы. 2022, Том: 3, № 3 (3), с. 28–34.*
42. *Кубасов И. А., Сушков В. И. Применение технологий искусственного интеллекта в робототехнических комплексах специального назначения в целях обеспечения правоохранительной деятельности // Вестник Воронежского института ФСИН России. 2022, № 3, с. 69–76.*
43. *Алексеенко С. П., Достов В. В. Нейросети и информационная безопасность в правоохранительных структурах // Охрана, безопасность, связь. 2022, № 7-2, с. 11–16.*
44. *Атаки на искусственный интеллект. Как защитить машинное обучение в системах безопасности. Александр Чистяков, Алексей Андреев «Лаборатория Касперского», Департамент исследования угроз. https://media.kaspersky.com/ru/business-security/attacks-on-artificial-intelligence-whitepaper.pdf*
45. *Котенко И. В., Саенко И. Б., Лаута О. С., Крибель А. М. Методика обнаружения аномалий и кибератак на основе интеграции методов фрактального анализа и машинного обучения. Информатика и автоматизация, 2022, 21(6), с. 1328–1358.*
46. *Зегжда Д. П., Калинин М. О., Крундышев В. М., Лаврова Д. С., Москвин Д. А., Павленко, Е. Ю. Применение алгоритмов биоинформатики для обнаружения мутирующих кибератак // Информатика и автоматизация, 2021, 20(4), с. 820–844.*
47. *Калинин М. О., Ткачева Е. И. Децентрализованный подход к обнаружению вторжений в динамических сетях интернета вещей на базе многоагентного обучения с подкреплением и межагентным взаимодействием // Проблемы информационной безопасности. Компьютерные системы. 2023, № 2 (54), с. 202–211.*
48. *Калинкин А. О. и др. Обнаружение программ-шифровальщиков на основе данных механизма трассировки событий и применения метода машинного обучения // Безопасность информационных технологий. 2022, т. 29, № 3, с. 82–93.*
49. *Синюк А. Д., Остроумов О. А., Тарасов А. А. (). Теоретико-информационное представление виртуализации сетевого канала перехвата // Информатика и автоматизация. 2023, 22(4), с. 721–744.*
50. *Макарова О. С., Поршнев С. В. Оценивание вероятностей компьютерных атак на основе функций // Безопасность информационных технологий. 2020, т. 27, № 2, с. 86–96.*
51. *Марков Г. А., Крундышев В. М., Калинин М. О., Зегжда Д. П., Бусыгин А. Г. Обнаружение компьютерных атак в сетях промышленного интернета вещей на основе вычислительной модели иерархической временной памяти // Проблемы информационной безопасности. Компьютерные системы. 2023, № 2 (54), с. 163–172.*
52. *Мещеряков Р.В., Исхаков С.Ю. Исследование индикаторов компрометации для средств защиты информационных и киберфизических систем // Вопросы кибербезопасности. 2022, № 5 (51), с. 82–99.*
53. *Павлова К. С. Применение предметных онтологий в области обеспечения безопасности информации // Проблемы информационной безопасности. Компьютерные системы. 2023, Том: 1, № 1 (1), с. 24–29.*
54. *Ручай А. Н., Токарев И. В., Грибачёв А. С. Методы машинного обучения и искусственного интеллекта в сфере информационной безопасности: анализ современного состояния и перспективы развития // Вестник УрФО. Безопасность в информационной сфере. 2022, 4 (46), с. 76–87.*
55. *Артамонов В. А., Артамонова Е. В., Сафонов А. Е. Безопасность искусственного интеллекта // Защита информации. Инсайд. 2022, № 6 (108), с. 8–17.*
56. *Артамонов В. А., Артамонова Е. В. Искусственный интеллект в системах безопасности // Защита информации. Инсайд. 2022, № 5 (107), с. 40–49.*
57. *Лебедев И. С., Сухопаров М. Е. Использование информации о влияющих факторах для разбиения выборок данных в методах машинного обучения для оценки состояния ИБ // Проблемы информационной безопасности. Компьютерные системы. 2023, №2 (54), с. 125–134.*
58. *Sarker I., Kayes A., Badsha S., Alqahtani H., Watters P., Ng A. Cybersecurity data science: an overview from machine learning perspective. Journal of Big Data, 2020.*
59. *Musser M., Garriott A. Machine Learning and Cybersecurity. Center for Security and Emerging Technology, 2021.*
60. *Чекмарев М. А., Клюев С. Г., Бобров Н. Д. Анализ методов обеспечения безопасности систем машинного обучения. Моделирование, оптимизация и информационные технологии. 2022; 10(1). DOI: 10.26102/2310-6018/2022.36.1.006*
61. *Evsutin O., Melman A., Meshcheryakov R. Digital steganography and watermarking for digital images: a review of current research directions IEEE Access. 2020, Vol. 8, pp. 166589–166611.*
62. *Хорев А. А. Некоторые подходы к оценке возможностей перехвата побочных электромагнитных излучений средств вычислительной техники, использующих цифровые интерфейсы // Вестник УрФО. Безопасность в информационной сфере. 2022, № 3 (45), с. 5–16.*
63. *Сычев М. П., Мазин А. В., Зеленцова Е. В., Крылов В. О., Сидельников А. П. Функциональные аспекты моделирования процесса перехвата информативных сигналов по параметрическим каналам // Приборы и системы. Управление, контроль, диагностика. 2022, № 2, с. 22–33.*
64. *Сычев М. П., Никулин С. С., Маньков Е. А. Перехват информации по параметрическим каналам: структуризация функционального представления этапа обработки перехваченных информативных сигналов с целью формирования целостного объема информации об объекте разведки // Вестник Воронежского института МВД России. 2023, № 2, с. 87–93.*
65. *Мещеряков Р. В., Лось В. П., Щербаков В. А., Рекунков И. С. Математическое моделирование защитных экранов для предотвращения утечки информации по техническим каналам в радиодиапазоне // Вопросы защиты информации. 2023, № 1 (140), с. 47–52.*
66. *Копытов П. Д., Королёв И. Д., Кулиш О. А., Степанцов С. В. Построение формальных моделей распространения побочных электромагнитных излучений по техническим каналам утечки информации для объектов вычислительной техники от технических средств разведки // Вестник УрФО. Безопасность в информационной сфере. 2023, № 1 (47), с. 102–111.*

67. Захаров А. В. Требования к современному программно-аппаратному комплексу радиоконтроля и цифрового анализа сигналов // Защита информации. Инсайд. 2022, № 1 (103), с. 24–33.
68. Алексеенко С. П., Антиликаторов А. Б., Астахов Н. В. Методика выбора модели охраны объекта радиотехническими средствами обнаружения // Вестник Воронежского института МВД России. 2023, № 1, с. 57–62.
69. Аверьянов А. А., Шадрив В. В., Бердюгин В. Ю. Математическая модель оценки угроз физического проникновения злоумышленника на защищенный объект // Вестник УрФО. Безопасность в информационной сфере. 2022, № 4 (46), с. 52–57.
70. Язов Ю. К., Соловьев С. В., Тарелкин М. А. Применение составных сетей Петри-Маркова при математическом моделировании угроз безопасности информации // Охрана, безопасность, связь. 2023, № 8–2, с. 185–196.
71. Авсентьев А. О. Проблема построения многоагентных систем защиты информации на объектах информатизации от утечки по техническим каналам // Вестник Воронежского института МВД России. 2022, № 3, с. 68–77.
72. Калач А. В., Здольник В. В. Математическая модель показателя эффективности мер, направленных на предотвращение утечки информации по каналам побочных электромагнитных излучений и наводок. Вестник Воронежского института ФСИН России. 2022, № 1, с. 54–61.
73. Минаев В. А., Коробец Б. Н., Сычев М. П., Севрюков Д. В., Дудоладов В. А. Ключевые функциональные показатели радиотехнических средств обнаружения проникновения на охраняемые объекты // Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. 2019, № 5–6 (131-132), с. 3–7.
74. Алексеев Д. С., Козлов Р. С. Метод практической оценки эффективности средств активной защиты от утечки конфиденциальной информации по техническому каналу // Научно-технический вестник Поволжья. 2023, № 4, с. 201–204.
75. Бурькова Е. В., Рычкова А. А. Методика принятия решений при выборе средств физической защиты на основе метода анализа иерархии // Научно-технический вестник Поволжья. 2021, № 5, с. 119–123.
76. Авсентьев О. С., Вальде А. Г. Вербальная модель защиты информации от утечки по техническим каналам в процессе формирования системы защиты информации на объектах информатизации // Вестник Воронежского института МВД России. 2022, № 2, с. 18–27.
77. Пантюхов Д. В., Логинов И. В. Варианты построения интеллектуальных систем физической безопасности с учетом развития технологий интеллектуализации // Охрана, безопасность, связь. 2023, № 8-1, с. 155–159.
78. Костогрызов А. И. Подход к вероятностному прогнозированию защищенности репутации политических деятелей от «фейковых» угроз в публичном информационном пространстве // Вопросы кибербезопасности. 2023, № 3 (55), с. 114–133
79. Аветисян А. И. Использование доверенного ПО при создании систем искусственного интеллекта как основа безопасности (доклад) // XXVII научно-практическая конференция «Комплексная защита информации», 24–26 мая 2022 года, Московская область.
80. Гарбук С. В. Задачи нормативно-технического регулирования интеллектуальных систем информационной безопасности // Вопросы кибербезопасности. 2021, № 3 (43), с. 68–83.

References

1. Markov A. S. Kiberbezopasnost' i informacionnaja bezopasnost' kak bifurkacija nomenklatury nauchnyh special'nostej // Voprosy kiberbezopasnosti. 2022, № 1(47), s. 2–10.
2. Jazov Ju. K. O nauchnyh special'nostjah «kiberbezopasnost'» i «Metody i sistemy zashhity informacii. Informacionnaja bezopasnost'» // Voprosy kiberbezopasnosti. 2022, № 2(48), s. 5-6.
3. Tolstoj A. I. Sistematika ponjatij v oblasti informacionnoj bezopasnosti. Bezopasnost' informacionnyh tehnologij, 2023, t. 30, № 1, s. 130–148.
4. Mel'nikov S. Ju., Peresypkin V. A. Ob jevoljucii klassicheskih verojatnostnyh modelej jazyka v estestvenno-jazykovyh prilozhenijah. Vestnik sovremennyh cifrovyh tehnologij. 2023, № 16, s. 4–14.
5. Informacionnye izmerenija jazyka. Programmnaja sistema ocenki chitaemosti iskazhennyh tekstov / A. V. Germanovich, S. Ju. Mel'nikov, V. A. Peresypkin [i dr.] // Izvestija JuFU. Tehnicheskie nauki. 2019, № 7 (209), s. 6–17.
6. Ivanov A. I., Sulavko A. E. Proekt tret'ego nacional'nogo standarta Rossii po bystromu avtomaticheskomu obucheniju bol'shih setej korreljacionnyh nejronov na malyh obuchajushhih vyborkah biometricheskih dannyh // Voprosy kiberbezopasnosti. 2021, № 3(43), s. 84–93.
7. Mashkina I. V., Belova E. P. Razrabotka nejrosetevoj bazy dannyh biometricheskih obrazov na osnove neskol'kih parametrov spektrov glasnyh zvukov dlja sistemy autentifikacii i avtorizacii po golosu // Bezopasnost' informacionnyh tehnologij. 2019, t. 26, № 3, s. 90–102.
8. Kostjuchenko E. Ju., Meshherjakov R. V. Identifikacija po biometricheskim parametram pri ispol'zovanii apparata nejronnyh setej // Nejrokomp'jutery: razrabotka, primenenie. 2007, № 7, s. 39–50.
9. Matveev Ju. N. Tehnologii biometricheskoj identifikacii lichnosti po golosu i drugim modal'nostjam // Vestnik Moskovskogo gosudarstvennogo tehnicheskogo universiteta im. N.Je. Baumana. 2012, № 3 (3), s. 5–15.
10. Ziems N., Wu S. Security Vulnerability Detection Using Deep Learning Natural Language Processing, IEEE INFOCOM 2021-IEEE Conference on Computer Communications Workshops, 2021, pp. 1–6.
11. Morris J. X. et al. Textattack: A framework for adversarial attacks in natural language processing. 2020. DOI: https://doi.org/10.48550/arXiv.2005.05909.
12. Sidnjaev N. I., Sineva E. E. Postroenie sostavnyh kriteriev dlja optimizacii termov i obobshhennogo pokazatelja baz znanij intellektual'nyh sistem // Voprosy kiberbezopasnosti. 2023, № 2(54), s. 23–35.
13. Vasil'ev V. I., Vul'fin A.M., Kuchkarova N. V. Tematicheskoe modelirovanie i summarizacija tekstov v oblasti kiberbezopasnosti // Voprosy kiberbezopasnosti. 2023, № 2(54), s. 2–22.
14. Baek S., Kim K. Recent advances of neural attacks against block ciphers //Proc. of SCIS. 2020.
15. Amigo G., Dong L., Ii R. J. M. Forecasting pseudo random numbers using deep learning // 2021 15th International Conference on Signal Processing and Communication Systems (ICSPCS). – IEEE, 2021. pp. 1–7.
16. Feng Y., Hao L. Testing randomness using artificial neural network //IEEE Access. 2020, Vol. 8, pp. 163685–163693.
17. Truong N. D. et al. Machine learning cryptanalysis of a quantum random number generator //IEEE Transactions on Information Forensics and Security. 2018, T. 14, №. 2, s. 403–414.

18. Jazov Ju. K., Solov'ev S. V., Tarelkin M.A Logiko-lingvisticheskoe modelirovanie ugroz bezopasnosti informacii v informacionnyh sistemah // Voprosy kiberbezopasnosti. 2022, № 4(50), s. 13–25.
19. Vasil'ev V. I., Vul'fin A. M., Gerasimova I. B., Kartak V. M. Analiz riskov kiberbezopasnosti s pomoshh'ju nechetkih kognitivnyh kart // Voprosy kiberbezopasnosti. 2020, № 2(36), s. 11–21.
20. Vasil'ev V. I., Vul'fin A. M., Kuchkarova N. V. Ocenka aktual'nyh ugroz bezopasnosti informacii s pomoshh'ju tehnologii transformerov // Voprosy kiberbezopasnosti. 2022, № 2(48), s. 27–38.
21. Plugatarev A. V. i dr. Primenenie nejronnyh setej v sistemah obespechenija informacionnoj bezopasnosti // Bezopasnost' informacionnyh tehnologij, 2021, t. 28, № 3, s. 73–80.
22. Par'ev S. E., Pravikov D. I., Karantaev V. G. Osobennosti primenenija risk-orientirovannogo podhoda dlja obespechenija kiberbezopasnosti promyshlennyh ob#ektov // Bezopasnost' informacionnyh tehnologij. 2020, t. 27, № 4, s. 37–52.
23. Voevodin V. A. Model' ocenki funkcional'noj ustojchivosti jelementov informacionnoj infrastruktury dlja uslovij vozdejstvija mnozhestva komp'juternyh atak. Informatika i avtomatizacija, 2023, 22(3), s. 691–715
24. Selifanov V. V., Soldatov A. Ju., Soldatov E. Ju., Podlegaev A. P., Skorikov V. S. Metod ocenivanija riskov v sistemah prinjatija reshenij s uchetom zashhity informacii. Vestnik SibGUTI. 2023; 17(2). s. 84–92.
25. Ermakov S. A., Chursin A. G., Bolgov A. A. Nechetko-mnozhestvennaja metodika ocenki riskov avtomatizirovannoj sistemy «Umnyj dom» s dinamicheskoj topologiej Informacija i bezopasnost'. 2022, Tom: 25, № 4, s. 495–500.
26. Ermakov S. A., Bolgov A. A. Ocenka riska s ispol'zovaniem nejro-nechetkoj sistemy // Informacija i bezopasnost'. 2022, Tom: 25, № 4, s. 583–592.
27. Ermakov S. A., Gusareva Ju. A., Bolgov A. A., Kostrova V. N. Povyshenie zashhishhennosti avtomatizirovannoj sistemy «umnyj dom»: algoritm ocenki riskov narushenija konfidencial'nosti informacii // Informacija i bezopasnost'. 2022, Tom: 25, № 3, s. 377–388.
28. Kosmacheva I. M., Davidjuk N. V., Sibikina I. V., Kuchin I. Ju. Model' ocenki jeffektivnosti konfiguracii sistemy zashhity informacii na baze geneticheskih algoritmov // Modelirovanie, optimizacija i informacionnye tehnologii. 2020; 8(3). Dostupno po: https://moit.vivt.ru/wp-content/uploads/2020/08/KosmachevaSoavtors_3_20_1.pdf DOI: 10.26102/2310-6018/2020.30.3.022.
29. Semenov V. V. Ocenivanie sostojanija informacionnoj bezopasnosti na osnove analiza vremennyh rjadov // Nauchno-tehnicheskij vestnik Povolzh'ja. 2021, № 10, s. 127–129.
30. Rychkova A. A., Bur'kova E. V., Konnov A. L. Analiz ugroz informacionnoj bezopasnosti na osnove metoda klasterizacii dannyh // Nauchno-tehnicheskij vestnik Povolzh'ja. 2023, № 6, s. 307–310.
31. Promyslov V. G., Akimov N. N., Abdulova E. A., Golubev P. A., Zharko E. F., Zhmajlov V. V., Lepehin I. Ju., Lobanok O. I., Ishakov A. Ju., Meshherjakov R. V., Poletykin A. G., Musihin A. M., Pronin V. V., Semenkov K. V., Cyrenov D. V. Ocenka riska i obespechenie kiberbezopasnosti atomnyh jelektrostancij. M.: IPU RAN, 2022. – 193 s.
32. Zharko E. F., Promyslov V. G., Ishakov A. Ju., Meshherjakov R. V., Semenkov K. V., Abdulova E. A., Bajbulatov A. A., Ishakov S. Ju. Kiberbezopasnost' bespilotnyh transportnyh sredstv. Arhitektura. Metody proektirovanija. M.: Radiotehnika, 2021. – 160 s.
33. Vetrov I. A., Podtopel'nyj V. V. Osobennosti formirovanija vektora sovremennyh setevyh atak. Vestnik SibGUTI. 2022, № 3, s. 3–13.
34. Meshherjakov R. V., Ishakov A. Ju., Evsjutin O. O. Sovremennye metody obespechenija celostnosti dannyh v protokolah upravlenija kiberfizicheskih sistem. Informatika i avtomatizacija. 2020, 19(5), s. 1089–1122.
35. Bukin A. V., Samonov A. V., Tihonov Je. I. Obnaruzhenie incidentov informacionnoj bezopasnosti na osnove tehnologii nejronnyh setej // Voprosy kiberbezopasnosti. 2022, № 5(51), s. 61–73.
36. Saenko I. B., Kotenko I. V., Al'-Barri M. H. Primenenie iskusstvennyh nejronnyh setej dlja vyjavlenija anomal'nogo povedenija pol'zovatelej centrov obrabotki dannyh // Voprosy kiberbezopasnosti. 2022, № 2(48), s. 87–97.
37. Merkal'do F., Martinelli F., Santone A. Proverka modeli dlja obnaruzhenija atak v real'nom vremeni v sistemah raspredelenija vody. Informatika i avtomatizacija. 2022, 21(2), s. 219–242.
38. Shtyrkina A. A. Metod rekonfiguracii topologii kiberfizicheskoj sistemy na osnove grafovoj iskusstvennoj nejronnoj seti // Problemy informacionnoj bezopasnosti. Komp'juternye sistemy. 2023, 2 (54), s. 173–182.
39. Sergadeeva A. I., Lavrova D. S. Primenenie modul'noj nejronnoj seti dlja obnaruzhenija DDOS-atak // Problemy informacionnoj bezopasnosti. Komp'juternye sistemy 2023, № 1 (53), s. 111–118.
40. Aleksandrova E. B., Shtyrkina A. A. Metod adaptivnoj nejtralizacii strukturnyh narushenij kiberfizicheskih sistem na osnove grafovyh iskusstvennyh nejronnyh setej // Problemy informacionnoj bezopasnosti. Komp'juternye sistemy. 2023, № 4 (52), s. 89-100.
41. Car'kova E. G. K voprosu primenenija iskusstvennyh nejronnyh setej v sistemah obespechenija transportnoj bezopasnosti // Problemy informacionnoj bezopasnosti. Komp'juternye sistemy. 2022, Tom: 3, № 3 (3), s. 28–34.
42. Kubasov I. A., Sushkov V. I. Primenenie tehnologij iskusstvennogo intellekta v robototehnicheskih kompleksah special'nogo naznachenija v celjah obespechenija pravoohranitel'noj dejatel'nosti // Vestnik Voronezhskogo instituta FSIN Rossii. 2022, № 3, s. 69–76.
43. Alekseenko S. P., Dostov V. V. Nejroseti i informacionnaja bezopasnost' v pravoohranitel'nyh strukturah // Ohrana, bezopasnost', svjaz'. 2022, № 7-2, s. 11–16.
44. Ataki na iskusstvennyj intellekt. Kak zashhitit' mashinnoe obuchenie v sistemah bezopasnosti. Aleksandr Chistjakov, Aleksej Andreev «Laboratorija Kasperskogo», Departament issledovanija ugroz. https://media.kaspersky.com/ru/business-security/attacks-on-artificial-intelligence-whitepaper.pdf
45. Kotenko I. V., Saenko I. B., Lauta O. S., Kribel' A. M. Metodika obnaruzhenija anomalij i kiberatak na osnove integracii metodov fraktal'nogo analiza i mashinnogo obuchenija. Informatika i avtomatizacija, 2022, 21(6), s. 1328–1358.
46. Zegzhda D. P., Kalinin M. O., Krundyshev V. M., Lavrova D. S., Moskvin D. A., Pavlenko, E. Ju. Primenenie algoritmov bioinformatiki dlja obnaruzhenija mutirujushhih kiberatak // Informatika i avtomatizacija, 2021, 20(4), s. 820–844.
47. Kalinin M. O., Tkacheva E. I. Decentralizovannyj podhod k obnaruzheniju vtorzhenij v dinamicheskih setjah interneta veshhej na baze mnogoagentnogo obuchenija s podkrepleniem i mezhagentnym vzaimodejstviem // Problemy informacionnoj bezopasnosti. Komp'juternye sistemy. 2023, № 2 (54), s. 202–211.
48. Kalinkin A. O. i dr. Obnaruzhenie programm-shifroval'shhikov na osnove dannyh mehanizma trassirovki sobytij i primenenija metoda mashinnogo obuchenija // Bezopasnost' informacionnyh tehnologij. 2022, t. 29, № 3, s. 82–93.
49. Sinjuk A. D., Ostroumov O. A., Tarasov A. A. (). Teoretiko-informacionnoe predstavlenie virtualizacii setevogo kanala perehvata // Informatika i avtomatizacija. 2023, 22(4), s. 721–744.

50. *Makarova O. S., Porshnev S. V. Ocenivanie verojatnostej komp'juternyh atak na osnove funkcij // Bezopasnost' informacionnyh tehnologij. 2020, t. 27, № 2, s. 86-96.*
51. *Markov G. A., Krundyshev V. M., Kalinin M. O., Zegzhda D. P., Busygin A. G. Obnaruzhenie komp'juternyh atak v setjah promyshlennogo interneta veshhej na osnove vychislitel'noj modeli ierarhicheskoj vremennoj pamjati // Problemy informacionnoj bezopasnosti. Komp'juternye sistemy. 2023, № 2 (54), s. 163–172.*
52. *Meshherjakov R. V., Ishakov S. Ju. Issledovanie indikatorov komprometacii dlja sredstv zashhity informacionnyh i kiberfizicheskih sistem // Voprosy kiberbezopasnosti. 2022, № 5 (51), s. 82–99.*
53. *Pavlova K. S. Primenenie predmetnyh ontologij v oblasti obespechenija bezopasnosti informacii // Problemy informacionnoj bezopasnosti. Komp'juternye sistemy. 2023, Tom: 1, № 1 (1), s. 24–29.*
54. *Ruchaj A. N., Tokarev I. V., Gribachjov A. S. Metody mashinnogo obuchenija i iskusstvennogo intellekta v sfere informacionnoj bezopasnosti: analiz sovremennogo sostojanija i perspektivy razvitija // Vestnik UrFO. Bezopasnost' v informacionnoj sfere. 2022, 4 (46), s. 76–87.*
55. *Artamonov V. A., Artamonova E. V., Safonov A. E. Bezopasnost' iskusstvennogo intellekta // Zashhita informacii. Insajd. 2022, № 6 (108), s. 8–17.*
56. *Artamonov V. A., Artamonova E. V. Iskusstvennyj intellekt v sistemah bezopasnosti // Zashhita informacii. Insajd. 2022, № 5 (107), s. 40–49.*
57. *Lebedev I. S., Suhoparov M. E. Ispol'zovanie informacii o vlijajushhih faktorah dlja razbienija vyborok dannyh v metodah mashinnogo obuchenija dlja ocenki sostojanija IB // Problemy informacionnoj bezopasnosti. Komp'juternye sistemy. 2023, №2 (54), s. 125–134.*
58. *Sarker I., Kayes A., Badsha S., Alqahtani H., Watters P., Ng A. Cybersecurity data science: an overview from machine learning perspective. Journal of Big Data, 2020.*
59. *Musser M., Garriott A. Machine Learning and Cybersecurity. Center for Security and Emerging Technology, 2021.*
60. *Chekmarev M. A., Kljuev S. G., Bobrov N. D. Analiz metodov obespechenija bezopasnosti sistem mashinnogo obuchenija. Modelirovanie, optimizacija i informacionnye tehnologii. 2022; 10(1). DOI: 10.26102/2310-6018/2022.36.1.006*
61. *Evsutin O., Melman A., Meshcheryakov R. Digital steganography and watermarking for digital images: a review of current research directions IEEE Access. 2020, Vol. 8, pp. 166589–166611.*
62. *Horev A. A. Nekotorye podhody k ocenke vozmozhnostej perehvata pobochnyh jelektromagnitnyh izluchenij sredstv vychislitel'noj tehniki, ispol'zujushhih cifrovye interfejsy // Vestnik UrFO. Bezopasnost' v informacionnoj sfere. 2022, № 3 (45), s. 5–16.*
63. *Sychev M. P., Mazin A. V., Zelencova E. V., Krylov V. O., Sidel'nikov A. P. Funkcional'nye aspekty modelirovanija processa perehvata informativnyh signalov po parametricheskim kanalam // Pribory i sistemy. Upravlenie, kontrol', diagnostika. 2022, № 2, s. 22–33.*
64. *Sychev M. P., Nikulin S. S., Man'kov E. A. Perehvat informacii po parametricheskim kanalam: strukturizacija funkcional'nogo predstavlenija jetapa obrabotki perehvachennyh informativnyh signalov s cel'ju formirovanija celostnogo ob#ema informacii ob ob#ekte razvedki // Vestnik Voronezhskogo instituta MVD Rossii. 2023, № 2, s. 87–93.*
65. *Meshherjakov R. V., Los' V. P., Shherbakov V. A., Rekunkov I. S. Matematicheskoe modelirovanie zashhitnyh jekranov dlja predotvrashhenija utechki informacii po tehnicheskim kanalam v radiodiapazone // Voprosy zashhity informacii. 2023, № 1 (140), s. 47–52.*
66. *Kopytov P. D., Koroljov I. D., Kulish O. A., Stepancov S. V. Postroenie formal'nyh modelej rasprostranenija pobochnyh jelektromagnitnyh izluchenij po tehnicheskim kanalam utechki informacii dlja ob#ektov vychislitel'noj tehniki ot tehnicheskih sredstv razvedki // Vestnik UrFO. Bezopasnost' v informacionnoj sfere. 2023, № 1 (47), s. 102–111.*
67. *Zaharov A. V. Trebovanija k sovremennomu programmno-apparatnomu kompleksu radiokontrolja i cifrovogo analiza signalov // Zashhita informacii. Insajd. 2022, № 1 (103), s. 24–33.*
68. *Alekseenko S. P., Antilikatorov A. B., Astahov N. V. Metodika vybora modeli ohrany ob#ekta radiotehnicheskimi sredstvami obnaruzhenija // Vestnik Voronezhskogo instituta MVD Rossii. 2023, № 1, s. 57–62.*
69. *Aver'janov A. A., Shadriv V. V., Berdjugin V. Ju. Matematicheskaja model' ocenki ugroz fizicheskogo proniknovenija zloumyshlennika na zashhishhennyj ob#ekt // Vestnik UrFO. Bezopasnost' v informacionnoj sfere. 2022, № 4 (46), s. 52–57.*
70. *Jazov Ju. K., Solov'ev S. V., Tarelkin M. A. Primenenie sostavnyh setej Petri-Markova pri matematicheskom modelirovanii ugroz bezopasnosti informacii // Ohrana, bezopasnost', svjaz'. 2023, № 8–2, s. 185–196.*
71. *Avsent'ev A. O. Problema postroenija mnogoagentnyh sistem zashhity informacii na ob#ektah informatizacii ot utechki po tehnicheskim kanalam // Vestnik Voronezhskogo instituta MVD Rossii. 2022, № 3, s. 68–77.*
72. *Kalach A. V., Zdol'nik V. V. Matematicheskaja model' pokazatelja jeffektivnosti mer, napravlennyh na predotvrashhenie utechki informacii po kanalam pobochnyh jelektromagnitnyh izluchenij i navodok. Vestnik Voronezhskogo instituta FSIN Rossii. 2022, № 1, s. 54-61.*
73. *Minaev V. A., Korobec B. N., Sychev M. P., Sevrjukov D. V., Dudoladov V. A. Kljuchevye funkcional'nye pokazateli radiotehnicheskih sredstv obnaruzhenija proniknovenija na ohranjaemye ob#ekty // Voprosy oboronnoj tehniki. Serija 16: Tehnicheskie sredstva protivodejstvija terrorizmu. 2019, № 5–6 (131-132), s. 3–7.*
74. *Alekseev D. S., Kozlov R. S. Metod prakticheskoj ocenki jeffektivnosti sredstv aktivnoj zashhity ot utechki konfidencial'noj informacii po tehnicheskomu kanalu // Nauchno-tehnicheskij vestnik Povolzh'ja. 2023, № 4, s. 201–204.*
75. *Bur'kova E. V., Rychkova A. A. Metodika prinjatija reshenij pri vybore sredstv fizicheskoj zashhity na osnove metoda analiza ierarhii // Nauchno-tehnicheskij vestnik Povolzh'ja. 2021, № 5, s. 119–123.*
76. *Avsent'ev O. S., Val'de A. G. Verbal'naja model' zashhity informacii ot utechki po tehnicheskim kanalam v processe formirovanija sistemy zashhity informacii na ob#ektah informatizacii // Vestnik Voronezhskogo instituta MVD Rossii. 2022, № 2, s. 18–27.*
77. *Pantjuhov D. V., Loginov I. V. Varianty postroenija intellektual'nyh sistem fizicheskoj bezopasnosti s uchetom razvitija tehnologij intellektualizacii // Ohrana, bezopasnost', svjaz'. 2023, № 8-1, s. 155–159.*
78. *Kostogryzov A. I. Podhod k verojatnostnomu prognozirovaniju zashhishhennosti reputacii politicheskih dejatelej ot «fejkovyh» ugroz v publichnom informacionnom prostranstve // Voprosy kiberbezopasnosti. 2023, № 3 (55), s. 114–133*
79. *Avetisjan A. I. Ispol'zovanie doverennogo PO pri sozdanii sistem iskusstvennogo intellekta kak osnova bezopasnosti (doklad) // XXVII nauchno-prakticheskaja konferencija «Kompleksnaja zashhita informacii», 24–26 maja 2022 goda, Moskovskaja oblast'.*
80. *Garbuk S. V. Zadachi normativno-tehnicheskogo regulirovanija intellektual'nyh sistem informacionnoj bezopasnosti // Voprosy kiberbezopasnosti. 2021, № 3 (43), s. 68–83.*

ПРОГНОЗИРОВАНИЕ РАЗМЕРА ИСХОДНОГО КОДА БИНАРНОЙ ПРОГРАММЫ В ИНТЕРЕСАХ ЕЕ ИНТЕЛЛЕКТУАЛЬНОГО РЕВЕРС-ИНЖИНИРИНГА

Израилов К. Е.[1]

DOI: 10.21681/2311-3456-2024-4-13-25

Цель исследования: *повышение эффективности поиска уязвимостей в машинном коде программ путем его реверс-инжиниринга на базе генетических алгоритмов, для чего решается частная задача прогнозирования размера исходного кода на языке программирования С по его скомпилированной версии.*

Методы исследования: *обзор работ, системный анализ, синтез метода, компьютерное моделирование, эксперимент.*

Полученные результаты: *создан метод получения зависимости размера исходного кода (выраженного в токенах языка программирования) от соответствующего ему машинного кода, что позволяет решать частную задачу определения длины хромосомы особи в рамках реверс-инжиниринга на базе генетических алгоритмов; разработан программный прототип, реализующий указанный метод, с помощью которого проведен эксперимент (с использованием датасета ExeBench, содержащего около 200 тысяч функций на языке программирования С), позволивший вывести аналитическую зависимость между размерами исходного и машинного кодов.*

Научная новизна *заключается как в общем развитии нового интеллектуального направления реверс-инжиниринга машинного кода, так и в авторском решении частной задачи прогнозирования размера исходного кода программы по ее бинарному представлению.*

Ключевые слова: *реинжиниринг, обратная разработка, обратный инжиниринг, генетический алгоритм, уязвимость, машинный код, метод, прототип, эксперимент, аналитическая зависимость.*

PREDICTING THE SIZE OF THE SOURCE CODE OF A BINARY PROGRAM IN THE INTERESTS OF ITS INTELLECTUAL REVERSE ENGINEERING

Izrailov K. E.[2]

The goal of the investigation: *increasing the efficiency of searching for vulnerabilities in machine code of programs by reverse engineering it based on genetic algorithms, for which the particular problem of predicting the size of source code in the C programming language from its compiled version is solved.*

Research methods: *works survey, system analysis, synthesis, computer modeling, experiment.*

Result: *a method has been created for obtaining the dependence of the size of the source code (expressed in programming language tokens) on the corresponding machine code, which allows solving the particular problem of determining the length of an individual's chromosome within the framework of reverse engineering based on genetic algorithms; a software prototype was developed that implements the specified method, with the help of which an experiment was carried out (using the ExeBench dataset containing about 200 thousand functions in the C programming language), which made it possible to derive an analytical relationship between the sizes of the source and machine codes.*

The scientific novelty *consists both in the general development of a new intellectual direction of reverse engineering of machine code, and in the author's solution to the particular problem of predicting the size of a program's source code from its binary representation.*

Keywords: *reengineering, reverse engineering, genetic algorithm, vulnerability, machine code, method, prototype, experiment, analytical dependence.*

1 Израилов Константин Евгеньевич, кандидат технических наук, доцент, старший научный сотрудник лаборатории проблем компьютерной безопасности Санкт-Петербургского Федерального исследовательского центра Российской академии наук, Санкт-Петербург, ORCHID: http://orcid.org/0000-0002-9412-5693. Scopus Author ID: 56122749800. E-mail: konstantin.izrailov@mail.ru

2 Konstantin E. Izrailov, Ph.D., Docent, Senior Researcher of Laboratory of Computer Security Problems of St. Petersburg Federal Research Center of the Russian Academy of Sciences, Saint-Petersburg. ORCHID: http://orcid.org/0000-0002-9412-5693. Scopus Author ID: 56123238800. E-mail: konstantin.izrailov@mail.ru

Введение

Безопасность программного обеспечения (далее – ПО) является актуальнейшей проблемой современного IT-мира [1]. Одним из путей ее разрешения считается анализ конечного продукта (т.е. программы) на предмет наличия уязвимостей, за которым следует их нейтрализация. При этом, если обнаружение достаточно тривиальных уязвимостей и возможно с помощью автоматических средств, то в случае сложных алгоритмических или архитектурных уязвимостей требуется привлечение экспертов по безопасности программного кода. И если при разработке программ на интерпретируемых языках программирования и/или компилируемых в байт-код (например, на Python или Java) эксперту может потребоваться изучение хорошо понятного исходного кода (далее – ИК), то для ряда популярных языков программирования (например, C и C++) программа имеет бинарный вид, содержащий машинный код (далее – МК), ручной анализ которого будет иметь сверхвысокую трудоемкость. Ситуация усугубляется тем, что «заложение» уязвимостей в код злоумышленником производится сознательно с применением механизмов усложнения их обнаружения – в том числе, через запутывание алгоритмов и ослабление архитектуры программного продукта.

Вышесказанное указывает на наличие в предметной области проблемного вопроса, как противопоставления следующих потребностей и возможностей. Во-первых, существующие методы и средства имеют высокую эффективность лишь для тривиальных уязвимостей или при наличии псевдо-исходного кода (приставка «псевдо» отражает тот факт, что код не будет в точности соответствовать исходному, он обязан лишь быть синтаксически корректным и компилироваться в анализируемый машинный). С другой стороны, для огромного количества областей IT-мира программы представляют собой машинный код, поиск нетривиальных уязвимостей в котором с применением экспертных методов имеют недопустимо высокую трудоемкость.

Одним из существующих подходов к поиску уязвимостей (в особенности обладающих средним и высоким уровнем внедрения) в машинном коде является его предварительное преобразование в человеко-ориентированную форму путем декомпиляции [2, 3] – т.е. получения соответствующего псевдо-исходного кода (а потенциально – программных алгоритмов и архитектуры). Однако, существующие средства декомпиляции (например, продукт IDA Pro [4] с плагином Hex-Rays и Ghidra [5]) используют встроенные сложные алгоритмы преобразования конструкций МК и их комбинаций в подобные элементы в ИК. Богатый авторский опыт работы в области реверс-инжиниринга [6–8] позволяет утверждать, что такие средства зачастую вызывают программные исключения, восстанавливают не компилируемый или неполный код, или же конечный результат слабо подходит для ручной обработки. Альтернативным подходом, развиваемым автором, является «генетический реверс-инжиниринг машинного кода» (далее – ГРИМК), основанный на применении искусственного интеллекта в части использования генетических алгоритмов для осуществления декомпиляции. Суть ГРИМК заключается в решении оптимизационной задачи подбора вариантов ИК, наиболее близких к МК после компиляции, декомпиляцию которого необходимо произвести; выбор архитектуры CPU и компилятора считается частично решенной задачей [9]. Результатом применения ГРИМК является не просто псевдо-исходный код, лишь отражающий логику ПО, а код реального языка программирования, гарантированно компилируемый в исследуемый МК. Такой ИК может быть проанализирован экспертом на предмет наличия в нем уязвимостей, модифицирован и скомпилирован в безопасный МК.

Принцип работы авторского подхода ГРИМК состоит в итеративном подборе такого варианта ИК, который бы компилировался в заданный МК. Для этого применяется «умный» перебор элементов языка программирования, из которых составляется ИК, сравниваемый после компиляции с исследуемым МК; с этой позиции, ГРИМК может быть отнесет к области генетического программирования, предназначенного для генерации или изменения программ, решающих некоторую вычислительную задачу [10]. Как следствие, одной из задач (возможно косвенной, но тем не менее, принципиально важной) в данном подходе является определение размера ИК. В ином случае пришлось бы подбирать не только элементы последовательности, но и ее размер, что не только качественно усложнит реализацию подхода, но и теоретически сделает задачу нерешаемой (поскольку, размер исходного кода может увеличиваться практически до бесконечности). Естественно, целесообразно составлять ИК не из отдельных символов, а из конструкций его языка программирования (для языка C/C++ это будут заголовки функций [11] и переменные [12], элементы границ блоков «{» и «}», операторы «+» или «–», операторы «if» или «else» и т.п.).

Таким образом, задачу текущего исследования можно сформулировать следующим образом:

«Создание метода и программного средства прогнозирования размера исходного кода по скомпилированному из него машинному коду».

Детали постановки и решения задачи будут раскрыты в статье далее, ее же актуальность обосновывается отсутствуем каких-либо подходящих методов или средства из числа существующих. Необходимо отметить, что данное исследование является продолжением предыдущего (а в частности – развитием, исправлением недочетов и адаптацией для российского научного сегмента), результаты которого были апробированы в 2024 году на международной научно-практической конференции «Индустрия 4.0» (https://smartindustrycon.ru/), публикующей труды в цифровой библиотеке «IEEE Xplore».

Проведем обзор работ, близких к задаче исследования – определению зависимости между размерами ИК и МК; в случае отсутствия подходящих публикаций рассмотрим более общие, затрагивающие вопрос определения длины хромосомы в генетических алгоритмах, а также ее представления.

В исследовании [13] приводится метод преобразования МК в алгоритмы без необходимости восстановления ИК. Приложением метода указывается обнаружение вредоносного кода, в особенности, ИК которого был сознательно «запутан». Метод в своей работе использует графы потоков управления для представления программы в виде алгоритмов.

Авторы работы [14] описывают средство BinDeep, предназначенное для сопоставления фрагментов ИК с аналогичными по функционалу фрагментами в МК. В качестве практической значимости решения указывается поиск клонов кода, и, в частности, содержащего вредоносный код.

В работе [15] для декомпиляции фрагментов МК применяется рекуррентная нейронная сеть. В качестве особенности предложенного подхода указывается его независимость от языка программирования. В основе модели нейронной сети заложено ее обучение на шаблонах ИК. Применяться решение может для ручного анализа ПО в случае, когда его ИК отсутствует.

Исследование [16] также посвящено декомпляции, но в части восстановления встроенных в МК функций, оптимизированных в процессе компиляции из ИК. Авторский метод построен на основе машинного обучения с учителем и может быть объединен с продуктом Ghidra. Применением метода является анализ ПО, соответствующего МК, для обнаружения вредоносного кода и определения факта хищения интеллектуальной собственности.

Работа [17] посвящена прогнозированию размера ИК кода, однако не по МК, а согласно конкретному процессу программной инженерии. Для этого предлагается метод из 6 шагов, учитывающих следующие особенности ПО: нескорректированные веса субъектов и вариантов использования, нескорректированные варианты использования, техническая сложность и факторы окружающей среды, скорректированные варианты использования, трудозатраты в человеко-часах. Таким образом, имеется возможность формального предсказания размера ИК крупных проектов.

В работе [18] представлена модель COCOMO II, предназначенная для оценки размера исходного кода программных средств. При этом расчет размера производится как с учетом нового разработанного кода, так и повторно используемого, а также модифицированного для адаптации. Аналитическая модель основана на 8 компонентах, для каждого из которых приводятся методики расчета. В качестве назначения модели указана оценка трудоемкости и длительность разработки программных продуктов.

В исследовании [19] производится общее сравнение генетических алгоритмов и генетического программирования, указывая, что в отличие от первых, последние имеют переменную длину хромосом, структура которых, как правило, является не строкой, а деревом.

Авторы в [20] описывают применение кода Грея для кодирования целочисленных признаков в результате чего хромосома в генетическом алгоритме имеет представление последовательности бит; длина же хромосомы, соответственно, определяется максимальным кодируемым числом. Одним из результатов такого способа кодирования является то, что изменение одного бита в результате мутации приведет к замене закодированного с помощью хромосомы числа на смежное – т.е. к небольшому изменению особи, что является достаточно важной особенностью работы генетического алгоритма.

В работе [21] исследуется влияние различных параметров генетических алгоритмов на его работу при решении задачи о рюкзаке (укладывание ценных вещей при ограничении его вместимости), а именно следующих: число вычислений целевой функции, тип селекции и скрещивания, а также вероятность мутации и опциональное добавление в новое поколение лучшего индивидуума предыдущего. При этом длина и представление хромосомы никак не рассматривались.

Исследование [22] посвящено решению задачи покрытия территории группой беспилотных летательных аппаратов (далее – БПЛА) с помощью генетического алгоритма. Для этого, в качестве возможных представлений хромосомы указывается как последовательность точек, которые необходимо посетить одному БПЛА, так и аналогичное объединение траекторий для нескольких БПЛА. Таким образом, длина хромосомы должна определяться минимально-

необходимым количеством точек траектории для покрытия всей заданной территории (чему в работе внимания не уделяется).

Краткий обзор работ показал практически полное отсутствие решений (под которым здесь понимаются методы и их программные реализации), применимых к задаче текущего исследования.

Генетический реверс-инжиниринг

Опишем далее общую идею авторского генетического реверс-инжиниринга, уделив особое внимание используемой терминологии и постановке задачи исследования.

Идея

Классический подход к декомпиляции может быть назван обратным (или реверс) инжинирингом, поскольку он согласно жизненному циклу ПО [23] осуществляет преобразование от текущего представления (т.е. МК или аналогичного ему ассемблерного кода) к предыдущему (т.е. ИК). При этом, как указывалось, могут применяться как автоматические средства, так и ручной труд эксперта. Предлагаемый же автором подход ГРИМК с этой точки зрения может быть назван «псевдо-прямым», поскольку он стремится подобрать такое представление ИК, которое бы при компиляции преобразовывалось в исследуемый МК. Таким образом, ГРИМК решает оптимизационную задачу [24], в которой параметром является последовательность конструкций ИК (символов, токенов, узлов абстрактного синтаксиса, шаблонов или иных сущностей), которые бы при компиляции получали МК, наиболее близкий к необходимому (в идеале – к оригиналу). Получение идентичных МК означает решение оптимизационной задачи и обнаружение ИК – т.е. достижение глобального экстремума. В этом аспекте, ГРИМК схож с ручной декомпиляцией, поскольку эксперт точно также подбирает такие конструкции ИК, последовательность которых бы в точности соответствовала анализируемому машинному. Данный процесс (для эксперта) усложняется тем, что неверный выбор конструкций в начале ИК может повлиять на невозможность подбора корректных конструкций в дальнейшем. Для обоснования этого приведем пример процесса реверс-инжиниринга тривиального МК (использованы следующие условные инструкции: MOV – операция сохранения значения второго аргумента в первом, CALL – вызов функции с аргументом в регистре AX и возвратом результата в том же регистре; здесь и далее префикс из числа и двоеточия соответствует порядковому номеру строки)

```
1: MOV AX, x
2: CALL funct
3: MOV y, AX
```

полученного из ИК:

```
y = funct(x);
```

В случае прямого преобразования инструкций МК (т.е. без возвратов и изменений в уже сформированном коде) в конструкции ИК строки 1 и 2 позволят получить следующий код:

```
funct(x)
```

Однако, строка 3 интерпретируется, как сохранение результата «funct()» в переменной «y», что потребует добавления соответствующего оператора присваивания перед функцией:

```
y = funct(x)
```

В случае последовательного преобразования такое изменение будет невозможно, поскольку ИК для вызова функций уже сформирован.

Прямой перебор

Отметим, что теоретически, задача получения ИК по соответствующему ему МК могла бы быть решена полным перебором всех конструкций ИК; тем не менее, на практике такой способ не применим, поскольку данный процесс будет недопустимо длительным. Приведем очень грубые примеры оценки такого процесса для ИК на языке программирования С, учитывая следующие ограничения и условия:

- символы текста ИК состоят из комбинации букв английского алфавита, цифр, знаков и пробелов;
- каждый символ может принимать одно из 50 значений;
- в случае рассмотрения ИК, как последовательности лексем синтаксиса языка программирования (идентификаторов, ключевых слов, операторов, цифр и специальных символов), их количество считается равным примерно 100;
- используется понятное эксперту деление текста ИК на строки (в конце логических конструкций);
- размер текста является условно минимальным за счет применения коротких имен переменных и функций, а также оптимизации количества пробелов, используемых конструкций, операторов и т.п.;
- приблизительное время компиляции одного ИК (с учетом длительности запуска процесса, загрузки исходного файла и сохранения ассемблерного) занимает 1 секунду;
- при переборе вариантов ИК не учитывается синтаксис языка программирования и, следовательно, даже изначально некорректная комбинация символов считается потенциально компилируемой в исследуемый МК (а не отбрасывается, что было бы более логичным).

Пример 1. ИК состоит из базового сложения двух переменных (без завершающего «;») и является следующим:

```
1: x+y
```

и содержит 3 символа (без учета перевода строки). Таким образом, для подбора такого ИК даже с учетом знаний о его длине максимально потребуется перебрать $50^3 = 125000 \approx 10^5$ вариантов комбинаций символов, компиляция которых суммарно займет ~35 часов.

Если рассматривать ИК, как последовательность лексем длиной 3, количество вариантов будет равно $100^3 = 10^6$, компиляция которых займет ~350 часов.

Пример 2. ИК состоит из «функции-заглушки», возвращающей число 0, является следующим:

```
1: int f()
2: {
3:  return 0;
4: }
```

и содержит 23 символа (с учетом одного на каждый перевод строки). Таким образом, поиск ИК максимально потребует перебрать $50^{23} \approx 10^{39}$ вариантов комбинаций символов, время компиляции которых уже будет сверхвысоким (отметим, что как считается, время жизни Вселенной не превосходит 10^{18} секунд).

Если рассматривать ИК, как последовательность лексем длиной 9 («int», «f», «(», «)», «{» и т.п.), количество вариантов будет равно $100^9 = 10^{18}$, компиляция которых также займет сверхвысокое время (хотя и на 20 порядков меньшее, чем при представлении ИК, как последовательности символов).

Пример 3. ИК состоит из реальной функции определения максимального из двух чисел:

```
1: int f(int x, int y)
2: {
3:  if(x > y)
4:   return x;
5:  else
6:   return y;
7: }
```

и содержит 66 символов (с учетом переводов строк). Таким образом, поиск ИК максимально потребует перебрать $50^{66} \approx 10^{112}$ вариантов комбинаций символов, что скорее всего недостижимо даже теоретически.

Если рассматривать ИК, как последовательность лексем длиной 24 («int», «f», «(», «int», «x» , «,», «int» , «y», «)», «{» и т.п.), количество вариантов будет равно $100^{24} = 10^{48}$, что хотя на 64 порядка и меньшее, чем при представлении ИК в виде последовательности символов, однако также недостижимо высоко.

Таким образом, решение задачи реверс-инжиниринга путем прямого перебора символов или лексем для поиска ИК, компилируемого в заданный МК, является нецелесообразным даже для небольших выражений.

Однако, решение такого рода задач может оказаться возможным применением различных методов оптимизаций, например, с помощью генетических алгоритмов [25]. Основная предпосылка такого выбора заключается в схожести принципов его работы и процесса ручного восстановления ИК экспертом.

Суть генетических алгоритмов заключается в создании популяции особей, особенности которых (структура, параметры, свойства и т.п.) задаются хромосомой, состоящей их набора генов.

На первом этапе генетического алгоритма создается начальная популяция особей, гены которых могут быть заданы случайным образом. Таким образом, после этого этапа будет сгенерировано множество случайных особей.

На втором этапе происходит селекция (т.е. отбор) особей, наиболее адаптированных к окружающей среде с применением так называемой Функции приспособленности. Данная функция в численном виде определяет «живучесть» каждой особи, что позволяет отобрать наиболее удачных из них. Таким образом, после этого этапа популяция состоит из ее «лучших» (с позиции Функции приспособленности) представителей. При этом очевидно, что приспособленность особей определяется именно их генами. Если для какой-либо особи Функция приспособленности оказывается равной заданному значению (например, максимально возможному) то задача считается решенной, а алгоритм завершается.

На третьем этапе происходит скрещивание особей, заключающееся в перемешивании их ген и получении других особей (для пополнения популяции, уменьшенной на втором этапе). Таким образом, после этого этапа новые особи обладают генами от лучших представителей популяции.

На четвертом этапе происходит мутация отдельных генов, что вносит некоторый «шум» в хромосомы особи и, как следствие, их в приспособленность. Этот этап необходим для выхода из локальных экстремумов при решении оптимизационной задачи [26].

Затем, выполнение повторяется со второго этапа.

Терминология

Приведем соответствие терминов генетических алгоритмов и ассоциированных с ним понятий ГРИМК:

1) Особь – некоторый вариант текста ИК на языке программирования С, который подвергается компиляции в МК (например, «x + y;», поскольку для сокращения записи далее в примерах заголовок функции будем опускать);
2) Популяция (особей) – множество вариантов ИК, сформированных в процессе работы генетического алгоритма (например, «x + y;», «x + z;» и «y + z;»);
3) Хромосома (особи) – последовательность конструкций ИК, а именно, токенов языка программирования (например, «x», «+», «y» и «;»);

4) Ген (хромосомы) – конструкция ИК в определенной позиции, составляющая всю хромосому (например, «x» в позиции 1, «+» в позиции 2, «y» в позиции 3 и «;» в позиции 4);
5) Селекция – отбор экземпляров ИК, компилируемых в МК, наиболее близкий к исследуемому (например, если МК получен из ИК – «x+y;», то из экземпляров «x+z» и «1*2» будет селектирован первый);
6) Скрещивание – перемешивание конструкций двух экземпляров ИК с получением нового экземпляра ИК (например, в результате скрещивания родителей «x+b» и «a+y» может быть получен потомок «x+y»);
7) Мутация – случайное изменение конструкции экземпляра ИК в виде замены одного токена на другой (например, экземпляр «x-y» с некоторой вероятностью может быть мутирован в «x+y»);
8) Функция приспособленности – функция, вычисляющая близость двух МК – исследуемого и полученного компиляцией из некоторой особи или экземпляра ИК (например, если искомым ИК является «x+y», то МК для «x+z» будет считаться лучше приспособленным или близким к анализируемому, чем МК для «1*2»);
9) Размер хромосомы – длина ИК в выбранных конструкциях, т.е. количество составляющих его токенов (например, для «x + y;» это будет 4).

В качестве конструкций ИК (т.е. генов хромосомы особи) выбраны токены языка программирования C, поскольку, следуя примерам ИК разбиение его на символы является крайне нецелесообразным, а использование более сложных конструкций, таких, как деревья абстрактного синтаксиса и/или ссылки на элементы формального синтаксиса языка программирования требует дополнительных исследований.

В указанных терминах алгоритм работы ГРИМК заключается в следующем. Во-первых, создается множество случайных экземпляров ИК. Во-вторых, все экземпляры ИК компилируются в некоторые МК. В-третьих, с помощью Функции приспособленности оценивается близость их МК и исследуемого, а затем отбираются наиболее близкие к искомому ИК. Если получен ИК, в точности компилируемый в нужный МК, то задача считается решенной. В-пятых, создаются новые экземпляры ИК из токенов старых. В-шестых, некоторые токены в ИК меняются на случайные. И, в-седьмых, процесс повторяется с момента компиляции множества ИК.

Также под токенами понимаются отдельные элементы языка, такие, как ключевые слова, переменные и пр. Так, функция нахождения суммы двух чисел со следующим ИК (из 43 символов):

```
int sum (int x, int y)
{
  return x + y;
}
```

состоит из последовательности 16 токенов – «int», «sum», «(», «int», «x», «,», «int», «y», «)», «{», «return», «x», «+», «y», «;», «}».

Задача исследования

Исходя из идеи ГРИМК, важным вопросом остается выбор длины хромосомы – т.е. длины экземпляра ИК. Несмотря на существование генетических алгоритмов с хромосомами переменной длины [27], одним из решений данного вопроса может быть предсказание размера ИК в токенах на основании размера экземпляра МК. Измерение длины в токенах более предпочтительно, поскольку оно не учитывает длину имен переменных и функций, которые, по сути, никак не влияют на логику работы программы, а используются лишь для лучшего понимания ИК разработчиком.

Отметим, что получение размера может быть использовано и в случае кодирования хромосомы, как последовательности не только символов или токенов, но и элементов формального синтаксиса языка программирования. Так, например, если рассмотрение текста ИК ограничивается тремя идентификаторами («x», «y» и «z»), а также четырьмя основными арифметическими операциями над их парами («+», «-», «*» и «/»), то формальный синтаксис такого ИК (как совокупность синтаксических правил языка программирования) имеет следующий вид:

```
1   : expression ::=
1.1:    identifier |
1.2:   identifier operator identifier ;

2   : identifier ::=
2.1: 'x' |
2.2: 'y' |
2.3: 'z' ;

3   : operator ::=
3.1: '+' |
3.2: '-' |
3.3: '*' |
3.4: '/' ;
```

И хотя синтаксис для любого разработчика компиляторов является интуитивно понятным, тем не менее, дадим ряд пояснений. Во-первых, идентификаторы («x», «y» и «z») и операторы («+», «-», «*» и «/») являются терминальными символами, поскольку имеют конкретное значение и не могут «раскрываться» через другие символы. Во-вторых, «expression», «identifier» и «operator» являются нетерминальными символами, значения которых заранее

неизвестны, поскольку состоят из комбинации других метапеременных или символов; они определяются через операцию «::=». В-третьих, нетерминальные символы определяются как один из вариантов последовательности других терминальных и нетерминальных символов, задаваемых через операцию альтернативы «|». Префикс для каждой строки (как и ранее, до символа «:») соответствует идентификатору правила, которые как раз могут соответствовать генам особи, определяющим ИК.

Согласно синтаксису, ИК может состоять или из единичных идентификаторов (т.е. «x», «y» и «z») или из комбинаций операций между ними (т.е. «x+x» … «x/z» … «z+x» … «z/z»). Тогда, каждый ИК через хромосому переменной длины можно кодировать последовательностью правил формального синтаксиса, задаваемых соответствующими идентификаторами. Так, ИК «y» соответствует хромосоме [1.1, 2.2], «x+y» – хромосоме [1.2, 2.1, 3.1, 2.2], а «y*z» – хромосоме [1.2, 2.2, 3.3, 2.3]; здесь, «[…]» означает последовательность генов, каждый из которых определяет путь по правилам формального синтаксиса.

Необходимо отметить, что в случае приведенного выше кодирования ИК (т.е. через путь по правилам синтаксиса) задача полного перебора может решаться еще за меньшее количество вариаций (за исключением Примера 1 со сложением двух переменных – там общее число всех вариантов будет таким же).

Несмотря на некоторое количество вариантов представления хромосомы для ИК, далее будет рассмотрено получение зависимости от МК именно количество токенов, поскольку оно, с точки зрения автора, будет иметь теоретическую и практическую значимость не только в рамках ГРИМК, но и для других подобного рода задач.

Метод и прототип

Для получения зависимости размера ИК в токенах от размера МК в байтах был разработан следующий метод (далее – Метод). Его суть заключается в сборе большого количества ИК функций на языке программирования C, их компиляции в МК, вычислении размеров обоих, сборе статистики касательно соответствия этих размеров и определении итоговой зависимости. Данный язык программирования был выбран исходя из его большой популярности для разработки ПО в различных сферах, а также общей сложности проведения реверс-инжиниринга для разработанных на нем программ. Также в качестве компилятора был взят входящий в состав продукта Microsoft Visual Studio Community 2019 (далее – MSVS2019).

Необходимое множество разнообразных функций на языке C было взято из проекта ExeBench, который как раз и ориентирован на предоставление датасета в интересах машинного обучения [28]. Необходимо отметить большую и качественно проведенную работу участниками данного проекта, за что автор текущей статьи им безусловно благодарен.

Далее приведем описание шагов предлагаемого Метода.

Шаг 1. Загрузка dataset с C-функциями

Происходит загрузка структур с метаинформацией в формате JSON, содержащих функции на языке программирования C, предоставляемых в рамках проекта ExeBench.

Шаг 2. Выделение ИК C-функций

Из загруженных JSON-структур выделяется ИК C-функций с назначением им уникальных имен, которые добавляются в единое внутреннее хранилище. Данные имена используются в отладочных целях для однозначной идентификации функций.

Шаг 3. Предобработка ИК C-функций

Производится предобработка ИК C-функций следующим образом:

- удаляются ключевые слова «inline» и «__inline__» перед сигнатурой функции, поскольку в ином случае компилятором не будет сгенерирован МК (исходя из назначения ключевых слов);
- удаляется ключевое слово «static» перед сигнатурой функции, поскольку в ином случае также не будет сгенерирован МК(исходя из назначения ключевого слова);
- делается замена «NULL» на «((void *)0)», поскольку данный макрос не является встроенным в синтаксис компилятора;
- удаляются фрагменты ИК «__attribute__((…))», поскольку они не являются стандартными для языка C и не поддерживаются многими компиляторами;
- удаляются функции с ИК, содержащим ассемблерные вставки (определяемые ключевым словом «__asm__»), поскольку требуется найти зависимость только между ИК и МК;
- опционально, исключаются заданные C-функции (в том случае, если они на основании экспертного анализа ИК признаны аномальными);
- опционально, исключаются функции с ИК, содержащим работы с типами с плавающей точкой («double» и «float»);
- опционально, исключаются функции с ИК, содержащим инициализацию сложных переменных (массивов и строк) в теле функции;
- опционально, исключаются функции с ИК, содержащим работы с дробными числами (например, «10.2»).

Необходимость в последних четырех опциональных действиях шага связана с тем, что C-код в ряде

случаев генерирует аномально большой МК, что негативно повлияет на формулу прогнозирования размера ИК; для этого, такой код изначально исключается из обработки Методом.

Шаг 4. Компиляция ИК С-функций

ИК каждой функции копируется в С-файл («filename.c»), который компилируется (утилитой «cl.exe») без оптимизации (ключ «/Od») с получением только объектных файлов (ключ «/c»), содержащих МК (ключ «/Fo»); для отладочных целей генерируется и ассемблерный файл (ключ «/Fa»). Итоговой строкой компиляции является следующая: «cl.exe filename.c /c /Od /Fafilename.asm /Fofilename.obj». Зависимость между ИК и МК для других ключей компилятора (например, включающих оптимизацию по размеру или скорости) также является интересной научно-практической задачей, но будет рассмотрена в дальнейших исследованиях.

Шаг 5. Вычисление размера ИК (в токенах)

Производится разбиение текста ИК на отдельные языковые токены, измерение в которых длины текста является более корректным (или целесообразным), поскольку устраняет влияние размеров пользовательских названий (имен функций, переменных, типов), которые никак не отражаются на логике работы программы. Так, например, два ИК с текстами «void f() {}» и «void f1234567890() {}» содержат 11 и 21 символ соответственно, хотя фактически, они абсолютно идентично описывают пустую функцию; количество же токенов для этих ИК одинаково и равняется шести.

Шаг 6. Вычисление размеров МК

Производится вычисление размера кода в машинном (бинарном) представлении, для чего используется объектный файл с МК, сгенерированный в результате компиляции. Поскольку объектный файл помимо самих инструкций CPU содержит и другую информацию (что определяется заголовком файла), то его необходимо «распарсить», выделить секцию с кодом и получить ее размер.

Все полученные размеры (ИК и МК) заносятся во внутреннее хранилище. В случае ошибки, ее текст также сохраняется, а функция помечается как некомпилируемая. Затем, для каждого размера МК вычисляется минимальное, максимальное и среднее значение размера соответствующего ему ИК; дополнительно, в хранилище сохраняется количество элементов этих списков.

Шаг 7. Вывод таблицы зависимости

Производится вывод зависимости размеров МК и соответствующих им количества токенов (минимального, максимального, среднего) в ИК в табличном виде для последующей визуализации. В Методе такая таблица предназначена для загрузки в Microsoft Excel для полу-автоматического анализа.

Шаг 8. Определение формулы зависимости

Производится определение формулы зависимости между размерами ИК (в токенах) и МК. Для этого в Методе используется инструментарий, встроенный в Microsoft Excel, в части построения трендов по предопределенному закону (в настройках точечных диаграмм).

Реализация

Метод был реализован в виде программного прототипа (далее – Прототип), выполняющего все шаги, кроме 8-го. Для разработки Прототипа использовался язык программирования Python 3.10, а также следующие библиотеки: json – для работы с файлами в JSON формате (т.е. содержащих С-функции), subprocess – для запуска внешних процессов (т.е. утилиты «cl.exe»); nltk – для разделения текста ИК функции на список токенов; coff – для парсинга получаемых объектных файлов формата The Common Object File Format (сокр. COFF) и выделения в них секций с МК; signal – для перехвата нажатия «Ctrl+C» с целью пользовательского завершения работы.

Прототип в автоматическом режиме сканирует заданную директорию на предмет наличия JSON-файлов с С-функциями, позволяет загружать и обновлять внутреннее хранилище функциями из новых JSON-файлов, делает промежуточные сохранения внутреннего хранилища во внешний файл, управляет пропуском С-функций с аномальными размерами, а также выводит лог своей работы на консоль.

Эксперимент

Опишем далее эксперимент, проведенный с применением Метода и, соответственно, Прототипа.

Исходные данные и параметры

В эксперименте были взяты следующие исходные данные и параметры:

- датасет с С-функциями скачивался по Интернет-адресу https://huggingface.co/datasets/jordiae/exebench/tree/main (размер отобранных файлов составил 12.5 Гб);
- С-функции с типами с плавающей точкой, дробными числами и инициализацией сложных переменных исключались;
- экспертно было исключено 18 функций с аномально длинным ИК, который не приводил к генерации МК соизмеримого размера; функции имели следующее содержание: конкатенацию большого числа символов и текстовых строк, применение неиспользуемых макросов, создание длинных строк, оперирование сложными выражениями, длинные комментарии;
- для расчета зависимости брался МК размером не более 300 байт, поскольку для большего размера соответствующих экземпляров С-функций было

менее 10, что можно считать недостаточным для получения корректной статистике;
- количество токенов ИК считалось, как усредненное значение множества всех ИК (для определённого размера МК);
- для определения формулы зависимости размера ИК (в токенах) от размера МК использовался степенной тренд (согласно терминологии Microsoft Excel).

Также для ускорения работы Прототипа при обработке большого количества метаинформации и функций из ExeBench, все данные (как исходные, так промежуточные и конечные) располагались на виртуальном диске в памяти (размером 16 Гб).

Ход выполнения

Лог работы Прототипа при проведении Эксперимента представлен ниже; пометкой «...» отмечены строки, аналогичные предыдущей (см. схему 1).

Следуя логу, процесс работы Прототипа занял 1 часа 33 минут и 25 секунд. При этом было загружено 219077 С-функций, из которых для компиляции было подготовлено 200037 экземпляров. Из всех С-функций было успешно скомпилировано 82451 экземпляров, а 117587 привели к различным ошибкам. Таким образом, для построения зависимости было получено примерно 82.5 тысяч соотношений количества токенов в ИК и соответствующих им размеров МК.

Результаты

В результате применения Прототипа и отбора ИК с размером не более 300 токенов для построения зависимости было использовано 80787 экземпляров, что составляет 80787 / 82451 = 98.0% от их общего количества и представляет собой достаточно репрезентативную для оценки выборку.

При формировании непосредственной зависимости размера ИК от МК было учтено, что объектные файлы (с расширением «*.obj») после компиляции С-функций в MSVS2019 имели формат COFF, а их инструкции для CPU содержались в секциях со служебным названием «.text$mn». Таким образом, вычисляемый размер МК существенно отличался от размера самого объектного файла.

Полученный график зависимости размера МК от ИК (с линейным трендом) представлен на Рисунке 1; используются следующие обозначения графиков: «Мин.» – минимальное количество токенов, «Макс.» – максимальное количество токенов, «Сред.» – усредненное количество токенов, «Линейная (Сред.)» – линейный тренд для усредненного количества токенов, полученный с помощью встроенного инструментария Microsoft Excel (его формула и погрешность указаны в верхней правой части графика).

Таким образом, формула зависимости размера ИК в токенах (SCT_{Size}) от размера МК (MC_{Size}) имеет следующий усредненный вид (см. правую верхнюю часть Рисунка 1):

$$SCT_{Size} = 0.6057 \times MC_{Size} + 9.8242,$$

при этом достоверность аппроксимации составляет достаточно высокое значение – $R^2 = 0.9543$.

Схема 1

```
(2024.06.09 17:05:03) Loading dataset from 'Dataset\real_test\data_0_
time1678114487_default.jsonl' ... OK (2132 items, {'WithRealError': 2})
...
(2024.06.09 17:07:13) Loading dataset from ' Dataset\train_synth_simple_io\
data_0_time'1677914260_default.jsonl' ... OK (4786 items, {'WithRealError':
5214})
(2024.06.09 17:07:18) Dataset preparing (219077) ... OK ({'Skip with asm': 478,
'Skip with double/float type': 13569, 'Skip with array init': 2438, 'Skip by
position': 18, 'Skip with fractional number': 2536})
(2024.06.09 17:07:26) Dataset compiling (200038 items) ...
(2024.06.09 17:07:26)   0) Compile function '[data_0_time1678114487_default:0]
num2str()' ... Succeeded
...
(2024.06.09 18:38:25)     200037) Compile function '[data_0_time1677914260_
default:9993] icosd()' ... Succeeded
(2024.06.09 18:38:25)     200038) Compile function '[data_0_time1677914260_
default:9996] get_current_frame()' ... Failed
(2024.01.24 22:39:55)   Saving to 'a_dataset_3.json' ... OK
(2024.06.09 18:38:28) ... OK ({'All': 200038, 'Skipped': 0, 'Compiled': 200038,
'Succeeded': 82451, 'Failed': 117587})
```

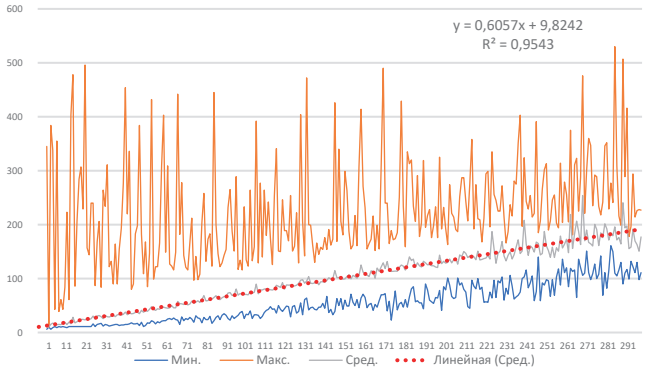


Рис. 1. Зависимость размера МК (в байтах) от размера ИК (в токенах)

Ограничения результатов

Приведем далее основные ограничения Метода и Прототипа, а также их обоснование и пути устранения.

В качестве источника ИК для С-функций выбран определенный датасет (т.е. ExeBench) по следующим причинам. Во-первых, подобных датасетов, содержащих отдельные функции, которые могут компилироваться без программного окружения (например, заголовочных файлов, включаемых с помощью препроцессорной директивы «#include») достаточно мало. Например, если взять любой крупный проект с множеством функций, то хотя он и будет компилируемым целиком, но отдельные функции будут «тянуть» за собой другие, в том числе библиотечные. Во-вторых, датасет ExeBench уже имеет достаточно хорошую структуру, поскольку состоит из JSON-файлов с ИК функциями, ассемблерным кодом под ряд компиляторов (кроме используемого в составе MSVS2019), ошибками компиляции и дополнительной метаинформацей. И, в-третьих, С-функции датасета не относятся к какой-либо определенной области ПО, а являются усредненными для программной инженерии.

Исходно, в датасете ExeBench был приведен ассемблерный код, полученный компиляторами GCC с различными оптимизациями и для ряда CPU (например, x86 и ARM), по которому можно было бы сгенерировать и соответствующие объектные файлы. Тем не менее, компилятор в составе MSVS2019 является полноценным средством получения МК [29]. При этом, теоретически, размеры ИК на одном языке программирования и МК для некоторого CPU будут слабо зависеть от выбора конкретного средства компиляции.

Как было указано, под размером ИК могут пониматься различные метрики – количество элементов текста (например, символы строки «int x = 0;»), лексических объектов (например, список токенов – TOK_INT, TOK_IDENT(«x»), TOK_ASSIGN, TOK_CONST(«0»), TOK_SEMICOLON), синтаксических конструкций (например, подграф в Abstract Syntax Tree [30] – AS_DECLARATION (AS_ASSIGN(AS_IDENT(«x»), AS_CONST(«0»))) и т.п. Однако, подсчет количества токенов ИК по сравнению с количеством символов приведет к увеличению производительности генетического алгоритма, поскольку генерация ИК из лексически верных фрагментов текста (а не случайной последовательности текста) будет с большей вероятностью приводить к компилируемому экземпляру. Использование более абстрактных сущностей (подграфов синтаксических конструкций, соответствующих формальному синтаксису языка) является возможным, но и более сложным, что и будет исследовано автором в дальнейшем.

В эксперименте при построении зависимости размера ИК от МК были обнаружены некоторые аномально высокие размеры МК в объектных файлах, что, однако, было обосновано особенностями кодирования ИК и спецификой генерируемого МК. Исходя из того, что количество таких аномалий (3 штуки) является несущественным по сравнению с общим количеством рассмотренных экземпляров (82282), а значение аномального размера является единичным и превышает средний не более чем в 10 раз (см. Рисунок 1), то и на формулу зависимости они не оказывают существенного влияния. По этой же причине, при расчете пропускался ИК, в котором использовались типы double и float, а также присутствовала динамическая инициализация массивов в теле функций.

Полученная формула зависимости размера ИК от размера МК имеет следующую достаточно простую линейную форму:

$$SC_{Size} = A \times MC_{Size} + B,$$

где A и B – некоторые коэффициенты. Впрочем, это является закономерным и вполне отражающим реальность, поскольку увеличение конструкций в ИК логично ведет к соизмеримому увеличению инструкций в МК.

Заключение

В работе приводится авторский альтернативный подход к декомпиляции МК с получением ИК, анализ которых на предмет наличия уязвимостей может существенно повысить безопасность любого ПО. Суть подхода (сокращенно ГРИМК) заключается в применении искусственного интеллекта в части генетических алгоритмов для итеративного приближения ИК к такому представлению, которое бы компилировалось в нужный МК. Одной из задач ГРИМК является определение размера исходного ИК (соответствующего длине хромосомы в терминологии генетического алгоритма), чему и посвящено данное исследование.

Основным результатом текущей работы является Метод (и Прототип), позволяющий с использованием статистических данных определить зависимость между размерами ИК и МК отдельно взятых функций (для этого используется открытый датасет – ExeBench). Также получена непосредственная формула зависимости размеров, а именно следующая:

$$SC_{Size} = 0.6057 \times MC_{Size} + 9.8242.$$

Теоретическая значимость исследования заключается в установлении прямой зависимости между размером ИК и МК для типовых функций. Практическая значимость состоит в возможности подбора параметров различных алгоритмов (включая генетические в рамках ГРИМК), которым необходимо прогнозировать размеры представлений ПО при взаимообратном преобразовании между ИК и МК.

Продолжением работы должно стать получение зависимостей между размерами ИК и МК С-функций для различных режимов работы компиляторов и инструкций CPU, уточнение формулы зависимости исходя из особенностей МК, а также выбор более сложных сущностей для конструирования ИК. Также планируется распространение описанного подхода ГРИМК и на другие, даже не смежные, области (например, для интеллектуальной адаптации графических интерфейсов под задачи пользователей [31] или обнаружения сложно-взаимодействующих уязвимостей [32, 33]).

Литература

1. *Абдуллин Т. И., Баев В.Д ., Буйневич М. В., Бурзунов Д. Д., Васильева И. Н., Галиуллина Э. Ф. и др. Цифровые технологии и проблемы информационной безопасности: монография. СПб: СПГЭУ 2021. 163 с.*
2. *Katz D. S., Ruchti J., Shulte E. Using recurrent neural networks for decompilation // The proceedings of 25th International Conference on Software Analysis, Evolution and Reengineering (Campobasso, Italy, 20–23 March 2018). 2018. PP. 346–356. DOI: 10.1109/SANER.2018.8330222.*
3. *Fokin A., Troshina K., Chernov A. Reconstruction of class hierarchies for decompilation of C++ programs // The proceedings of 14th European Conference on Software Maintenance and Reengineering (Madrid, Spain, 15–18 March 2010). 2011. PP. 240–243. DOI: 10.1109/CSMR.2010.43.*
4. *Ревнивых А. В., Велижанин А. С. Методика автоматизированного формирования структуры дизассемблированного листинга // Кибернетика и программирование. 2019. № 2. С. 1–16. 10.25136/2306-4196.2019.2.28272*
5. *Poudyal S., Dasgupta D. AI-powered ransomware detection framework // The proceedings of Symposium Series on Computational Intelligence (Canberra, ACT, Australia, 01–04 December 2020). 2021. PP. 1154–1161. DOI: 10.1109/SIKI47803.2020.9308387.*
6. *Израилов К. Е. Методология реверс-инжиниринга машинного кода. Часть 3. Динамическое исследование и документирование. Труды учебных заведений связи. 2024. Т. 10. № 1. С. 86–96. DOI: 10.31854/1813-324X-2024-10-1-86-96.*
7. *Израилов К. Е. Методология реверс-инжиниринга машинного кода. Часть 2. Статическое исследование. Труды учебных заведений связи // 2023. Т. 9. № 6. С. 68–82. DOI: 10.31854/1813-324X-2023-9-6-68-82.*
8. *Израилов К. Е. Методология реверс-инжиниринга машинного кода. Часть 1. Подготовка объекта исследования // Труды учебных заведений связи. 2023. Т. 9. № 5. С. 79–90. DOI: 10.31854/1813-324X-2023-9-5-79-90.*
9. *Kotenko I., Izrailov K., Buinevich M. The Method and Software Tool for Identification of the Machine Code Architecture in Cyberphysical Devices // Journal of Sensor and Actuator Networks. 2023. Vol. 12. Iss. 1. PP. 11. DOI: 10.3390/jsan12010011*
10. *Частикова В. А., Чич А. И. Генетические алгоритмы и генетическое программирование: особенности реализации // Перспективы науки. 2019. № 1 (112). С. 13–16.*
11. *Xia B., Ge Y., Yang R., Yin J., Pang J., Tang C. BContext2Name: naming functions in stripped binaries with multi-label learning and neural networks // The proceedings of 10th International Conference on Cyber Security and Cloud Computing (CSCloud) / 9th International Conference on Edge Computing and Scalable Cloud (Xiangtan, Hunan, China, 01-03 July 2023). 2023. PP. 167–172. DOI: 10.1109/CSCloud-EdgeCom58631.2023.00037.*
12. *A. Jaffe, J. Lacomis, Schwartz E. J., Goues C. L., Vasilescu B. Meaningful variable names for decompiled code: a machine translation approach // The proceedings of 26th International Conference on Program Comprehension (Gothenburg, Sweden, 27 May 2018 – 03 June 2018). 2020. PP. 20–2010.*
13. *Shudrak M., Zolotarev V. The new technique of decompilation and its application in information security // The proceedings of Sixth UKSim/AMSS European Symposium on Computer Modeling and Simulation (Malta, Malta, 14–16 November 2012). 2013. PP. 115–120. DOI: 10.1109/EMS.2012.20.*
14. *Alrabaee S., Choo K. -K. R., Qbea'h M., Khasawneh M. BinDeep: binary to source code matching using deep learning // The proceedings of 20th International Conference on Trust, Security and Privacy in Computing and Communications (Shenyang, China, 20–22 October 2021). 2022. PP. 1100–1107. DOI: 10.1109/TrustCom53373.2021.00150.*
15. *Katz D. S., Ruchti J., Schulte E. Using recurrent neural networks for decompilation // The proceedings of 25th International Conference on Software Analysis, Evolution and Reengineering (Campobasso, Italy, 20–23 March 2018). 2018. PP. 346–356. DOI: 10.1109/SANER.2018.8330222.*
16. *Ahmed T., Devanbu P., Sawant A. A. Learning to find usages of library functions in optimized binaries // IEEE Transactions on Software Engineering. 2021. Vol. 48. No. 10. PP. 3862–3876. DOI: 10.1109/TSE.2021.3106572.*
17. *Badri M., Badri L., Flageol W., Toure F. Source code size prediction using use case metrics: an empirical comparison with use case points // Innovations in Systems and Software Engineering. 2016. Vol. 13. PP. 143–159. DOI: 10.1007/s11334-016-0285-7.*
18. *Тютюнников Н. Н. Оценка размера программного средства с учетом адаптированного и повторно используемого исходного кода в модели COCOMO II // Фундаментальные и прикладные исследования: проблемы и результаты. 2014. № 11. С. 136–141.*

19. Частикова В. А., Чич А. И. Генетические алгоритмы и генетическое программирование: особенности реализации // Перспективы науки. 2019. № 1 (112). С. 13–16.
20. Архипов А. Н., Панов А. В. Применение кода Грея в генетическом алгоритме при кодировании признаков, представляемых целыми числами // ИТ-Стандарт. 2020. № 4 (25). С. 25–30.
21. Вавилина Е. А., Варламова С. А., Чеснов В. В. Исследование влияния изменения параметров генетического алгоритма на скорость решения задачи о рюкзаке // Информационные технологии в управлении и экономике. 2021. № 1 (22). С. 15–22.
22. Файзуллин Р. Ф. Потенциал генетических алгоритмов в задачах покрытия территории группой БЛА // Вестник РГГУ. Серия: Информатика. Информационная безопасность. Математика. 2024. № 1. С. 36–50. DOI: 10.28995/2686-679X-2024-1-36-50.
23. Kotenko, I., Izrailov, K., Buinevich, M., Saenko I., Shorey R. Modeling the Development of Energy Network Software, Taking into Account the Detection and Elimination of Vulnerabilities // Energies. 2023. Vol. 16. Iss. 13. PP. 5111. DOI: 10.3390/en16135111.
24. Kaleybar H. J., Davoodi M., Brenna M., Zaninelli D. Applications of genetic algorithm and its variants in rail vehicle systems: a bibliometric analysis and comprehensive review // Access. 2023. Vol. 11. PP. 68972–68993. DOI: 10.1109/ACCESS.2023.3292790.
25. Yu C. -Y., Huang C. -Y., Utilizing multi-objective evolutionary algorithms to optimize open source software release management // IEEE Access. 2023. Vol. 11. PP. 112248–112262. DOI: 10.1109/ACCESS.2023.3323615.
26. Jiacheng L., Lei L. A hybrid genetic algorithm based on information entropy and game theory // IEEE Access. 2020. Vol. 8. PP. 36602–36611. DOI: 10.1109/ACCESS.2020.2971060.
27. Bin Z., Zhichun G., Qiangqiang H. A genetic clustering method based on variable length string // The proceedings of 2nd International Conference on Safety Produce Informatization (Chongqing, China, 8-30 November 2019). 2020. PP. 460–464. DOI: 10.1109/IICSPI48186.2019.9095977.
28. Armengol-Estapé J., Woodruff J., Brauckmann A., Magalhães J. W. de S., O'Boyle M .F. P. ExeBench: an ML-scale dataset of executable C functions // The proceedings of 6th ACM SIGPLAN International Symposium on Machine Programming New York, NY, USA, 13 June 2022). 2022. PP. 50–59. DOI:10.1145/3520312.353486
29. Pashinska-Gadzheva M. Comparison of compiler efficiency with SSE and AVX instructions // The proceedings of International Conference Automatics and Informatics (Varna, Bulgaria, 06–08 October 2022). 2022. PP. 56–59. DOI: 10.1109/ICAI55857.2022.9960080.
30. Si G., Zhang Y., Li M., Jing S. Malicious code utilization chain detection scheme based on Abstract Syntax Tree // The proceedings of 6th Advanced Information Technology, Electronic and Automation Control Conference (Beijing, China, 03–05 October 2022). 2022. PP. 1108–1111. DOI: 10.1109/IAEAC54830.2022.9929773.
31. Курта П. А., Израилов К. Е. Обзор способов построения динамических адаптивных интерфейсов и их интеллектуализация // Научно-аналитический журнал «Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России». 2023. № 4. С. 119–132. DOI: 10.61260/2218-130X-2024-2023-4-119-132.
32. Буйневич М. В., Израилов К. Е. Антропоморфический подход к описанию взаимодействия уязвимостей в программном коде. Часть 1. Типы взаимодействий // Защита информации. Инсайд. 2019. № 5 (89). С. 78–85.
33. Буйневич М. В., Израилов К. Е. Антропоморфический подход к описанию взаимодействия уязвимостей в программном коде. Часть 2. Метрика уязвимостей // Защита информации. Инсайд. 2019. № 6 (90). С. 61–65.

References

1. Abdullin T.I., Baev V.D., Bujnevich M.V., Burzunov D.D., Vasil'eva I.N., Galiullina Je.F. i dr. Cifrovye tehnologii i problemy informacionnoj bezopasnosti: monografija. SPb: SPGJeU 2021. 163 s.
2. Katz D. S., Ruchti J., Shulte E. Using recurrent neural networks for decompilation // The proceedings of 25th International Conference on Software Analysis, Evolution and Reengineering (Campobasso, Italy, 20–23 March 2018). 2018. PP. 346–356. DOI: 10.1109/SANER.2018.8330222.
3. Fokin A., Troshina K., Chernov A. Reconstruction of class hierarchies for decompilation of C++ programs // The proceedings of 14th European Conference on Software Maintenance and Reengineering (Madrid, Spain, 15–18 March 2010). 2011. PP. 240–243. DOI: 10.1109/CSMR.2010.43.
4. Revnivyh A. V., Velizhanin A. S. Metodika avtomatizirovannogo formirovanija struktury dizassemblirovannogo listinga // Kibernetika i programmirovanie. 2019. № 2. S. 1–16. 10.25136/2306-4196.2019.2.28272
5. Poudyal S., Dasgupta D. AI-powered ransomware detection framework // The proceedings of Symposium Series on Computational Intelligence (Canberra, ACT, Australia, 01-04 December 2020). 2021. PP. 1154–1161. DOI: 10.1109/SIKI47803.2020.9308387.
6. Izrailov K. E. Metodologija revers-inzhiniringa mashinnogo koda. Chast' 3. Dinamicheskoe issledovanie i dokumentirovanie. Trudy uchebnyh zavedenij svjazi. 2024. T. 10. № 1. S. 86–96. DOI: 10.31854/1813-324X-2024-10-1-86-96.
7. Izrailov K. E. Metodologija revers-inzhiniringa mashinnogo koda. Chast' 2. Staticheskoe issledovanie. Trudy uchebnyh zavedenij svjazi // 2023. T. 9. № 6. S. 68–82. DOI: 10.31854/1813-324X-2023-9-6-68-82.
8. Izrailov K. E. Metodologija revers-inzhiniringa mashinnogo koda. Chast' 1. Podgotovka ob#ekta issledovanija // Trudy uchebnyh zavedenij svjazi. 2023. T. 9. № 5. S. 79–90. DOI: 10.31854/1813-324X-2023-9-5-79-90.
9. Kotenko I., Izrailov K., Buinevich M. The Method and Software Tool for Identification of the Machine Code Architecture in Cyberphysical Devices // Journal of Sensor and Actuator Networks. 2023. Vol. 12. Iss. 1. PP. 11. DOI: 10.3390/jsan12010011
10. Chastikova V. A., Chich A. I. Geneticheskie algoritmy i geneticheskoe programmirovanie: osobennosti realizacii // Perspektivy nauki. 2019. № 1 (112). S. 13–16.
11. Xia B., Ge Y., Yang R., Yin J., Pang J., Tang C. BContext2Name: naming functions in stripped binaries with multi-label learning and neural networks // The proceedings of 10th International Conference on Cyber Security and Cloud Computing (CSCloud) / 9th International Conference on Edge Computing and Scalable Cloud (Xiangtan, Hunan, China, 01–03 July 2023). 2023. PP. 167–172. DOI: 10.1109/CSCloud-EdgeCom58631.2023.00037.
12. A. Jaffe, J. Lacomis, Schwartz E. J., Goues C. L., Vasilescu B. Meaningful variable names for decompiled code: a machine translation approach // The proceedings of 26th International Conference on Program Comprehension (Gothenburg, Sweden, 27 May 2018 – 03 June 2018). 2020. PP. 20–2010.
13. Shudrak M., Zolotarev V. The new technique of decompilation and its application in information security // The proceedings of Sixth UKSim/AMSS European Symposium on Computer Modeling and Simulation (Malta, Malta, 14-16 November 2012). 2013. PP. 115–120. DOI: 10.1109/EMS.2012.20.

14. *Alrabaee S., Choo K. -K. R., Qbea'h M., Khasawneh M. BinDeep: binary to source code matching using deep learning // The proceedings of 20th International Conference on Trust, Security and Privacy in Computing and Communications (Shenyang, China, 20–22 October 2021). 2022. PP. 1100–1107. DOI: 10.1109/TrustCom53373.2021.00150.*
15. *Katz D. S., Ruchti J., Schulte E. Using recurrent neural networks for decompilation // The proceedings of 25th International Conference on Software Analysis, Evolution and Reengineering (Campobasso, Italy, 20-23 March 2018). 2018. PP. 346-356. DOI: 10.1109/SANER.2018.8330222.*
16. *Ahmed T., Devanbu P., Sawant A. A. Learning to find usages of library functions in optimized binaries // IEEE Transactions on Software Engineering. 2021. Vol. 48. No. 10. PP. 3862–3876. DOI: 10.1109/TSE.2021.3106572.*
17. *Badri M., Badri L., Flageol W., Toure F. Source code size prediction using use case metrics: an empirical comparison with use case points // Innovations in Systems and Software Engineering. 2016. Vol. 13. PP. 143–159. DOI: 10.1007/s11334-016-0285-7.*
18. *Tjutjunnikov N. N. Ocenka razmera programmnogo sredstva s uchetom adaptirovannogo i povtorno ispol'zuemogo ishodnogo koda v modeli COCOMO II // Fundamental'nye i prikladnye issledovanija: problemy i rezul'taty. 2014. № 11. S. 136–141.*
19. *Chastikova V. A., Chich A. I. Geneticheskie algoritmy i geneticheskoe programmirovanie: osobennosti realizacii // Perspektivy nauki. 2019. № 1 (112). S. 13–16.*
20. *Arhipov A. N., Panov A. V. Primenenie koda Greja v geneticheskom algoritme pri kodirovanii priznakov, predstavljaemyh celymi chislami // IT-Standart. 2020. № 4 (25). S. 25–30.*
21. *Vavilina E. A., Varlamova S. A., Chesnov V. V. Issledovanie vlijanija izmenenija parametrov geneticheskogo algoritma na skorost' reshenija zadachi o rjukzake // Informacionnye tehnologii v upravlenii i jekonomike. 2021. № 1 (22). S. 15–22.*
22. *Fajzullin R. F. Potencial geneticheskih algoritmov v zadachah pokrytija territorii gruppoj BLA // Vestnik RGGU. Serija: Informatika. Informacionnaja bezopasnost'. Matematika. 2024. № 1. S. 36–50. DOI: 10.28995/2686-679X-2024-1-36-50.*
23. *Kotenko, I., Izrailov, K., Buinevich, M., Saenko I., Shorey R. Modeling the Development of Energy Network Software, Taking into Account the Detection and Elimination of Vulnerabilities // Energies. 2023. Vol. 16. Iss. 13. PP. 5111. DOI: 10.3390/en16135111.*
24. *Kaleybar H. J., Davoodi M., Brenna M., Zaninelli D. Applications of genetic algorithm and its variants in rail vehicle systems: a bibliometric analysis and comprehensive review // Access. 2023. Vol. 11. PP. 68972–68993. DOI: 10.1109/ACCESS.2023.3292790.*
25. *Yu C. -Y., Huang C. -Y., Utilizing multi-objective evolutionary algorithms to optimize open source software release management // IEEE Access. 2023. Vol. 11. PP. 112248–112262. DOI: 10.1109/ACCESS.2023.3323615.*
26. *Jiacheng L., Lei L. A hybrid genetic algorithm based on information entropy and game theory // IEEE Access. 2020. Vol. 8. PP. 36602–36611. DOI: 10.1109/ACCESS.2020.2971060.*
27. *Bin Z., Zhichun G., Qiangqiang H. A genetic clustering method based on variable length string // The proceedings of 2nd International Conference on Safety Produce Informatization (Chongqing, China, 8-30 November 2019). 2020. PP. 460–464. DOI: 10.1109/IICSPI48186.2019.9095977.*
28. *Armengol-Estapé J., Woodruff J, Brauckmann A., Magalhães J. W. de S., O'Boyle M. F. P. ExeBench: an ML-scale dataset of executable C functions // The proceedings of 6th ACM SIGPLAN International Symposium on Machine Programming New York, NY, USA, 13 June 2022). 2022. PP. 50–59. DOI:10.1145/3520312.353486*
29. *Pashinska-Gadzheva M. Comparison of compiler efficiency with SSE and AVX instructions // The proceedings of International Conference Automatics and Informatics (Varna, Bulgaria, 06–08 October 2022). 2022. PP. 56–59. DOI: 10.1109/ICAI55857.2022.9960080.*
30. *Si G., Zhang Y., Li M., Jing S. Malicious code utilization chain detection scheme based on Abstract Syntax Tree // The proceedings of 6th Advanced Information Technology, Electronic and Automation Control Conference (Beijing, China, 03-05 October 2022). 2022. PP. 1108–1111. DOI: 10.1109/IAEAC54830.2022.9929773.*
31. *Kurta P. A., Izrailov K. E. Obzor sposobov postroenija dinamicheskih adaptivnyh interfejsov i ih intellektualizacija // Nauchno-analiticheskij zhurnal «Vestnik Sankt-Peterburgskogo universiteta Gosudarstvennoj protivopozharnoj sluzhby MChS Rossii». 2023. № 4. S. 119–132. DOI: 10.61260/2218-130X-2024-2023-4-119-132.*
32. *Bujnevich M. V., Izrailov K. E. Antropomorficheskij podhod k opisaniju vzaimodejstvija ujazvimostej v programmnom kode. Chast' 1. Tipy vzaimodejstvij // Zashhita informacii. Insajd. 2019. № 5 (89). S. 78–85.*
33. *Bujnevich M. V., Izrailov K. E. Antropomorficheskij podhod k opisaniju vzaimodejstvija ujazvimostej v programmnom kode. Chast' 2. Metrika ujazvimostej // Zashhita informacii. Insajd. 2019. № 6 (90). S. 61–65.*

ПРИМЕНЕНИЕ ЛОГИКО-ВЕРОЯТНОСТНОГО МЕТОДА В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. Часть 5

Калашников А. О.[1], Аникина Е. В.[2], Бугайский К. А.[3], Бирин Д. С.[4], Дерябин Б. О.[5], Цепенда С. О.[6], Табаков К. В.[7]

DOI: 10.21681/2311-3456-2024-4-26-37

Цель исследования: *адаптация логико-вероятностного метода оценивания сложных систем к задачам построения систем защиты информации в многоагентной системе.*

Метод исследования: *при проведении исследования использовались основные положения методологии структурного анализа, системного анализа, теории принятия решений, методов оценивания событий при условии неполной информации, логико-вероятностных методов.*

Полученный результат: *данная статья продолжает рассмотрение вопросов информационной безопасности на основе анализа отношений между субъектами и объектом защиты. Показано, что состояние отношений агента может быть получено на основе соответствующих оценок состояний на уровне информационных ресурсов и информационных потоков. Показано, что оценка состояний может быть проведена как на качественном, так и на количественном уровнях, на основе формируемых в агенте, в результате внешних воздействий, наборов событий и сообщений. Предложены механизмы качественного и количественного оценивания состояний отношений между субъектами и объектом защиты. Полученные результаты обеспечивают обоснованное вычисление и применение вероятностных характеристик для последующего применения логико-вероятностного метода при анализе указанных отношений.*

Научная новизна: *рассмотрение вопросов защиты информации с использованием аппарата математических и логических отношений. Сформулирована гипотеза о структуре многоагентной системы с точки зрения информационной безопасности. Разработаны методы качественного определения состояний отношений на уровне агентов. Разработаны методы получения вероятностных оценок состояний отношений на уровне. Показана возможность получения интегральных вероятностных оценок для различных подсистем современных информационных систем за счет агрегирования соответствующих оценок агентов.*

Вклад авторов: *Калашников А. О. выполнил постановку задачи и общую разработку модели применения логико-вероятностного метода в информационной безопасности. Бугайский К. А. и Аникина Е. В. участвовали в написании всех разделов статьи. Бирин Д. С. и Дерябин Б. О. участвовали в написании раздела о доверии состояния агента. Цепенда С. О. и Табаков К. В. участвовали в написании раздела о масштабировании доверии агента.*

Ключевые слова: *модель информационной безопасности, оценка сложных систем, логико-вероятностный метод, теория отношений, системный анализ.*

APPLICATION OF THE LOGICAL-PROBABILISTIC METHOD IN INFORMATION SECURITY. Part 5

Kalashnikov A. O.[8], Anikina E. V.[9], Bugajskij K. A.[10], Birin D. S.[11], Deryabin B. O.[12], Tsependa S. O.[13], Tabakov K. V.[14]

1 Калашников Андрей Олегович, доктор технических наук, главный научный сотрудник лаборатории «Безопасности сложных систем» ФГБУН Институт проблем управления им. В. А. Трапезникова РАН, г. Москва, Россия. E-mail: aokalash@ipu.ru
2 Аникина Евгения Владимировна, научный сотрудник лаборатории «Безопасности сложных систем» ФГБУН Институт проблем управления им. В. А. Трапезникова РАН, г. Москва, Россия. E-mail: ajanet@ipu.ru
3 Бугайский Константин Алексеевич, младший научный сотрудник лаборатории «Безопасности сложных систем» ФГБУН Институт проблем управления им. В. А. Трапезникова РАН, г. Москва, Россия. E-mail: kabuga@ipu.ru
4 Бирин Денис Сергеевич, младший научный сотрудник Научно-внедренческого отдела 89 ФГБУН Институт проблем управления им. В. А. Трапезникова РАН, г. Москва, Россия. E-mail: birin@phystech.edu
5 Дерябин Богдан Олегович, младший научный сотрудник Научно-внедренческого отдела 89 ФГБУН Институт проблем управления им. В. А. Трапезникова РАН, г. Москва, Россия. E-mail: baga_d@mail.ru
6 Цепенда Сергей Олегович, младший научный сотрудник Научно-внедренческого отдела 89 ФГБУН Институт проблем управления им. В. А. Трапезникова РАН, г. Москва, Россия. E-mail: tsepende.s@gmail.com
7 Табаков Кирилл Викторович, младший научный сотрудник Научно-внедренческого отдела 89 ФГБУН Институт проблем управления им. В. А. Трапезникова РАН, г. Москва, Россия. E-mail: tabakov2002@mail.ru

8 Andrey O. Kalashnikov, Dr.Sc., Chief Scientist of the Laboratory «Security of complex systems» Institute of Control Sciences of Russian Academy of Sciences, Moscow, Russia. E-mail: aokalash@ipu.ru
9 Eugenia V. Anikina, Research Fellow of the Laboratory « Security of complex systems » Institute of Control Sciences of Russian Academy of Sciences, Moscow, Russia. E-mail: ajanet@ipu.ru
10 Konstantin A. Bugajskij, Junior Researcher of the Laboratory « Security of complex systems » Institute of Control Sciences of Russian Academy of Sciences, Moscow, Russia. E-mail: kabuga@ipu.ru
11 Denis S. Birin, Junior Researcher of the Scientific and Implementation Department Institute of Control Sciences of Russian Academy of Sciences, Moscow, Russia. E-mail: birin@phystech.edu
12 Bogdan O. Deryabin, Junior Researcher of the Scientific and Implementation Department Institute of Control Sciences of Russian Academy of Sciences, Moscow, Russia. E-mail: baga_d@mail.ru
13 Sergey O. Tsependa, Junior Researcher of the Scientific and Implementation Department Institute of Control Sciences of Russian Academy of Sciences, Moscow, Russia. E-mail: tsepende.s@gmail.com
14 Kirill V. Tabakov, Junior Researcher of the Scientific and Implementation Department Institute of Control Sciences of Russian Academy of Sciences, Moscow, Russia. E-mail: tabakov2002@mail.ru

The purpose of the article: *adaptation of the logical-probabilistic method of evaluating complex systems to the tasks of building information security systems in a multi-agent system.*

Research method: *during the research, the main provisions of the methodology of structural analysis, system analysis, decision theory, methods of evaluating events under the condition of incomplete information were used.*

The result: *this article continues the consideration of information security issues based on the analysis of the relationship between the subjects and the object of protection. It is shown that the state of the agent's relations can be obtained on the basis of appropriate assessments of states at the level of information resources and information flows from the agent. It is shown that the assessment of states can be carried out at the qualitative and quantitative levels on the basis of sets of events and messages formed in the agent as a result of external influences. The mechanisms of qualitative and quantitative assessment of the states of relations are proposed. The obtained results provide a reasonable acquisition and application of probabilistic characteristics for the subsequent application of the logical-probabilistic method in the analysis of relations between subjects and the object of protection.*

Scientific novelty *consideration of information security issues using the apparatus of mathematical and logical relations. A hypothesis about the structure of a multi-agent system from the point of view of information security is formulated. Methods of qualitative determination of the states of relations at the agent level have been developed. Methods for obtaining probabilistic estimates of the states of relations at the level have been developed. The possibility of obtaining integral probabilistic estimates for various subsystems of modern information systems by aggregating the corresponding estimates of agents is shown.*

Keywords: *information security model, assessment of complex systems, logical-probabilistic method, theory of relations, system analysis.*

Введение

Данная статья является пятой из серии публикаций, посвященных исследованию вопроса применения логико-вероятностного метода при изучении вопросов защиты информации. Метод был разработан Рябининым И.А. [1, см. ссылки на соответствующую литературу там же] и приобрел популярность при проведении исследований, в том числе, связанных с анализом и оценкой рисков сложных систем. Прежде всего для решения вопросов оценки надежности работы систем и анализа причин возникновения аварийных ситуаций. Логико-вероятностный метод предполагает решение следующих задач:

1. Построение структурно-логической модели системы за счет выделения и использования событий с несовместными исходами.
2. Проведение преобразований полученных логических уравнений на основе функций булевой алгебры с целью получения системы уравнений с конечным числом переменных.
3. Теоретически обоснованный переход от уравнений булевой алгебры к уравнениям с вероятностными переменными.

К несомненным достоинствам логико-вероятностного метода следует отнести его способность обеспечить прозрачность процедур анализа и оценки сложных систем, а также хорошие адаптационные способности к новым задачам. Результатом применения логико-вероятностного метода являются количественные оценки риска как вероятности нарушения работоспособности системы. Интерес к логико-вероятностному методу – помимо типичных вопросов надежности систем, – в настоящее время подкрепляется исследованием задач машинного обучения и связанных с ними проблем оптимизации расчетов [см., например, 2–5]. В частности, логико-вероятностный метод обеспечивает хорошую точность и стабильность результатов в задачах распознавания тех или иных объектов. Логико-вероятностный метод также находит свое применение и при решении задач защиты информации [см., например, 6–11].

Тем не менее, представляется, что логико-вероятностный метод обладает значительно большим, пока не раскрытым, потенциалом в случае его дальнейшего развития и адаптации к решению различных задач в области информационной безопасности (далее – ИБ).

Постановка задачи

Логико-вероятностный метод обладает достаточно обширным набором подходов и решений по работе с логическими функциями, описывающими функционирование сложных систем, какими являются современные информационные системы (далее – ИС). Исследование применимости логико-вероятностного метода для решения задач ИБ базируется на представлении ИС в виде отношений между агентами.

В рамках достижения общей цели исследования возникает задача разработки формально-логических основ для вычисления вероятностных параметров характеризующих состояния отношений конкретного агента с другими агентами из состава ИС. Разработка таких вероятностных параметров на системном уровне выполнена в настоящей статье.

Общие положения

Приведем некоторые сведения из предыдущих статей цикла [12–15], которые необходимы для решения поставленной задачи.

1. Определим агентов из состава ИС, участвующих в обмене информацией с данным, как респондентов. Состояние отношений между агентом β и его респондентом γ являются следствием внешнего воздействия на агента со стороны респондента. Такие состояния отношений $\beta R \gamma$ агента с респондентом (далее – состояния) образуют множество $R = \{Lr,Dr,Ir,Ur\}$, где Lr означает Лояльное, Dr – Нелояльное, Ir – Неопределенное и Ur – Безразличное.
2. Агент (см. [13], определение *Def.* 5) представляет из себя набор информационных ресурсов (далее – ИР) и информационных потоков (далее – ИП), обеспечивающих обработку определенной категории данных в интересах субъекта, представленного аккаунтом в ИС. В дальнейшем все ИП и ИР агента будем определять как объекты. Обозначим через K множество объектов, входящих в состав агента.
3. Для каждого объекта $k \in K$ и для каждого из возможных состояний агента $r \in R$ может быть вычислена [15] оценка правдоподобия нахождения объекта в том или ином состоянии или уровень доверия к нахождению объекта в определенном состоянии. В дальнейшем этот уровень доверия будем обозначать как p_k^r.
4. Нахождение агента в том или ином состоянии определяется аналогичными (по типу) состояниями объектов из его состава. Для определения состояния агента необходимо учитывать уровни доверия состояний всех объектов из его состава.
5. В предыдущих статьях цикла [12, 13] были рассмотрены аксиомы о характере отношений между агентами в ИС. Приведем краткое содержание этих аксиом, сохраняя их нумерацию в [12, 13]:

Аксиома 3. Любой агент – участник отношения может быть только Лояльным или Безразличным (отключенным) по отношению к себе.

Аксиома 5. Любой агент – участник отношения может находиться только в одном состоянии из R в фиксированный момент времени:

Аксиома 7. Объекты (ИП и ИР) внутри агента всегда Лояльны по отношению друг к другу.

Аксиома 8. Любой субъект – пользователь ИС представлен в ИС как агент.

Аксиома 10. Отношения «субъект-субъект» и «субъект-объект» в ИС эквивалентны отношениям агентов из состава ИС.

Доверие состояния агента

Процесс функционирования агента и его взаимодействия с окружением [12–18] описывается единым множеством состояний: $R = \{Lr,Dr,Ir,Ur\}$, независимо от типа аккаунта и числа объектов в составе агента. Сформулируем следующее утверждение.

Утверждение 1. Все объекты из состава агента подобны друг другу (изоморфны) в смысле аналогии в характере элементов и отношений между элементами.

Доказательство утверждения основано на следующих соображениях. Обычно различение объектов из состава агента основывается на рассмотрении потенциальных возможностей использования уязвимостей в деструктивных целях, а также на категорировании обрабатываемой объектами информации. В обоих случаях все объекты из состава агента эквивалентны в силу их функционирования в едином пространстве прав доступа аккаунта определяющего состав агента (*Аксиома 8*). Также *Аксиома 7* дает основание говорить об эквивалентности и единообразии отношений между объектами в составе агента. Кроме того, на основании *Аксиом 3*, *7* и *10* можно положить, что все объекты из состава агента оказывают влияние на его оценку состояний отношений с респондентами, причем это влияние имеет синергетический эффект. Наконец, еще раз укажем, что в рамках принятого подхода объекты определяются наборами событий (как реакция на внешние воздействия), которые описываются единым для всех набором параметров, то есть обладают подобием в силу ортогонализации их параметров, описанной в [14].

Современные вычислительные средства, содержащие сотни программных компонент, а также методы их разработки, основанные прежде всего на широком повторном использовании кода (например, в виде сторонних фреймворков различных разработчиков) позволяют сделать следующие допущения.

D1. Взаимодействие объектов в процессе функционирования агента носит в известной степени стохастический характер с точки зрения возникновения и существования связей между объектами.

D2. С точки зрения степени участия в реализации отдельных функций агента роли объектов также отличаются высокой вариативностью.

Утверждение 1 и *допущения D1, D2* позволяют представить агента в виде множества изоморфных объектов, вносящих переменный и слабо предсказуемый вклад в оценку внешних воздействий на агента или формирование состояний отношений агента с респондентами. Необходимо подчеркнуть, что состояния объектов принимают значения из единого множества состояний $R = \{Lr,Dr,Ir,Ur\}$, тождественному множеству состояний агента [13, 14].

При этом объекты можно считать независимыми поскольку процедура вычисления уровня доверия их состояний базируется на независимых и уникальных для каждого объекта множествах событий. Кроме того, объекты из состава агента преимущественно

имеют различное функциональное назначение, а, следовательно, необходимо говорить о независимости и вариативности трактовок событий и состояний с точки зрения защиты информации. Таким образом, значения уровней доверия состояний для каждого из объектов из состава агента образуют вектор $Q_k^r = [p_k^L, p_k^D, p_k^I, p_k^U]$.

Используя подход, изложенный в предыдущей статье цикла [15], в качестве вероятностной характеристики состояния отношений агент-респондент $\beta R\gamma$, как отклика на внешнее воздействие, будем рассматривать уровень доверия к нахождению агента в определенном состоянии.

Согласно *Аксиоме 5* в каждый фиксированный момент времени отношение агент-респондент $\beta R\gamma$ может принимать только одно значение из R. Следовательно, каждое из состояний множества R можно рассматривать как альтернативную гипотезу для отношения $\beta R\gamma$ агента. Таким образом, следует рассматривать определение состояния отношения агента как задачу выбора гипотезы и определения уровня доверия к этому выбору на основании доказательств представленных уровнями доверия p_k^r состояний объектов из состава агента.

Определим функцию выбора гипотезы о состоянии отношений агента, например $H(Lr) = FG(\cup_{k\in K} p_k^L)$ или в общем виде:

$$H(r) = FG(\cup_{k\in K} p_k^r) \quad (1)$$

Из выражения (1) следует, что для выбора гипотез, функция FG должна опираться на метрику, позволяющую обрабатывать различные сочетания компонент векторов Q_k^r объектов из состава агента. Изоморфность объектов позволяет рассматривать вектор Q_k^r для каждого объекта как множество $A_k^r = \{p_k^L, p_k^D, p_k^I, p_k^U\}$. Обозначим $B = \cup_{k\in K} A_k^r$ и определим величину $\mu: R \times B \longrightarrow E$, $E = [1,2,3,4]$ как меру $\mu \in E$, которая должна для каждого из объектов выполнять условия:

$$1 \le \mu_k^r \le 4,$$
$$p_k^i < p_k^j \Longrightarrow \mu_k^i < \mu_k^j,\ i, j \in R.$$

Фактически речь идет о ранжировании состояний объектов в соответствии со значениями вектора Q_k^r: $minQ_k^r \Longrightarrow \mu_k^r = 1$ и $maxQ_k^r \Longrightarrow \mu_k^r = 4$. Введенная мера позволяет при определении состояний объекта перейти от вектора уровней доверия $Q_k^r = [p_k^L, p_k^D, p_k^I, p_k^U]$ к вектору рангов $V_k^r = [\mu_k^L, \mu_k^D, \mu_k^I, \mu_k^U]$ и на основании изоморфности объектов переписать выражение (1) как:

$$H(r) = FG(\cup_{k\in K} \mu_k^r) \quad (2)$$

Из выражения (2) следует, что для сравнения гипотез функция FG должна выполнять агрегирование величин из множества $M_H = \cup_{k\in K} \mu_k^r$. Проведенные ранее исследования, связанные с описанием внешних воздействий на агента [19–23], а также выражения (1) и (2) позволяют говорить об аддитивном и немонотонном характере функции FG.

Напомним, что объекты из состава агента преимущественно имеют различное функциональное назначение, что влечет независимость и вариативность трактовок событий и состояний и позволяет (согласно [15]) рассматривать уровни доверия p_k^r и соответствующую меру μ_k^r состояния каждого объекта из состава агента в качестве критериев для выбора гипотезы $H(r)$.

Следовательно, функция FG должна обеспечивать агрегирование величин из множества $M_H = \cup_{k\in K} \mu_k^r$ через операцию многокритериальной свертки. Данную свертку проведем на базе методологии комплексного оценивания состояний объектов агента, для чего будем опираться на положения и выводы, изложенные в [24–28]. Свертка на основе комплексного оценивания определяется структурой матриц свертки и порядком их применения, что практически полностью определяется порядком следования и значимостью (весом в агрегированном результате) сворачиваемых критериев. Выражение (2) позволяет сформулировать следующее утверждение.

Утверждение 2. Для выбора гипотезы о состоянии отношений агента достаточно учитывать только порядок следования рангов объектов как критериев свертки.

Доказательство утверждения. Из предыдущих рассуждений следует, что состояние отношений агента определяется состояниями объектов, то есть их реакцией на внешние воздействия. Реакция объекта на внешние воздействия определяется наличием уязвимостей, слабостей и ошибок в объектах. Если рассмотреть все объекты (ИР и ИП) из состава агента с точки зрения их функционирования как элементов вычислительной системы, то все они эквивалентны в силу наличия системных вызовов при обращении к физическим носителям информации [16–18]. Поскольку для выбора гипотезы имеет значение наличие реакции объекта, то есть его состояние, а не вызвавшие его причины, то все объекты из состава агента *равноценны* в смысле веса при проведении комплексного оценивания. *Аксиома 7* и допущения *D1*, *D2* позволяют представить структуру агента в виде полного графа, при этом любое внешнее воздействие на агента имеет «точку входа» и «целевую точку», которые целесообразно ассоциировать с тем или иным объектом из состава агента. Следовательно, внешнее воздействие отображается на некую последовательность объектов на графе различающихся только расстоянием от начальной («точки входа») или конечной («целевой точки») вершин.

Таким образом, на основании *Утверждения 2* порядок следования матриц комплексного оценивания должен обеспечивать последовательный перебор необходимых критериев и представлять собой ветвь дерева.

Утверждение 3. Все узлы ветви дерева комплексного оценивания представляют собой единую матрицу свертки.

Доказательство вытекает из *Утверждения 1* и *Утверждения 2*.

С учетом свойства синергии объектов матрица свертки рангов состояний объектов $E{\times}E$ для оценки отдельного состояния отношений агента примет вид:

$$\|\eta_{ij}\| = E{\times}E = \begin{bmatrix} 3 & 3 & 4 & 4 \\ 2 & 2 & 3 & 4 \\ 1 & 2 & 2 & 3 \\ 1 & 1 & 2 & 3 \end{bmatrix} \quad (3)$$

Утверждение 3 позволяет определить необходимое число шагов с применением матрицы свертки как: $S = |K| - 1$.

Отметим, что *Утверждение 2* и *Утверждение 3* обеспечивают наименьшие вычислительные затраты и возможность распараллеливания процедур комплексного оценивания для каждой из гипотез (2).

Обозначим операцию свертки как «⋈», сворачиваемый на отдельном шаге ранг объекта как $\mu(k)$, а результат свертки на данном шаге как $\eta(s)$. Процедуру комплексного оценивания можно представить в виде рекурсии:

$$\eta(s) = \eta(s-1) \bowtie \mu(k) \quad (4)$$

Свертка на каждом шаге комплексного оценивания представляет из себя один из следующих вариантов соотношений сворачиваемых величин:

$sy1$: $\mu(k) < \eta(s-1) \longrightarrow \eta(s) < \eta(s-1)$ – ранг очередного объекта уменьшает результат свертки;

$sy2$: $\mu(k) < \eta(s-1) \longrightarrow \eta(s) > \eta(s-1)$ – ранг очередного объекта увеличивает результат свертки;

$sy3$: $\mu(k) < \eta(s-1) \longrightarrow \eta(s) = \eta(s-1)$ – результат свертки остается неизменным.

Варианты строгого неравенства $sy1$ и $sy2$ позволяют использовать аналогию ставок, которые понижают и повышают итоговый ранг комплексного оценивания. Соответственно, принимаем величины $\mu(k)$ на каждом шаге как участвующие в свертке критерии несущие отрицательную и положительную коннотацию с точки зрения получения конечного результата комплексного оценивания гипотезы $H(r)$ о текущем состоянии отношения агента. То есть, будем трактовать $\mu(k)$ как категории «за» или «против» результата, что дает возможность для формирования следующих логических выражений:

pro – участвующий на данном шаге комплексного оценивания объект своим состоянием подтверждает гипотезу $H(r)$ о текущем состоянии отношения агента;

contra – участвующий на данном шаге комплексного оценивания объект своим состоянием отрицает гипотезу $H(r)$ о текущем состоянии отношения агента;

undef – участвующий на данном шаге комплексного оценивания объект своим состоянием вносит неопределенность в оценке гипотезы $H(r)$ о текущем состоянии отношения агента.

Для случая неизменности результата свертки дадим следующие трактовки:

$sy31$ – при значении ячейки матрицы $\eta_{ij} = 1$ состояние объекта отрицает гипотезу H(r) о текущем состоянии отношения агента;

$sy32$ – при значении ячейки матрицы $\eta_{ij} = 2$ состояние объекта в основном отрицает гипотезу $H(r)$ о текущем состоянии отношения агента;

$sy33$ – при значении ячейки матрицы $\eta_{ij} = 3$ состояние объекта в основном поддерживает гипотезу $H(r)$ о текущем состоянии отношения агента;

$sy34$ – при значении ячейки матрицы $\eta_{ij} = 4$ состояние объекта подтверждает гипотезу $H(r)$ о текущем состоянии отношения агента.

Образуем множество $SY = \{sy1, sy2, sy31, sy32, sy33, sy34\}$ и на его основе введем правила формирования категорий оценки соответствующих логическим выражениям *pro*, *contra* и *undef*, предварительно сделав следующее утверждение.

Утверждение 4. Элементы множества SY, получаемые в результате применения матрицы свертки на каждом шаге комплексного оценивания, могут использоваться в качестве критерия отнесения величин p_k^r сворачиваемых объектов к той или иной категории – pro, contra или undef.

Доказательство утверждения основано на аддитивности функции FG и тождественности $\mu_k^r \equiv p_k^r$, вытекающей из выражений (1–4).

Обозначим через $p_k^r(y)$, $y \in SY$ величину p_k^r соответствующую правилу формирования конкретного логического выражения на основании выбора элементов из множества SY.

Категорию $pro(r,SY)$ будем рассматривать как сумму доказательств повышающих уверенность в результате комплексного оценивания гипотезы $H(r)$:

$$pro(r,SY) = \sum_K p_k^r(y),\ y = sy2 \cup sy34 \quad (5)$$

Категорию $contra(r,SY)$ будем рассматривать как сумму доказательств снижающих уверенность в результате комплексного оценивания гипотезы $H(r)$:

$$contra(r,SY) = \sum_K p_k^r(y),\ y = sy1 \cup sy31 \quad (6)$$

Категорию $undef(r,SY)$ будем рассматривать как сумму доказательств снижающих уверенность в результате комплексного оценивания гипотезы $H(r)$:

$$undef(r,SY) = \sum_K p_k^r(y),\ y = sy32 \cup sy33 \quad (7)$$

Согласно *Аксиомы 5* в фиксированный момент времени агент может находиться только в одном из возможных состояний отношений:

$$\beta R\gamma = Lr\,\overline{DrIrUr} \vee \overline{Lr}\,Dr\,\overline{IrUr} \vee \overline{LrDr}\,Ir\,\overline{Ur} \vee \overline{LrDrIr}\,Ur \quad (8)$$

Выражение (8) определяет «активное» состояние отношения агента и показывает, что порядок определения активного состояния единообразен для всех состояний. Предыдущие рассуждения позволяют отождествить состояние агента с той или иной гипотезой. Это дает основание определить множество гипотез $H = \{h_1,h_2,h_3,h_4\}$ и ввести высказывания x_i – «гипотеза принимается» и $\bar{x}_i$ – «гипотеза отвергается», которые образуют функции $f^1(x_1,x_2,x_3,x_4) = 1$ и $f^0(\bar{x}_1,\bar{x}_2,\bar{x}_3,\bar{x}_4) = 0$. Соответственно, выражение (8) можем записать как $h_1 \vee h_2 \vee h_3 \vee h_4 = 1$, где гипотезы принимают вид $h_1 = x_1\bar{x}_2\bar{x}_3\bar{x}_4$, $h_2 = x_2\bar{x}_1\bar{x}_3\bar{x}_4$, $h_3 = x_3\bar{x}_1\bar{x}_2\bar{x}_4$ и $h_4 = x_4\bar{x}_1\bar{x}_2\bar{x}_3$. Тогда: $1 - h_1 = h_2 \vee h_3 \vee h_4$ означает условие для отказа от гипотезы h_1, что полностью запишется как;

$$1 - x_1\bar{x}_2\bar{x}_3\bar{x}_4 = x_2\bar{x}_1\bar{x}_3\bar{x}_4 \vee x_3\bar{x}_1\bar{x}_2\bar{x}_4 \vee x_4\bar{x}_1\bar{x}_2\bar{x}_3 \quad (9)$$

Выражение (9) представляет собой совершенную ДНФ, что позволяет перейти к определению оценки доверия состояния отношения (гипотезы) агента в соответствии с выражениями (5–7). Обозначим вероятности истинности аргументов за принятие гипотезы, как $\varrho_i = p(x_i)$, а вероятности истинности аргументов за отвержение гипотезы как $\epsilon_i = p(x_i)$. Тогда выражение (9) с учетом $h_1' = 1 - h_1$ примет вид:

$$p(h_1') = \epsilon_1\,\epsilon_3\,\epsilon_4\,\varrho_2 + \epsilon_1\,\epsilon_2\,\epsilon_4\,\varrho_3 + \epsilon_1\,\epsilon_2\,\epsilon_3\,\varrho_4 \quad (10)$$

Для гипотез h_2, h_3, h_4 расчеты выполняются аналогично выражениям (9) и (10). Для определения величин $\varrho_i = p(x_i)$ и $\epsilon_i = p(x_i)$ вернемся к определениям результатов комплексного оценивания данных в (4)–(7) и введем нормировочную величину $norm(r) = \sum_K p_k^r$. Тогда нормализованное доказательство повышающее уверенность в результате комплексного оценивания гипотезы $H(r)$ равно $\varrho_r = pro(r,SY) / norm(r)$, а, соответственно, нормализованное доказательство снижающее уверенность – $\epsilon_r = contra(r,SY) / norm(r)$. Обозначим: $\upsilon_r = undef(r,SY) / norm(r)$. Роль этой величины как показателя неопределенности при определении состояния отношений агента будет рассмотрена в следующих статьях цикла. Отметим, что из выражений (4)–(7) следует $\varrho_r + \epsilon_r + \upsilon_r = 1$. В итоге мы получим матрицу исходных оценок гипотез состояний агента $AQ = \|\alpha_{row,col}\|$, где $row = \{h_1,h_2,h_3,h_4\}$ и $col = \{pro,contra,undef,\eta_r,p(h_r')\}$ общий вид которой приведен в табл. 1.

Таблица 1.

Матрица исходных оценок гипотез

	pro	***contra***	***undef***	$\boldsymbol{\eta_r}$	$\boldsymbol{p(h_r')}$
h_1	ϱ_1	ϵ_1	υ_1	η_1	$p(h_1')$
h_2	ϱ_2	ϵ_2	υ_2	η_2	$p(h_2')$
h_3	ϱ_3	ϵ_3	υ_3	η_3	$p(h_3')$
h_4	ϱ_4	ϵ_4	υ_4	η_4	$p(h_4')$

Выбор текущего или «активного» состояния отношения агента из $R = \{Lr,Dr,Ir,Ur\}$ определяется через максимизацию результатов комплексного оценивания η_r, а в случае их равенства – через минимизацию $p(h_r')$:

$$\beta R\gamma = q_\gamma = \min_{p(h_r')} \max_{\eta_r} \|\alpha_{row,col}\| \quad (11)$$

Масштабирование доверия агента

Выражение (11) позволяет описать состояние отношения агента β с отдельным респондентом γ как $q_\gamma[\![\eta_r,P_\gamma^\beta]\!]$, где $P_\gamma^\beta = 1 - p(h_r')$, $r \in R$. Если в качестве примера агента взять веб-портал, то число респондентов может составлять несколько тысяч и полной характеристикой агента с точки зрения ИБ будет вектор состояний отношений агента со всеми его респондентами Q_β^γ с учетом рекурсии (4). Таким образом, можно говорить о необходимости «горизонтального» масштабирования результатов предыдущего раздела с целью оптимизации размера вектора Q_β^γ состояний отношений агента.

Во второй части статьи [13] было показано, что каждый агент содержит в своем составе как минимум одну точку доступа. Точка доступа представляет из себя набор предопределенных на этапе разработки логических протоколов и правил обработки входящих данных поступающих через фиксированные открытые TCP и UDP порты, различные сокеты, каналы и т.п. Можно утверждать, что главное свойство точки доступа – это безотказность приема входящих данных. Вернемся к примеру с веб-порталом, когда все клиенты используют единую точку доступа соответствующего агента. Здесь необходимо сделать следующее допущение.

D3. С учетом развития современных ИС можно говорить о наличии следующих особенностей присущих агенту:

- отдельные объекты из состава агента могут имеет внутренний список пользователей;
- списки пользователей отдельных объектов могут различаться вплоть до полного несовпадения;
- на объектах и в целом в рамках агента управление доступом осуществляется на основе ролевого доступа и его модификаций;
- точка доступа агента по своему входу индифферентна по отношению к клиентам.

Как показано во второй [13] и третьей [14] частях настоящей работы, точки доступа агента представляют из себя сочетания объектов (ИП и ИР). Именно такие ИП и ИР формируют и являются носителями подмножества M^{α} событий и сообщений, отвечающие на вопросы «кто, где, когда» и позволяющих идентифицировать клиента на уровне объектов (см. [14], раздел «Формализация исходных данных»). Возвращаясь к примеру веб-портала отметим, что идентификацию клиентов осуществляет (как правило) веб-сервер и при этом его доступ к клиентским данным в базе данных портала идет от ограниченного круга ее пользователей. Что можно отобразить в виде следующей схемы:

$$\underbrace{IdClient \longrightarrow Role\,(IdClient)}_{HTTP\ server} \longrightarrow$$
$$\longrightarrow \underbrace{UserDB(Role) \longrightarrow DataDB(IdClient)}_{Data\ Base}$$

Отметим, что выражение $DataDB(IdClient)$ означает, что идентификатор клиента является одним из индексов базы данных обеспечивающих обработку требуемой информации. Выражение «$IdClient \longrightarrow$» как раз и является аналогом точки доступа агента. Сделаем следующее утверждение.

Утверждение 5. Каждая из точек доступа агента эквивалентна одному из его респондентов, что позволяет принять число респондентов агента равным числу его точек доступа.

Для доказательства утверждения приведем следующие рассуждения.

Обозначим: QR – ИР, QS – ИП, D^{in} – входные данные, D^{out} – выходные данные, а D^*, M^* – промежуточные данные и сопутствующие события и сообщения агента. Тогда схему работы агента в рамках текущего подхода можно представить следующим образом:

$$D^{in} \longrightarrow QS_1\,(D^{in},M^{\alpha}) \longrightarrow QR_1\,(D^{in},M^{\alpha}) \longrightarrow QS_i\,(D^*,M^*) \longrightarrow$$
$$\longrightarrow QR_i\,(D^*,M^*) \longrightarrow \cdots \longrightarrow QR_s\,(D^*,M^*) \longrightarrow D^{out} \quad (12)$$

Компонент $D^{in} \longrightarrow QS_1\,(D^{in},M^{\alpha}) \longrightarrow QR_1\,(D^{in},M^{\alpha})$ выражения (12) описывает реакцию агента на поступающие данные или «$IdClient \longrightarrow$». Отметим, что именно через этот компонент возможно деструктивное воздействие и именно здесь в ответ на деструктивные действия одного из клиентов, агент может принять только такие меры противодействия, которые отразятся на параметрах работоспособности всей точки доступа, а значит на всех клиентах. Вопросы, связанные с такими действиями, как выборочная фильтрация клиентов или их запросов, на данном этапе рассматривать не будем, поскольку обычно эти действия (например, функции межсетевого экрана или файервола веб-приложений) выполняет другой агент в ИС. Таким образом, объекты QS_1 и QR_1 фактически образуют точку доступа агента, что и требовалось доказать.

Компонент $QR_s\,(D^*,M^*) \longrightarrow D^{out}$ выражения (12) можно рассматривать в виде цели внешнего воздействия со стороны нарушителя, который получает требуемый доступ к определенным данным агента или получает возможность манипулировать выходными данными агента, то есть воздействовать на другие агенты ИС.

Компонент $QR_i\,(D^*,M^*) \longrightarrow QR_s\,(D^*,M^*)$ выражения (12) представляет собой промежуточные объекты из состава агента участвующие в обработке входящих данных. Представляется очевидным, что все перечисленные типы компонент могут быть представлены в виде непересекающихся между собой подмножеств LC, CC и RC множества объектов из состава агента $K = LC \cup CC \cup RC$, которые взаимодействуют между собой по мере развития внешнего воздействия со стороны нарушителя. Тогда выражение (12) можно представить в виде $LC \longrightarrow CC \longrightarrow \cdots \longrightarrow CC \longrightarrow RC$, что дает основания положить, что все объекты агента могут быть упорядочены при проведении процедуры комплексного оценивания.

В качестве промежуточного вывода отметим, что выражение (12) дает основание для введения следующих типов агентов в многоагентной системе по их отношению к данным D^{out}:

1. Конечный агент – если с точки зрения нарушителя соответствующий ИР является конечной целью его действий с точки зрения нарушения конфиденциальности, целостности и доступности данных D^{out}. То есть можно полагать, что на этом ИР возможна остановка атаки.
2. Поддерживающий агент – если с точки зрения нарушителя данные D^{out} агента являются предметом манипуляции в соответствующем выходном ИП для воздействия на респондентов. То есть можно полагать, что ИР и ИП агента используются для развития атаки.

Исследования механизмов комплексного оценивания показывают, что наиболее значимые критерии должны включаться в эту процедуру на завершающих этапах. Тогда можно положить следующий порядок (слева на право) комплексного оценивания объектов на уровне подмножеств $CC \bowtie RC \bowtie LC$. При этом подмножество LC следует рассматривать как состоящее из отдельных непересекающихся подмножеств АР, каждое из которых представляет собой отдельную точку доступа $LC = \{AP_1,\cdots, AP_l\}$, где l – число точек доступа агента.

Далее сделаем следующие допущения с точки зрения ИБ.

D4. В силу наличия общесистемных вызовов, дающих общую поверхность атак для всех объектов, а также повторного использования кода, результат комплексного оценивания η_r^{CC} объектов из подмножества CC и получаемая в итоге матрица AQ_{CC}

является общей для всех объектов из состава подмножеств LC и RC.

D5. По результатам анализа известных атак, выполненных компаниями в области ИБ, целевые объекты из RC как правило могут быть достигнуты из любой точки доступа, что дает основания результаты комплексного оценивания η_r^{RC} объектов из подмножества RC и получаемую в итоге матрицу AQ_{RC} полагать общими для всех объектов из состава подмножеств LC.

Поскольку точки доступа агента LC эквивалентны его респондентам, то для определения состояния отношений агента $q_\gamma[\![\eta_r,P_\gamma^\beta]\!]$ достаточно последовательно использовать элементы матриц AQ_{CC} и AQ_{RC} при проведении процедуры комплексного оценивания (в силу ее аддитивности) по объектам каждого из подмножеств $AP_i \in LC$:

$$CC \bowtie RC \bowtie AP_i \qquad (13)$$

В результате вычисления (13) получаем вектор состояний отношений агента с его респондентами $Q_\beta^\gamma = [q_1,\cdots,q_\kappa]$, где $\kappa = |LC|$ – число точек доступа данного агента β.

Предлагаемое «горизонтальное» масштабирование позволяет сократить вычислительную нагрузку при определении состояния отношений агента за счет однократного вычисления матриц AQ_{CC} и AQ_{RC} для последующего применения в выражении (13) для каждой из точек доступа.

Упорядочивание объектов из состава агента будем выполнять раздельно на основании следующих рассуждений. Предыдущие статьи цикла показывают, что состояния, принимаемое объектом в результате внешнего воздействия, описываются комбинациями порождаемых этим воздействием событий. То есть, в самом общем виде можно проводить аналогию с термодинамическим определением энтропии. Описанное ранее [15] определение доверия состояния объекта, основанное на сравнении матрицы свертки событий с текущим их набором, позволяет полагать наличие неопределенности в самом факте сравнения. То есть, равномерность заполнения ячеек матрицы свертки событий с одной стороны повышает вероятность совпадения эталонного и текущего наборов событий, но с другой стороны снижает значимость такого совпадения. На основании изложенного сделаем следующее допущение.

D6. Чем более неравномерно по количеству содержание ячеек матрицы сравнения, тем значительнее результат совпадения эталонного и текущего наборов событий.

Поскольку процедура комплексного оценивания выполняется раздельно для каждого из состояний объекта и для каждого из этих состояний существует своя матрица свертки событий, то, неравномерность заполнения ячеек матрицы свертки событий можно рассматривать как основу для построения соответствующего индекса упорядочивания объектов при комплексном оценивании. В качестве такого индекса будем использовать энтропийный индекс неравенства Тейла. Для наших целей индекс запишем в следующем виде:

$$I_k^r = \frac{1}{N}\sum_{i\in N}\frac{Y_i}{X}\ln\frac{Y_i}{X} \qquad (14),$$

где: $a_{row,col}$ – число значений в ячейке матрицы свертки событий; $Y = \sum_{row}\sum_{col} a_{row,col}$ – сумма всех значений ячеек отдельной матрицы; $N = row \times col$ – число ячеек матрицы свертки; $X = \sum_{i\in N} Y_i / N$ – среднее значение по всем ячейкам; $k \in K$ – индексируемый объект; $r \in R$ – индексируемое состояние объекта.

Таким образом, каждая матрица свертки событий, описывающая состояние объекта, в свою очередь описывается индексом (14), что позволяет строить порядок применения объектов агента как параметров комплексного оценивания по возрастанию индекса для каждого из подмножеств $K = \langle LC,\le_{I_k^r}\rangle \cup \langle CC,\le_{I_k^r}\rangle \cup \langle RC,\le_{I_k^r}\rangle$.

Необходимо отметить две важные особенности предлагаемого подхода.

1. Построение индекса неравенства осуществляется по эталонным наборам событий и, следовательно, может быть выполнено заранее – на этапе разработки или внедрения агента в состав ИС.
2. В ячейках матрицы свертки событий располагаются значения для признака *SI*, которые в соответствии с принятыми в ИБ подходами соответствуют операции типа Запись, Чтение, вызывающие изменения Конфиденциальности, Целостности, Доступности для носителя информации (см. [14], раздел «Формализация исходных данных»), что дает возможность углубленной оценки при проведении комплексного оценивания.

Для дальнейших расчетов переопределим вектор $Q_\beta^\gamma = [q_1,\cdots,q_\gamma,\cdots,q_\kappa]$, $\kappa = |LC|$ состояний отношений агента за счет добавления значений из столбцов матрицы исходных оценок гипотез состояний агента AQ (табл.1). Как отмечалось в начале раздела, выражение (11) обеспечивает выбор строки матрицы на основе представления состояния отношения агента β с отдельным респондентом γ, как $q_\gamma[\![\eta_r,P_\gamma^\beta]\!]$, где $P_\gamma^\beta = 1 - p(h_r')$, $r \in R$. Это позволяет описать состояние отношения с отдельным респондентом в виде: $q_\gamma[\![\varrho_r,\epsilon_r,\upsilon_r,\eta_r,P_\gamma^\beta]\!]$. Фактически полное описание состояний отношений агента со всеми респондентами будет представлять из себя матрицу состояний отношений относительно точек доступа $Q_\beta^{LC} = \|q_{row,col}\|$, где $row \in LC$ и $col = \{pro,contra,undef,\eta_r,P_\gamma^\beta\}$.

Рассмотрение работы ИС с точки зрения различных уровней прав доступа аккаунтов может трактоваться как процедура укрупнения агентов. Согласно определению агента ИБ, приведенному в первом разделе настоящей статьи, ведущим свойством агента является наличие у него прав доступа, что подразумевает вхождение объектов (ИП и ИР) из состава агента с меньшими правами доступа в состав агента с большими правами доступа. Таким образом, возникает проблема определения интегрального уровня доверия при объединении нескольких агентов в один при рассмотрении их работы в ИС с точки зрения аккаунта с повышенными правами доступа.

Обозначим интегрального агента с повышенными правами доступа как CA, множество интегрируемых агентов как $A = \{a_1,\cdots,a_n\}$, где n – число интегрируемых агентов, которое определяется правами доступа соответствующего аккаунта.

Прежде всего отметим, что в состав агента CA будут входить все объекты, образующие каждого из агентов множества A. Но помимо этих объектов CA будет содержать некоторое количество объектов (ИП и ИР), которые в силу прав доступа не входят состав любого агента из A. Обозначим множество таких объектов K^+, и представим их как нового агента, обозначаемого a_+.

Будем полагать, что для объектов из K^+ определены как матрицы сверток событий, так и уровни доверия отношений к внешним воздействиям, а также необходимые индексы неравенства. Соответственно, по результатам выполнения процедуры комплексного оценивания получим описание отдельного агента $a_+[\![Q_+^{LC}]\!]$. Тогда интегральный агент с повышенными правами доступа описывается как: $CA[\![A,a_+]\!]$.

Поскольку агент a_+ обладает повышенными правами доступа, то необходимо учесть его влияние на всех интегрируемых агентов. Сделаем следующее утверждение.

Утверждение 6. При объединении агентов с меньшими правами доступа в интегральный агент с более высокими правами доступа вопросами взаимодействия интегрируемых агентов можно пренебречь.

Доказательство утверждения основывается на *Аксиоме 7*, *Утверждениях 1*, *5* и допущениях *D3*–*D5*.

Утверждение 6 и предыдущие разделы статьи позволяют утверждать, что для оценки влияния агента a_+ на остальных агентов в рамках рассматриваемого аккаунта, достаточно выполнить процедуру комплексного оценивания:

$$\forall a_i \, q_\gamma = a_i \bowtie a_+ \qquad (15)$$

Рассмотрим процедуру комплексного оценивания на уровне агентов (15) подробнее. В общем случае величины Q_+^{LC} *и* Q_i^{LC} содержат для каждой из строк значение η_r, которое фактически является входным значением для матрицы свертки рангов (3). В силу более высоких прав доступа агента a_+ будем полагать, что все строки row_+ матрицы Q_+^{LC} влияют на каждую из строк row_i матрицы Q_i^{LC} агента a_i. Это означает, что для каждой row_i строится дерево матриц свертки рангов и порядок свертки рангов для всех строк row_i определяется соответствующим индексом неравенства I_+^r, определяемого для агента a_+ в соответствии с (14). по результатам процедуры комплексного оценивания на уровне агентов будут пересчитаны оценки отдельных состояний отношений агентов из A с их респондентами, а также соответствующие уровни доверия.

Отметим, что расчеты для агента a_+ выполняются однократно и затем используются в (15) для всех агентов из A, что, в частности, обеспечивает хорошее распараллеливание операций комплексного оценивания.

Выражения (11–15) дают основание утверждать, что в результате последовательной интеграции агентов по мере повышения их прав доступа, на каждом уровне интеграции агент $CA[\![A,a_+]\!]$ будет содержать число точек доступа $LC_+ = \cup_{i=[1,|A|]} LC_i$ не меньшее, чем сумма точек доступа интегрируемых агентов. При этом изменение уровня доверия состояния агента $a_i \in A$ будет влиять только на соответствующие точки доступа $AP_i \in LC$ данного агента, в то время как изменение уровня доверия отношения агента a_+ будет влиять на все точки доступа LC_+ агента CA.

Материалы текущего раздела позволяют сформулировать следующую гипотезу о структуре многоагентной системы с точки зрения ИБ.

Представление ИС в виде многоагентной системы предполагает наличие внутренней структуры агентов определяемой структурой прав доступа пользователей данной ИС таким образом, что изменение уровней доверия у агента выше лежащего уровня влияет на все ниже лежащие агенты из состава ИС.

Заключение

В рамках общей цели исследования (адаптации логико-вероятностного метода для решения задач ИБ) в статье разработаны формально-логические основы определения вероятностных оценок состояний отношений агентов в многоагентных системах как результат обработки событий и сообщений, формируемых в процессе функционирования агента. Данные вероятностные оценки закладывают основы для последующего применения логико-вероятностного метода при рассмотрении вопросов защиты информации в многоагентных системах. Предлагаемые механизмы количественного и качественного оценивания состояния отношений агентов позволяют получать агрегированные результаты для подсистем современных ИС.

Литература

1. *Рябинин И. А. Решение одной задачи оценки надежности структурно-сложной системы разными логико-вероятностными методами / И. А. Рябинин, А. В. Струков // Моделирование и анализ безопасности и риска в сложных системах, Санкт-Петербург, 19–21 июня 2019 года. – Санкт-Петербург: Санкт-Петербургский государственный университет аэрокосмического приборостроения, 2019. – С. 159–172.*
2. *Демин А. В. Глубокое обучение адаптивных систем управления на основе логико-вероятностного подхода / А. В. Демин // Известия Иркутского государственного университета. Серия: Математика. – 2021. – Т. 38. – С. 65–83.*
3. *Викторова В. С. Вычисление показателей надежности в немонотонных логико-вероятностных моделях многоуровневых систем / В. С. Викторова, А. С. Степанянц // Автоматика и телемеханика. – 2021. – № 5. – С. 106–123.*
4. *Леонтьев А. С. Математические модели оценки показателей надежности для исследования вероятностно-временных характеристик многомашинных комплексов с учетом отказов / А. С. Леонтьев, М. С. Тимошкин // Международный научно-исследовательский журнал. – 2023. – № 1(127). С. 1–13.*
5. *Пучкова Ф. Ю. Логико-вероятностный метод и его практическое использование / Ф. Ю. Пучкова // Информационные технологии в процессе подготовки современного специалиста: Межвузовский сборник научных трудов / Министерство просвещения Российской Федерации; Федеральное государственное бюджетное образовательное учреждение высшего образования «Липецкий государственный педагогический университет имени П. П. Семенова-Тян-Шанского». Том Выпуск 25. – Липецк: Липецкий государственный педагогический университет имени П.П . Семенова-Тян-Шанского, 2021. – С. 187–193.*
6. *Россихина Л. В. О применении логико-вероятностного метода И. А. Рябинина для анализа рисков информационной безопасности / Л. В. Россихина, О. О. Губенко, М. А. Черноситова // Актуальные проблемы деятельности подразделений УИС: Сборник материалов Всероссийской научно-практической конференции, Воронеж, 20 октября 2022 года. – Воронеж: Издательско-полиграфический центр «Научная книга», 2022. – С. 108–109.*
7. *Карпов А. В. Модель канала утечки информации на объекте информатизации / А. В. Карпов // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018): VII Международная научно-техническая и научно-методическая конференция. Сборник научных статей. В 4-х томах, Санкт-Петербург, 28 февраля – 01 марта 2018 года / Под редакцией С. В. Бачевского. Том 2. – Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, 2018. – С. 378–382.*
8. *Методика кибернетической устойчивости в условиях воздействия таргетированных кибернетических атак / Д. А. Иванов, М. А. Коцыняк, О. С. Лаута, И. Р. Муртазин // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018): VII Международная научно-техническая и научно-методическая конференция. Сборник научных статей. В 4-х томах, Санкт-Петербург, 28 февраля – 01 марта 2018 года / Под редакцией С. В. Бачевского. Том 2. – Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, 2018. – С. 343–346.*
9. *Елисеев Н. И. Оценка уровня защищенности автоматизированных информационных систем юридически значимого электронного документооборота на основе логико-вероятностного метода / Н. И. Елисеев, Д. И. Тали, А. А. Облаженко // Вопросы кибербезопасности. – 2019. – № 6(34). – С. 7–16.*
10. *Коцыняк М. А. Математическая модель таргетированной компьютерной атаки / М. А. Коцыняк, О. С. Лаута, Д. А. Иванов // Наукоемкие технологии в космических исследованиях Земли. – 2019. – Т. 11, № 2. – С. 73–81.*
11. *Белякова Т. В. Функциональная модель процесса воздействия целевой компьютерной атаки / Т. В. Белякова, Н. В. Сидоров, М. А. Гудков // Радиолокация, навигация, связь: Сборник трудов XXV Международной научно-технической конференции, посвященной 160-летию со дня рождения А. С. Попова. В 6 томах, Воронеж, 16–18 апреля 2019 года. Том 2. – Воронеж: Воронежский государственный университет, 2019. – С. 108–111.*
12. *Калашников А. О. Применение логико-вероятностного метода в информационной безопасности (Часть 1) / А. О. Калашников, К. А. Бугайский, Д. С. Бирин, Б. О. Дерябин, С. О. Цепенда, К. В. Табаков // Вопросы кибербезопасности. – 2023. – № 4 (56). – С. 23–32.*
13. *Калашников А. О. Применение логико-вероятностного метода в информационной безопасности (Часть 2) / А. О. Калашников, К. А. Бугайский, Е. И. Аникина, И. С. Перескоков, Ан. О. Петров, Ал. О. Петров, Е. С. Храмченкова, А. А. Молотов // Вопросы кибербезопасности. – 2023. – № 5 (57). – С. 113–127.*
14. *Калашников А. О. Применение логико-вероятностного метода в информационной безопасности (Часть 3) / А. О. Калашников, К. А. Бугайский, Е. И. Аникина, И. С. Перескоков, Ан. О. Петров, Ал. О. Петров, Е. С. Храмченкова, А. А. Молотов // Вопросы кибербезопасности. – 2023. – № 6 (58). – С. 20–34.*
15. *Калашников А. О. Применение логико-вероятностного метода в информационной безопасности (Часть 4) / А. О. Калашников, Е. В Аникина, К. А. Бугайский, Д. С. Бирин, Б. О. Дерябин, С. О. Цепенда, К. В. Табаков // Вопросы кибербезопасности. – 2024. – № 3 (61). – С. 23–32.*
16. *Бугайский К. А. Расширенная модель открытых систем (Часть 1) / К. А. Бугайский, Д. С. Бирин, Б. О. Дерябин, С. О. Цепенда // Информация и безопасность. – 2022. – Т. 25, № 2. – С. 169–178.*
17. *Бугайский К. А. Расширенная модель открытых систем (Часть 2) / К. А. Бугайский, И. С. Перескоков, А. О. Петров, А. О. Петров // Информация и безопасность. – 2022. – Т. 25, № 3. – С. 321–330.*
18. *Бугайский К. А. Расширенная модель открытых систем (Часть 3) / К. А. Бугайский, Б. О. Дерябин, К. В. Табаков, Е. С. Храмченкова, С. О. Цепенда // Информация и безопасность. – 2022. – Т. 25, № 4. – С. 501–512.*
19. *Калашников А. О. Модель количественного оценивания агента сложной сети в условиях неполной информированности / А. О. Калашников, К. А. Бугайский // Вопросы кибербезопасности. – 2021. – № 6 (46). – С. 26–35.*
20. *Калашников А. О. Методика оценки возможности реализации информационных угроз / А. О. Калашников, К. А. Бугайский // Информация и безопасность. – 2020. Т. 23, № 2. С. 163–178.*
21. *Бугайский К. А. Определение успешности действий нарушителя в однородной среде / К. А. Бугайский // Проблемы управления безопасностью сложных систем: Материалы XXIX международной научно-практической конференции, Москва, 15 декабря 2021 года. – Москва: Институт проблем управления им. В. А. Трапезникова РАН, 2021. – С. 227–232.*

22. Калашников А. О. Модель оценки безопасности сложной сети. (часть 1) / А. О. Калашников, К. А. Бугайский // Вопросы кибербезопасности. – 2022. – № 4 (50). – С. 26–38.
23. Калашников А. О. Модель оценки безопасности сложной сети (Часть 2) / А. О. Калашников, К. А. Бугайский, А. А. Молотов // Вопросы кибербезопасности. – 2022. – № 5 (51). – С. 47–60.
24. Бурков В. Н. Идентификация механизмов комплексного оценивания на основе унитарного кода / В. Н. Бурков, В. А. Сергеев, Н. А. Коргин // Управление большими системами: сборник трудов. – 2020. – № 87. – С. 67–85.
25. Бурков В. Н. Проблемы синтеза механизма комплексного оценивания на основе обучающего набора данных / В. Н. Бурков, Н. А. Коргин, О. Л. Марин // XIII Всероссийское совещание по проблемам управления ВСПУ-2019: Сборник трудов XIII Всероссийского совещания по проблемам управления ВСПУ-2019, Москва, 17–20 июня 2019 года / Институт проблем управления им. В. А. Трапезникова РАН. – Москва: Институт проблем управления им. В. А. Трапезникова РАН, 2019. – С. 2280–2284.
26. Бурков В. Н. Метод синтеза системы комплексного оценивания / В. Н. Бурков, И. В. Буркова, А. В. Щепкин // Вестник Южно-Уральского государственного университета. Серия: Компьютерные технологии, управление, радиоэлектроника. – 2020. – Т. 20, № 4. – С. 63–73.
27. Сергеев В. А. Синтез механизмов комплексного оценивания на основе разделительной декомпозиции / В. А. Сергеев // Проблемы управления. – 2022. – № 6. – С. 3–13.
28. Казакова Е. А. Автоматизированное построение матричных процедур комплексного оценивания на основе оптимизационного подхода / Е. А. Казакова, П. Н. Курочка, А. И. Половинкина // Вестник Воронежского государственного технического университета. – 2010. – Т. 6, № 10. – С. 140–146.

References

1. Rjabinin I. A. Reshenie odnoj zadachi ocenki nadezhnosti strukturno-slozhnoj sistemy raznymi logiko-verojatnostnymi metodami / I. A. Rjabinin, A. V. Strukov // Modelirovanie i analiz bezopasnosti i riska v slozhnyh sistemah, Sankt-Peterburg, 19–21 ijunja 2019 goda. – Sankt-Peterburg: Sankt-Peterburgskij gosudarstvennyj universitet ajerokosmicheskogo priborostroenija, 2019. – S. 159–172.
2. Demin A. V. Glubokoe obuchenie adaptivnyh sistem upravlenija na osnove logiko-verojatnostnogo podhoda / A.V. Demin // Izvestija Irkutskogo gosudarstvennogo universiteta. Serija: Matematika. – 2021. – T. 38. – S. 65–83.
3. Viktorova V. S. Vychislenie pokazatelej nadezhnosti v nemonotonnyh logiko-verojatnostnyh modeljah mnogourovnevyh sistem / V. S. Viktorova, A. S. Stepanjanc // Avtomatika i telemehanika. – 2021. – № 5. – S. 106–123.
4. Leont'ev A. S. Matematicheskie modeli ocenki pokazatelej nadezhnosti dlja issledovanija verojatnostno-vremennyh harakteristik mnogomashinnyh kompleksov s uchetom otkazov / A. S. Leont'ev, M. S. Timoshkin // Mezhdunarodnyj nauchno-issledovatel'skij zhurnal. – 2023. – № 1(127). S. 1–13.
5. Puchkova F. Ju. Logiko-verojatnostnyj metod i ego prakticheskoe ispol'zovanie / F. Ju. Puchkova // Informacionnye tehnologii v processe podgotovki sovremennogo specialista: Mezhvuzovskij sbornik nauchnyh trudov / Ministerstvo prosveshhenija Rossijskoj Federacii; Federal'noe gosudarstvennoe bjudzhetnoe obrazovatel'noe uchrezhdenie vysshego obrazovanija «Lipeckij gosudarstvennyj pedagogicheskij universitet imeni P.P. Semenova-Tjan-Shanskogo». Tom Vypusk 25. – Lipeck: Lipeckij gosudarstvennyj pedagogicheskij universitet imeni P.P. Semenova-Tjan-Shanskogo, 2021. – S. 187–193.
6. Rossihina L. V. O primenenii logiko-verojatnostnogo metoda I.A. Rjabinina dlja analiza riskov informacionnoj bezopasnosti / L. V. Rossihina, O. O. Gubenko, M. A. Chernositova // Aktual'nye problemy dejatel'nosti podrazdelenij UIS: Sbornik materialov Vserossijskoj nauchno-prakticheskoj konferencii, Voronezh, 20 oktjabrja 2022 goda. – Voronezh: Izdatel'sko-poligraficheskij centr «Nauchnaja kniga», 2022. – S. 108–109.
7. Karpov A. V. Model' kanala utechki informacii na ob#ekte informatizacii / A. V. Karpov // Aktual'nye problemy infotelekommunikacij v nauke i obrazovanii (APINO 2018): VII Mezhdunarodnaja nauchno-tehnicheskaja i nauchno-metodicheskaja konferencija. Sbornik nauchnyh statej. V 4-h tomah, Sankt-Peterburg, 28 fevralja – 01 marta 2018 goda / Pod redakciej S. V. Bachevskogo. Tom 2. – Sankt-Peterburg: Sankt-Peterburgskij gosudarstvennyj universitet telekommunikacij im. prof. M. A. Bonch-Bruevicha, 2018. – S. 378–382.
8. Metodika kiberneticheskoj ustojchivosti v uslovijah vozdejstvija targetirovannyh kiberneticheskih atak / D. A. Ivanov, M. A. Kocynjak, O. S. Lauta, I. R. Murtazin // Aktual'nye problemy infotelekommunikacij v nauke i obrazovanii (APINO 2018): VII Mezhdunarodnaja nauchno-tehnicheskaja i nauchno-metodicheskaja konferencija. Sbornik nauchnyh statej. V 4-h tomah, Sankt-Peterburg, 28 fevralja – 01 marta 2018 goda / Pod redakciej S.V. Bachevskogo. Tom 2. – Sankt-Peterburg: Sankt-Peterburgskij gosudarstvennyj universitet telekommunikacij im. prof. M.A. Bonch-Bruevicha, 2018. – S. 343–346.
9. Eliseev N. I. Ocenka urovnja zashhishhennosti avtomatizirovannyh informacionnyh sistem juridicheski znachimogo jelektronnogo dokumentooborota na osnove logiko-verojatnostnogo metoda / N. I. Eliseev, D. I. Tali, A. A. Oblanenko // Voprosy kiberbezopasnosti. – 2019. – № 6(34). – S. 7–16.
10. Kocynjak M. A. Matematicheskaja model' targetirovannoj komp'juternoj ataki / M. A. Kocynjak, O. S. Lauta, D. A. Ivanov // Naukoemkie tehnologii v kosmicheskih issledovanijah Zemli. – 2019. – T. 11, № 2. – S. 73–81.
11. Beljakova T. V. Funkcional'naja model' processa vozdejstvija celevoj komp'juternoj ataki / T. V. Beljakova, N. V. Sidorov, M. A. Gudkov // Radiolokacija, navigacija, svjaz': Sbornik trudov XXV Mezhdunarodnoj nauchno-tehnicheskoj konferencii, posvjashhennoj 160-letiju so dnja rozhdenija A. S. Popova. V 6 tomah, Voronezh, 16–18 aprelja 2019 goda. Tom 2. – Voronezh: Voronezhskij gosudarstvennyj universitet, 2019. – S. 108–111.
12. Kalashnikov A. O. Primenenie logiko-verojatnostnogo metoda v informacionnoj bezopasnosti (Chast' 1) / A. O. Kalashnikov, K. A. Bugajskij, D. S. Birin, B. O. Derjabin, S. O. Cependa, K. V. Tabakov // Voprosy kiberbezopasnosti. – 2023. – № 4 (56). – S. 23–32.
13. Kalashnikov A. O. Primenenie logiko-verojatnostnogo metoda v informacionnoj bezopasnosti (Chast' 2) / A. O. Kalashnikov, K. A. Bugajskij, E. I. Anikina, I. S. Pereskokov, An. O. Petrov, Al. O. Petrov, E. S. Hramchenkova, A. A. Molotov // Voprosy kiberbezopasnosti. – 2023. – № 5 (57). – S. 113–127.
14. Kalashnikov A. O. Primenenie logiko-verojatnostnogo metoda v informacionnoj bezopasnosti (Chast' 3) / A. O. Kalashnikov, K. A. Bugajskij, E. I. Anikina, I. S. Pereskokov, An. O. Petrov, Al. O. Petrov, E. S. Hramchenkova, A. A. Molotov // Voprosy kiberbezopasnosti. – 2023. – № 6 (58). – S. 20–34.

15. *Kalashnikov A. O. Primenenie logiko-verojatnostnogo metoda v informacionnoj bezopasnosti (Chast' 4) / A. O. Kalashnikov, E. V Anikina, K. A. Bugajskij, D. S. Birin, B. O. Derjabin, S. O. Cependa, K. V. Tabakov // Voprosy kiberbezopasnosti. – 2024. – № 3 (61). – S. 23–32.*
16. *Bugajskij K. A. Rasshirennaja model' otkrytyh sistem (Chast' 1) / K. A. Bugajskij, D. S. Birin, B. O. Derjabin, S. O. Cependa // Informacija i bezopasnost'. – 2022. – T. 25, № 2. – S. 169–178.*
17. *Bugajskij K. A. Rasshirennaja model' otkrytyh sistem (Chast' 2) / K. A. Bugajskij, I. S. Pereskokov, A. O. Petrov, A. O. Petrov // Informacija i bezopasnost'. – 2022. – T. 25, № 3. – S. 321–330.*
18. *Bugajskij K. A. Rasshirennaja model' otkrytyh sistem (Chast' 3) / K. A. Bugajskij, B. O. Derjabin, K. V. Tabakov, E. S. Hramchenkova, S. O. Cependa // Informacija i bezopasnost'. – 2022. – T. 25, № 4. – S. 501–512.*
19. *Kalashnikov A. O. Model' kolichestvennogo ocenivanija agenta slozhnoj seti v uslovijah nepolnoj informirovannosti / A. O. Kalashnikov, K. A. Bugajskij // Voprosy kiberbezopasnosti. – 2021. – № 6 (46). – S. 26–35.*
20. *Kalashnikov A. O. Metodika ocenki vozmozhnosti realizacii informacionnyh ugroz / A. O. Kalashnikov, K. A. Bugajskij // Informacija i bezopasnost'. – 2020. T. 23, № 2. S. 163–178.*
21. *Bugajskij K. A. Opredelenie uspeshnosti dejstvij narushitelja v odnorodnoj srede / K. A. Bugajskij // Problemy upravlenija bezopasnost'ju slozhnyh sistem: Materialy XXIX mezhdunarodnoj nauchno-prakticheskoj konferencii, Moskva, 15 dekabrja 2021 goda. – Moskva: Institut problem upravlenija im. V. A. Trapeznikova RAN, 2021. – S. 227–232.*
22. *Kalashnikov A. O. Model' ocenki bezopasnosti slozhnoj seti. (chast' 1) / A. O. Kalashnikov, K. A. Bugajskij // Voprosy kiberbezopasnosti. – 2022. – № 4 (50). – S. 26–38.*
23. *Kalashnikov A. O. Model' ocenki bezopasnosti slozhnoj seti (Chast' 2) / A. O. Kalashnikov, K. A. Bugajskij, A. A. Molotov // Voprosy kiberbezopasnosti. – 2022. – № 5 (51). – S. 47–60.*
24. *Burkov V. N. Identifikacija mehanizmov kompleksnogo ocenivanija na osnove unitarnogo koda / V. N. Burkov, V. A. Sergeev, N. A. Korgin // Upravlenie bol'shimi sistemami: sbornik trudov. – 2020. – № 87. – S. 67–85.*
25. *Burkov V. N. Problemy sinteza mehanizma kompleksnogo ocenivanija na osnove obuchajushhego nabora dannyh / V. N. Burkov, N. A. Korgin, O. L. Marin // XIII Vserossijskoe soveshhanie po problemam upravlenija VSPU-2019: Sbornik trudov XIII Vserossijskogo soveshhanija po problemam upravlenija VSPU-2019, Moskva, 17–20 ijunja 2019 goda / Institut problem upravlenija im. V. A. Trapeznikova RAN. – Moskva: Institut problem upravlenija im. V.A. Trapeznikova RAN, 2019. – S. 2280–2284.*
26. *Burkov V. N. Metod sinteza sistemy kompleksnogo ocenivanija / V. N. Burkov, I. V. Burkova, A. V. Shhepkin // Vestnik Juzhno-Ural'skogo gosudarstvennogo universiteta. Serija: Komp'juternye tehnologii, upravlenie, radiojelektronika. – 2020. – T. 20, № 4. – S. 63–73.*
27. *Sergeev V. A. Sintez mehanizmov kompleksnogo ocenivanija na osnove razdelitel'noj dekompozicii / V. A. Sergeev // Problemy upravlenija. – 2022. – № 6. – S. 3–13.*
28. *Kazakova E. A. Avtomatizirovannoe postroenie matrichnyh procedur kompleksnogo ocenivanija na osnove optimizacionnogo podhoda / E. A. Kazakova, P. N. Kurochka, A. I. Polovinkina // Vestnik Voronezhskogo gosudarstvennogo tehnicheskogo universiteta. – 2010. – T. 6, № 10. – S. 140–146.*

ОБЕСПЕЧЕНИЕ СОВМЕСТИМОСТИ ТЕХНИЧЕСКИХ КОМПОНЕНТОВ ПРИ СОЗДАНИИ СИСТЕМЫ МОНИТОРИНГА ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Девицына С. Н.[1], Пилькевич П. В.[2]

DOI: 10.21681/2311-3456-2024-4-38-44

Цель исследования: *создание прототипа системы мониторинга инцидентов информационной безопасности типа pre-commit на рабочих станциях разработчиков программного обеспечения для внедрения DevSecOps в процесс разработки технических продуктов.*

Методы исследования: *анализ способов модернизации исходного кода компонентов системы мониторинга, синтез системы мониторинга инцидентов информационной безопасности, имитационное моделирование инцидентов информационной безопасности, обрабатываемых системой мониторинга, эксперимент.*

Результаты исследования. *В работе предложено решение по обеспечению защищенности разрабатываемого программного обеспечения в рамках методологии DevSecOps. Приведено описание процесса редактирования исходного кода для обеспечения совместимости программного модуля gitleaks и Filebeat при создании системы мониторинга инцидентов информационной безопасности. Показано, что процессы создания программного продукта должны проводиться параллельно с процедурами обеспечения безопасности исходного кода. В результате получен прототип многокомпонентной системы мониторинга инцидентов типа pre-commit, обнаруживающей и предоставляющей статистику по событиям, связанным с оставлением критической информации внутри произвольного исходного кода. Апробация работы и оценка эффективности системы мониторинга реализована на основе имитационного моделирования и эксперимента. Доказана работоспособность и эффективность системы мониторинга, в рамках эксперимента сделано нагрузочное тестирование в формате отправки большого потока инцидентов в систему с целью проверки корректности обработки каждого из них, и исключения потери инцидентов из-за большой нагрузки на сеть и технические модули. В результате исследования и моделирования предложен эффективный прототип системы мониторинга инцидентов информационной безопасности, который может быть использован отечественными компаниями-разработчиками для обеспечения и повышения эффективности кибербезопасности объектов информатизации с учетом требований импортозамещения.*

Новизна: *впервые предложено использовать систему мониторинга для исследования инцидентов DevSecOps с автоматизированным поиском уязвимостей в анализируемом исходном коде.*

Ключевые слова: *информационная безопасность, кибербезопасность, SIEM-системы, системы мониторинга, инциденты информационной безопасности, Opensearch, DevSecOps, безопасность программного обеспечения, импортозамещение.*

METHOD FOR ENSURING COMPATIBILITY OF TECHNICAL COMPONENTS WHEN CREATING A SYSTEM FOR MONITORING INFORMATION SECURITY INCIDENTS

Devitsyna S. N.[3], Pilkevich P. V.[4],

The purpose of the research *is to create a prototype of a pre-commit information security incident monitoring system at software developers' workstations to implement DevSecOps in the process of developing technical products.*

Research methods: *analysis of ways to modernize the source code of the monitoring system components, synthesis of the information security incident monitoring system, simulation modeling of information security incidents processed by the monitoring system, experiment.*

1 Девицына Светлана Николаевна, кандидат технических наук, доцент, ФГАОУ ВО «Севастопольский государственный университет», Севастополь, Россия. E-mail: sndevitsyna@sevsu.ru, ORCHID 0009-0009-1647-6701

2 Пилькевич Павел Вадимович, студент, ФГАОУ ВО «Севастопольский государственный университет», Севастополь, Россия. E-mail: pavel.piksel2012@mail.ru

3 Svetlana N. Devitsyna, PhD., Associate Professor, Sevastopol State University, Sevastopol, Russia. E-mail: sndevitsyna@sevsu.ru, ORCHID 0009-0009-1647-6701

4 Pavel V. Pilkevich, student, Sevastopol State University, Sevastopol, Russia. E-mail: pavel.piksel2012@mail.ru

Results of the study. *The paper proposes a solution to ensure the security of the developed software within the framework of the DevSecOps methodology. The article describes the process of editing the source code to ensure the compatibility of the gitleaks and Filebeat software modules when creating an information security incident monitoring system. It is shown that the processes of creating a software product should be carried out in parallel with the procedures for ensuring the security of the source code. As a result, a prototype of a multi-component pre-commit incident monitoring system that detects and provides statistics on events related to the retention of critical information within arbitrary source code. Approbation of the work and assessment of the effectiveness of the monitoring system was implemented on the basis of simulation modeling and experiment. The operability and efficiency of the monitoring system were proved, as part of the experiment, load testing was carried out in the format of sending a large stream of incidents to the system in order to check the correctness of processing each of them, and exclude the loss of incidents due to a heavy load on the network and technical modules. As a result of the research and modeling, an effective prototype of an information security incident monitoring system is proposed, which can be used by domestic development companies to ensure and improve the efficiency of cybersecurity of informatization objects, taking into account the requirements of import substitution.*

Novelty: *for the first time, it is proposed to use a monitoring system to investigate DevSecOps incidents with an automated search for vulnerabilities in the analyzed source code.*

Keywords: *information security, cybersecurity, SIEM systems, monitoring systems, information security incidents, Opensearch, DevSecOps, software security, import substitution.*

Введение

Реализация сквозных цифровых технологий заключается во внедрении ИБ-решений в процесс автоматизации технологических процессов сборки, настройки и развёртывания разрабатываемого ПО (DevSecOps), при этом методология создания безопасного продукта заключается в совместной работе команд информационной безопасности с командами, непосредственно разрабатывающими приложения. Наиболее перспективным стеком технологий для создания систем мониторинга на данный момент является совокупность технических средств Opensearch, Opensearch Dashboards, Logstash, Filebeat и gitleaks. Это обусловлено возможностью реализации требования по импортозамещению вследствие открытого исходного кода каждого из технических компонентов. Однако, существует проблема: не предусмотрено возможности корректного взаимодействия между модулями gitleaks и Filebeat, что создаёт трудности в объединении данных средств и делает невозможным создание системы мониторинга в текущий момент [1].

Целью работы является обеспечение совместимости программного модуля gitleaks и Filebeat при создании системы мониторинга инцидентов информационной безопасности.

Проблема модернизации исходного кода компонентов системы мониторинга

Для выбора решения проведен анализ актуальных научных работ и исследований по данной тематике. В работе Степанова Я. В. и др. [1] рассмотрены теоретическое основы создания собственного Центра обеспечения безопасности (SOC) на основе стека ELK и классификации MITRE. Авторами предлагается openssource стек ELK. Предлагается построить все процессы SOC на основе классификации MITRE, подобрать квалифицированный персонал и при помощи стека ELK эффективно реализовывать сбор и анализ больших данных в реальных проектах. Машанов В. В. [6] рассматривает важность проверки git-репозиториев на утечки и уязвимости для обеспечения безопасности проекта и конфиденциальности данных. Описывает несколько инструментов, таких как Gitrob, GitLeaks, TruffleHog и GitGuardian, которые помогают обнаружить и исправить проблемы безопасности в git-репозиториях. Каждый инструмент обладает своими особенностями. Работа содержит полезную информацию для разработчиков, которые заинтересованы в обеспечении безопасности своих проектов. Вместе с тем, никто из авторов не предлагает использовать систему мониторинга для исследования инцидентов DevSecOps с автоматизированным поиском уязвимостей в анализируемом исходном коде.

Предлагаемый подход

В ходе анализа особенностей функционирования системы мониторинга выявлено, что программная утилита для обнаружения оставленной конфиденциальной информации в произвольном исходном коде записывает результаты своей работы в файл формата JSON. Определён способ получения информации от gitleaks путём считывания данного файла указанного формата средствами сборщика данных Filebeat, у которого, в свою очередь, имеется специальный конфигурационный параметр для считывания информации именно в формате JSON [2]. Выяснилось, что ключевым различием между способом считывания средством Filebeat и способом записи средством gitleaks является то, что запись информации осуществляется блоками по соответствующим отчётам в один массив внутри файла, а считывания данных

предполагается построчное, причём в каждой строке должен находиться объект формата JSON. Такое различие приводит к успешной записи инцидентов в файл и неудачной попытке считывания этой информации сборщиком данных Filebeat, что не позволяет передать информацию об инцидентах оставления конфиденциальной информации в репозитории в Систему мониторинга данных инцидентов [3].

Для устранения выявленного несоответствия был изменён программный код внутри системной утилиты gitleaks, отвечающий за запись отчёта об обнаруженном инциденте с целью формирования постраничной записи отдельных объектов формата JSON в лог-файл для дальнейшего корректного считывания его сборщиком данных. Код представляет собой отдельную функцию для кодировки информации в формат JSON, на вход которой подаётся список со всеми отчётами обнаружения конфиденциальной информации в репозитории проекта. Ранее кодировка информации осуществлялась путём установки параметра отступа для повышения «читабельности» формируемых отчётов, и непосредственного разового преобразования всех отчётов в формат JSON [4]. Изменение кода представляет собой замену данного механизма на использование цикла, который берёт каждый отдельный сформированный отчёт и преобразовывает его в необходимый формат. Далее данные объекты постранично записываются в лог-файл[5].

Помимо этого, по умолчанию, с целью упрощения и ускорения работы с утилитой детектирования конфиденциальной информации в репозитории, существует возможность настройки автоматического запуска работы утилиты при выполнении определённых команд в репозитории. В разрабатываемой системе мониторинга это действие — коммит или же попытка записи изменений в репозиторий [5–7]. Для того, чтобы убрать необходимость загрузки всех файлов технического решения для обнаружения конфиденциальной информации в исходном коде, существует возможность указания специального параметра в своём репозитории, который ссылается на удалённый адрес к проекту утилиты gitleaks и, тем самым, производится автоматический запуск утилиты при попытке записи данных в репозиторий из адреса, зафиксированного в данной конфигурации (git hooks). Описанный механизм будет работать в том случае, если в папке проекта, который пытается автоматически запуститься, будет находиться другой конфигурационный файл[6,7,8] (.pre-commit-hooks.yaml). В этом файле будет указан идентификатор действия, необходимый для выполнения, и команда, запускающаяся автоматически с помощью git hooks. По умолчанию, такой конфигурационный файл с командой в gitleaks уже присутствует, однако, в нём указана команда, служащая лишь для демонстрации работы продукта, а запись обнаруженных утечек конфиденциальных данных нигде не остаётся, только демонстрируется пользователю, который совершает попытку фиксации изменений в своём репозитории[9].

Таким образом, для настройки автоматического запуска корректной команды при обращении к удалённому репозиторию изменённой утилиты gitleaks, была изменена команда, находящаяся в поле entry, которая указывает на необходимость включения полноценного режима обнаружения всех инцидентов утечки информационной безопасности по корневому адресу анализируемого репозитория с дальнейшей записью всех сформированных отчётов формата JSON в файл с фиксированным названием.

Обнаружение утечки конфиденциальной информации в произвольном репозитории средством gitleaks производится путём применения им конфигурируемых правил, создаваемых пользователями. Данные правила базируются на регулярных выражениях, которые, при совпадении со строками внутри исходного кода анализируемого продукта, формируют оповещение об обнаруженном инциденте информационной безопасности. Правила включают в себя [8, 9]:

- наименование правила, отображаемое в дальнейшем в сформированном отчёте в случае «срабатывания» данного правила;
- краткое описание правила, указывающего характер обнаруженной утечки;
- регулярное выражение (опционально), по которому осуществляется поиск совпадений с целью обнаружения инцидентов утечек конфиденциальной информации;
- значение степени важности обнаруженного инцидента;
- ключевые слова, по которым также осуществляется поиск внутри файлов с исходным кодом.

5 Программные инструменты обработки и визуализации данных. Elasticsearch, Logstash, Kibana, Grafana, Prometheus = Software tools for data processing and visualization. Elasticsearch, Logstash, Kibana, Grafana, Prometheus: учебное пособие / [И. В. Никифоров, О. А. Юсупова, Н. В. Воинов [и др.]; Санкт-Петербургский политехнический университет Петра Великого, Институт компьютерных наук и технологий, Высшая школа программной инженерии. — Санкт-Петербург: Политех-Пресс, 2023.

6 Ушаков, М. GitLab: локальный хостинг в стиле GitHub // Системный администратор. 2013. – №. 5. – С. 87–91.

7 Беккер, М. Я. и др. Использование цифровых сертификатов и протоколов SSL/TLS для шифрования данных при облачных вычислениях // Научно-технический вестник информационных технологий, механики и оптики. — 2011. – №. 4 (74). – С. 125–130.

8 Котенко, И. В., Кулешов, А. А., Ушаков, И. А. Система сбора, хранения и обработки информации и событий безопасности на основе средств Elastic Stack // Информатика и автоматизация. 2017. – Т. 5. – №. 54. – С. 5–34.

9 Шепелев, А. Н. и др. Анализ подходов и средств обработки сервисных журналов // Инженерный вестник Дона. – 2013. – Т. 27. – №. 4 (27). – С. 89.

Существует определённый набор правил, доступных по умолчанию, и возможность указания своих собственных правил в отдельном файле для настройки гибкого поиска всевозможных утечек информации, соответствующих требованиям безопасности предприятия. В случае автоматизированного удалённого обращения к репозиторию с утилитой gitleaks не представляется возможности передачи каким-либо эффективным и удобным способом пользовательских правил обнаружения инцидентов информационной безопасности. Следовательно, возникает необходимость редактирования уже имеющихся конфигураций с правилами безопасности с целью добавления туда своих собственных правил [10–13].

Конфигурация компонентов серверного блока системы мониторинга

Конфигурация поискового движка Opensearch включает в себя перечень параметров, отвечающих за имя сервиса, его адрес, настройки безопасности и иные специализированные настройки для кластера. В случае конфигурации конкретного прототипа, используются наиболее оптимальные с точки зрения технических мощностей и функциональных требований к продукту параметры:

- устанавливается имя кластера, который будет использоваться во всей системе мониторинга данным поисковым движком;
- указывается необходимость прослушивания всех имеющихся сетевых интерфейсов на наличие подключений к нему;
- включается режим блокирования в области памяти RAM с целью избежания критических неполадок, вызванных отсутствием памяти;
- включается использование пороговых значений для распределения узлов на диске;
- устанавливаются верхние и нижние пороги использования диска поисковым движком с целью оптимизации работы с памятью;
- разрешается использование демонстративных сертификатов для настройки тестового шифрования между узлами в системе;
- включается режим использования шифрования SSL при обмене информацией с поисковым движком;
- указываются пути для сертификатов шифрования как для транспортных путей, отвечающих за получение информации, так и для протокола http, необходимого для доступа к поисковому движку посредством средства визуализации Opensearch Dashboards;
- для ускорения работы отключается проверка имени хоста в транспортных соединениях.

Для корректной конфигурации средства визуализации информации Opensearch Dashboards необходимо указать параметры, отвечающие за имя сервиса, прослушиваемый адрес, настройки безопасности и иные специализированные параметры[10]. В конкретном случае развёртывания экспериментального демонстрационного прототипа системы мониторинга, были сконфигурированы следующие параметры:

- указывается имя запускаемого сервиса;
- включается прослушивание всех сетевых интерфейсов на прослушивание клиентских подключений к средству визуализации;
- указывается имя учётной записи, по которой осуществляется подключение к поисковому движку Opensearch;
- указывается пароль для учётной записи, используемой для подключения к поисковому движку Opensearch;
- включается полноценная поддержка шифрования SSL во всех сетевых соединениях как между клиентами, так и между средством визуализации и поисковым движком;
- указываются пути к файлам ключа и сертификата, которые задействуются в налаживании шифрования при сетевых соединениях между техническими продуктами.

Конфигурация компонентов клиентского блока системы мониторинга

Для обеспечения корректной работы всех технических составляющих клиентского блока системы мониторинга инцидентов типа pre-commit, необходимо осуществить конфигурацию утилиты git hooks. Данная утилита будет отвечать за автоматический вызов команды при попытке фиксации новых изменений исходного кода в репозитории для поиска оставленной конфиденциальной информации в данном репозитории путём задействования модернизированной утилиты gitleaks. Помимо данной операции конфигурирования, необходимо также наладить работу сборщика инцидентов с рабочих станций анализируемых пользователей (Filebeat). Это необходимо для получения и отправки сведений об инцидентах оставления конфиденциальной информации в серверную составляющую разрабатываемой системы мониторинга [14].

Для корректной работы утилиты git hooks был создан файл .pre-commit-hooks.yaml с содержимым, реализующим требуемое поведение при попытке пользователя занести новые изменения в репозиторий. Код содержит в себе адрес репозитория, к которому нужно обратиться при выполнении пользователем команды git commit, хэш-сумму конкретной

10 Календарев, А. Горизонтальное масштабирование. Проблемы и пути решения // Системный администратор. – 2014. – №. 10. – С. 54–62.

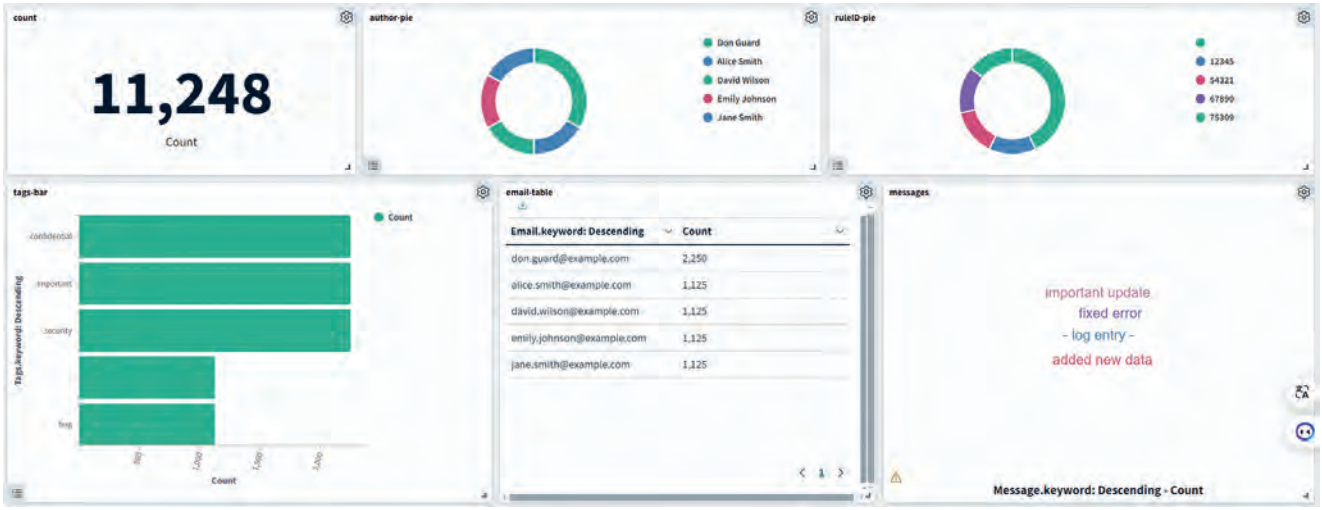


Рис. 1. Демонстрационный стенд, построенный в средстве визуализации Opensearch Dashboards

ветки удалённого репозитория gitleaks, содержащем изменения для обеспечения совместимости, а также идентификатор действия, по которому будет найдена команда, необходимая для выполнения в проекте утилиты gitleaks при запуске корректной команды поиска утечек конфиденциальной информации в анализируемом репозитории.

Для корректного функционирования сборщика данных Filebeat была создана специализированная конфигурация, соответствующая всем описанным требованиям для внедрения данного технического блока в состав разрабатываемой системы мониторинга и обеспечения бесперебойной связи клиентской составляющей с серверной составляющей. Конфигурация включает в себя параметры настройки разрешения системных вызовов процесса rseq с целью обеспечения бесперебойной работы сборщика данных и отсутствия конфликтов с нехваткой прав доступа к системным вызовам[11]. Отсутствие подобной настройки может вызывать отказ в запуске сборщика данных, что нарушит цепочку получения инцидентов с анализируемых рабочих станций пользователей. Помимо этого, добавлены четыре процессора, выполняющих следующие действия:

- добавление системной информации о хосте, на котором расположен Filebeat;
- добавление системной информации об облачном хранилище в случае, если Filebeat запущен на нём;
- добавление системной информации о контейнере docker в случае, если Filebeat запущен на нём;
- добавление системной информации о кластере Kubernetes в случае, если Filebeat развёрнут в рамках данного кластера.

11 Каменная, Е. В., Путилова, С. Е., Щербинина, И. А. Обзор современных подходов к обеспечению безопасности клиентской части веб-приложений // Транспортное дело России. – 2017. – №. 6. – С. 66–71.

Для полноценного функционирования разрабатываемой системы мониторинга произведено конфигурирование всех составляющих системы. В результате был получен пример полноценной и функционирующей системы мониторинга, и проведен анализ ее эффективности.

Проверка эффективности системы мониторинга

Смоделировав несколько различных вариантов инцидентов информационной безопасности, обрабатываемых системой мониторинга, было произведено нагрузочное тестирование, которое предполагало собой отправку большого потока инцидентов в систему с целью проверки корректности обработки каждого из инцидентов, и исключения потери инцидентов из-за большой нагрузки на сеть и технические модули разработанной системы мониторинга.

В средстве визуализации данных был создан демонстрационный стенд, показывающий информацию об общем количестве обнаруженных инцидентов. Стенд отражает: визуализацию соотношения количества событий относительно пользователей и идентификаторов сработанных правил gitleaks, график количества событий с агрегацией по тегам, таблицу электронных почт авторов коммитов, вызвавших инцидент информационной безопасности, перечень описаний коммитов, визуализацию количества событий относительно имени файлов, в которых был обнаружен инцидент (рис. 1).

Также имеются дополнительные информативные диаграммы, содержащие в себе агрегации по оставшимся полям инцидентов (рис. 2).

В ходе нагрузочного тестирования было подано 11 248 инцидентов, на демонстрационном стенде отображено такое же количество событий, что свидетельствует об отсутствии потерь событий. Выбранная

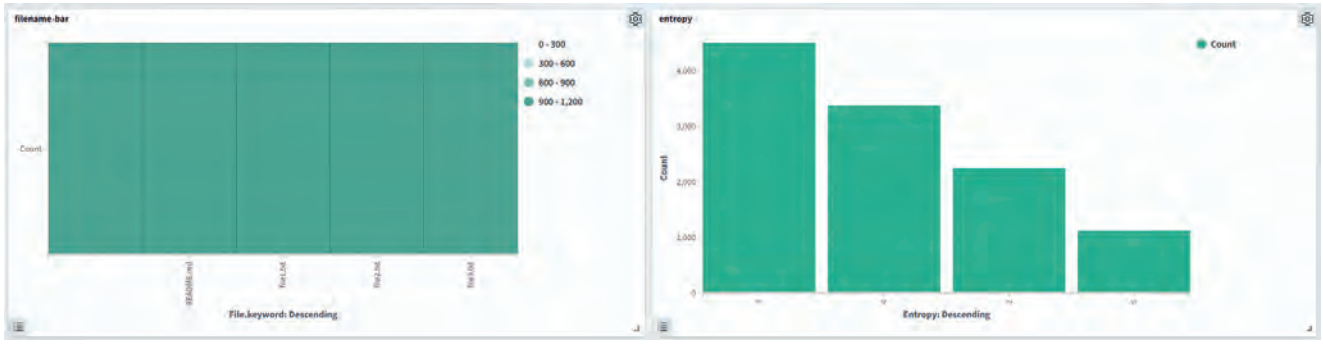


Рис. 2. Вспомогательная часть демонстрационного стенда, построенного в средстве визуализации Opensearch Dashboards

архитектура системы позволяет эффективно обнаруживать утечки разного типа и иные данные, соответствующие шаблонам поиска, в исходном коде произвольных проектов любых размеров.

Заключение

Для полноценного развёртывания системы мониторинга были внесены изменения в исходный код использующихся продуктов с целью обеспечения и улучшения совместимости продуктов друг с другом. Отредактирована система логирования инцидентов и изменены конфигурации запуска скриптов, проверяющих наличие утечек конфиденциальной информации в исходном коде проектов. Для полноценного функционирования разрабатываемой системы мониторинга произведено конфигурирование всех составляющих системы. В результате получен прототип полноценной и функционирующей системы мониторинга. Формирующиеся события содержат в себе максимально подробную информацию, доступную для визуализации в любом виде с целью досконального анализа и проведения подробного расследования инцидента. На основе имитационного моделирования была доказана эффективность прототипа системы, что позволяет внедрять её в промышленных масштабах отечественными компаниями-разработчиками. Практическая значимость заключается в разработке интеллектуального продукта на основе созданной архитектуры и востребованности подобного технического решения крупными отечественными ИТ-компаниями, заинтересованными в обеспечении кибербезопасности различных объектов информатизации, с учетом требований импортозамещения [15, 16].

Литература

1. *Степанов Я. В. и др. Создание собственного SOC при помощи классификации MITRE и Opensource стека ELK / Я. В. Степанов, Т. Н. Копышева, Т. В. Митрофанова, Т. Н. Смирнова // Информационные технологии в науке, управлении и образовании: междисциплинарный подход и тенденции развития: Сб. матер. Всероссийской научно-практической конференции (Димитровград, 12 ноября 2021 года). — Димитровград: Изд-во Димитровградского инженерно-технологического института — филиала федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский университет «МИФИ», 2021. С. 229—236.*
2. *Петров В. В., Брюханов, К. В., Авксентьева, Е. Ю. Сетевой мониторинг: анализ сетевого трафика с помощью ELK // Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки. 2020. №. 5. С. 102–105.*
3. *Еровлева Р. В., Еровлев, П. А. Мониторинг с помощью Micrometer, Prometheus и Grafana // Постулат. 2021. № 7.*
4. *Dhakal K. et al. Log Analysis and Anomaly Detection in Log Files with Natural Language Processing Techniques. — Appl. Sci. 2022, 12.*
5. *Шелепина О. Д., Хадорич Д. Д. Сравнительный анализ инструментов управления журналами на примере ELK и Graylog // Вызовы глобализации и развитие цифрового общества в условиях новой реальности: Сб. матер. IV Международной научно-практической конференции. Москва, 2022. – Изд-во: Алеф. 2022. С. 137–141.*
6. *Машанов В. В. Как обезопасить git-репозитории: обзор инструментов для обнаружения утечек и уязвимостей // Актуальные вопросы современной науки: сборник статей. – Изд-во: Наука и Просвещение (ИП Гуляев Г.Ю.). 2023. С. 53–56.*
7. *Вахрамов С. В. и др. Использование prettier и git hooks для автоматического поддержания культуры кода в typescript-проекте // Научное обозрение. Технические науки. 2020. №. 4. С. 24–28.*
8. *Сарнавский А. П. Разработка инструмента управления уязвимостями на основе Elasticsearch: выпускная квалификационная работа бакалавра: направление 10.03.01 «Информационная безопасность»; образовательная программа 10.03.01_03 «Безопасность компьютерных систем». 2022.*
9. *Симанков В. С., Петрова В. А. Мониторинг информационной безопасности в интеллектуальном ситуационном центре // Поведенческие теории и практика российской науки. 2021. С. 29–35.*
10. *Коптева А. В., Князев И. В. Анализ проблемы преобразования данных формата JSON в строго типизированных языках программирования на примере Golang // Проблемы науки. 2021. №. 7 (66). С. 5.*
11. *Кутузов К. О. Программирование RESTful приложений на языке программирования Golang // Молодость. Интеллект. Инициатива. 2021. С. 23–24.*

12. Разумков И. А. Автоматизация поиска уязвимостей в программах на языке Golang: выпускная квалификационная работа бакалавра: направление 10.03.01 «Информационная безопасность»; образовательная программа 10.03.01_03 «Безопасность компьютерных систем». 2023.
13. Палаш Б. В., Голубничий А. А. Основные способы обеспечения безопасности клиент-серверных приложений // Modern Science. 2020. №. 2-1. С. 383–385.
14. Черников А. С. и др. Обзор применения подхода микросервисной архитектуры при проектировании клиентской части веб-приложения //Дневник науки. 2020. №. 4. С. 31.
15. Девицына С. Н., Пилькевич П. В., Удод Е. В. Способы улучшения защищённости сервисов, использующих JWT-токены // Экономика. Информатика. 2023. Т. 50. №1. С. 144–151.
16. Адгемов И. Э., Девицына С. Н. Управление безопасностью беспроводной локальной вычислительной сети // Экономика. Информатика. 2023. Т. 50. № 1. С. 183–190.

References

1. Stepanov Ja. V. i dr. Sozdanie sobstvennogo SOC pri pomoshhi klassifikacii MITRE i Opensource steka ELK / Ja. V. Stepanov, T. N. Kopysheva, T. V. Mitrofanova, T. N. Smirnova // Informacionnye tehnologii v nauke, upravlenii i obrazovanii: mezhdisciplinarnyj podhod i tendencii razvitija: Sb. mater. Vserossijskoj nauchno-prakticheskoj konferencii (Dimitrovgrad, 12 nojabrja 2021 goda). — Dimitrovgrad: Izd-vo Dimitrovgradskogo inzhenerno-tehnologicheskogo instituta — filiala federal'nogo gosudarstvennogo avtonomnogo obrazovatel'nogo uchrezhdenija vysshego obrazovanija "Nacional'nyj issledovatel'skij universitet «MIFI», 2021. S. 229—236.
2. Petrov V. V., Brjuhanov, K. V., Avksent'eva, E. Ju. Setevoj monitoring: analiz setevogo trafika s pomoshh'ju ELK // Sovremennaja nauka: aktual'nye problemy teorii i praktiki. Serija: Estestvennye i tehnicheskie nauki. 2020. №. 5. S. 102–105.
3. Erovleva R. V., Erovlev, P. A. Monitoring s pomoshh'ju Micrometer, Prometheus i Grafana // Postulat. 2021. № 7.
4. Dhakal K. et al. Log Analysis and Anomaly Detection in Log Files with Natural Language Processing Techniques. — Appl. Sci. 2022, 12.
5. Shelepina O. D., Hadorich D. D. Sravnitel'nyj analiz instrumentov upravlenija zhurnalami na primere ELK i Graylog // Vyzovy globalizacii i razvitie cifrovogo obshhestva v uslovijah novoj real'nosti: Sb. mater. IV Mezhdunarodnoj nauchno-prakticheskoj konferencii. Moskva, 2022. – Izd-vo: Alef. 2022. S. 137–141.
6. Mashanov V. V. Kak obezopasit' git-repozitorii: obzor instrumentov dlja obnaruzhenija utechek i ujazvimostej // Aktual'nye voprosy sovremennoj nauki: sbornik statej. — Izd-vo: Nauka i Prosveshhenie (IP Guljaev G.Ju.). 2023. S. 53–56.
7. Vahramov S. V. i dr. Ispol'zovanie prettier i git hooks dlja avtomaticheskogo podderzhanija kul'tury koda v typescript-proekte // Nauchnoe obozrenie. Tehnicheskie nauki. 2020. №. 4. S. 24–28.
8. Sarnavskij A. P. Razrabotka instrumenta upravlenija ujazvimostjami na osnove Elasticsearch: vypusknaja kvalifikacionnaja rabota bakalavra: napravlenie 10.03.01 «Informacionnaja bezopasnost'»; obrazovatel'naja programma 10.03.01_03 «Bezopasnost' komp'juternyh sistem». 2022.
9. Simankov V. S., Petrova V. A. Monitoring informacionnoj bezopasnosti v intellektual'nom situacionnom centre // Povedencheskie teorii i praktika rossijskoj nauki. 2021. S. 29–35.
10. Kopteva A. V., Knjazev I. V. Analiz problemy preobrazovanija dannyh formata JSON v strogo tipizirovannyh jazykah programmirovanija na primere Golang // Problemy nauki. 2021. №. 7 (66). S. 5.
11. Kutuzov K. O. Programmirovanie RESTful prilozhenij na jazyke programmirovanija Golang // Molodost'. Intellekt. Iniciativa. 2021. S. 23–24.
12. Razumkov I. A. Avtomatizacija poiska ujazvimostej v programmah na jazyke Golang: vypusknaja kvalifikacionnaja rabota bakalavra: napravlenie 10.03.01 «Informacionnaja bezopasnost'»; obrazovatel'naja programma 10.03.01_03 «Bezopasnost' komp'juternyh sistem». 2023.
13. Palash B. V., Golubnichij A. A. Osnovnye sposoby obespechenija bezopasnosti klient-servernyh prilozhenij // Modern Science. 2020. №. 2-1. S. 383–385.
14. Chernikov A. S. i dr. Obzor primenenija podhoda mikroservisnoj arhitektury pri proektirovanii klientskoj chasti veb-prilozhenija // Dnevnik nauki. 2020. №. 4. S. 31.
15. Devicyna S. N., Pil'kevich P. V., Udod E. V. Sposoby uluchshenija zashhishhjonnosti servisov, ispol'zujushhih JWT-tokeny // Jekonomika. Informatika. 2023. T. 50. №1. S. 144–151.
16. Adgemov I. Je., Devicyna S. N. Upravlenie bezopasnost'ju besprovodnoj lokal'noj vychislitel'noj seti // Jekonomika. Informatika. 2023. T. 50. № 1. S. 183–190.

АНАЛИЗ ТРЕБОВАНИЙ ПРИМЕНЕНИЯ И ТЕХНОЛОГИЧЕСКИХ ВОЗМОЖНОСТЕЙ РАДИОСИГНАЛОВ, ПЕРСПЕКТИВНЫХ ДЛЯ СЕТЕЙ 6G

Барабошин А. Ю.[1], Лучин Д. В.[2], Маслов Е. Н.[3]

DOI: 10.21681/2311-3456-2024-4-45-56

Цель исследования: *Исследовать технологические возможности различных сигнальных конструкций (СК) радиосигналов для выявления типов, способных наиболее полно обеспечить функциональность систем связи 6G.*

Методы исследования: *Системный анализ параметров перспективных вариантов СК в направлении обеспечения расширенной мобильной широкополосной связи (eMBB), сверхнадежной связи с ультрамалыми задержками (URLLC) и массовой связи межмашинного типа (mMTC), эффективных по показателям уровня внеполосных излучений (OOBE), пик-фактора (PAPR), совместимости с MIMO, при обеспечении высокоскоростной передачи данных множественного доступа и одновременного сканирования стохастического радиоканала с частотно-временным рассеянием (ISAC/DFRC).*

Полученные результаты: *Определена технологичность СК, как способность наиболее полно обеспечить установленные показатели качества и требуемые сценарии связи, при максимальной унификации структуры сигнала и алгоритмов его обработки. Предложена методология исследования технологических возможностей СК с точки зрения эффективности их применения в 6G. Получены оценки и классифицированы технологические возможности различных вариантов СК с множественной несущей типа OFDM и с одной несущей (SC), включая СК типа DFT-s-OFDM. Показано, что сигнал множественной несущей технологии CP-OFDM имеет высокие показатели OOBE и PAPR, а способы улучшения этих параметров не технологичны, поскольку реализуются посредством сложных и специфических технических решений. Показано, что сигнал одиночной широкополосной несущей технологии DFT-s-OFDM по определению обладает низким показателем PAPR и посредством процедуры спектрального прекодирования обеспечивает гибкость программного управления параметрами сигнальной конструкции сообразно различным сценариям связи в системах 6G, использующих типовые приемопередатчики DFT-s-OFDM.*

Научная новизна: *Согласно предложенной методологии исследования технологических возможностей СК, получен вывод о том, что по критериям установленных требований, технологичность использования в перспективных сетях 6G СК типа CP-OFDM уступает технологичности применения СК типа DFT-s-OFDM, обладающей, благодаря SDR-процедуре спектрального прекодирования, гибкостью адаптации унифицированной структуры сигнала к широкому спектру применений по требуемым сценариям связи.*

Ключевые слова: *Функционал и требования 6G, технологичность сигнальной конструкции, сравнение технологичности применения в 6G CP-OFDM и DFT-s-OFDM.*

ANALYSIS REQUIREMENTS OF APPLICATION AND TECHNOLOGICAL CAPABILITIES OF RADIO SIGNALS, PROMISING FOR 6G NETWORKS

Baraboshin A. Y.[4], Luchin D. V.[5], Maslov E. N.[6]

Purpose of the study: *To investigate the technological capabilities of various signal constructions (SC) of radio signals in order to identify the types that can most fully provide functionality of 6G communication systems.*

Research methods: *System analysis of the parameters of promising SC options in the direction of providing enhanced Mobile Broadband (eMBB), Ultra-reliable Low-Latency Communication (URLLC) and massive Machine Type of Communication (mMTC) in terms of minimization Out-of-Band Emission (OOBE), Peak-to-Average Power Ratio (PAPR), compatibility ensuring*

1 Барабошин Андрей Юрьевич, кандидат технических наук, начальник лаборатории филиала ФГБУ НИИР – СОНИИР, г. Самара, Россия. E-mail: bay@soniir.ru
2 Лучин Дмитрий Вячеславович, кандидат технических наук, директор научно-технического центра филиала ФГБУ НИИР – СОНИИР, г. Самара, Россия. E-mail: dmyl@soniir.ru
3 Маслов Евгений Николаевич, кандидат технических наук, ведущий научный сотрудник филиала ФГБУ НИИР – СОНИИР, г. Самара, Россия. E-mail: maslov@soniir.ru

4 Andrey Yu. Baraboshin, Ph.D., Head of the Laboratory of the Branch of the Federal State Budgetary Institution NIIR – SONIIR, Samara, Russia. E-mail: bay@soniir.ru
5 Dmitry V. Luchin, Ph.D., Director of the Scientific and Technical Center of the Branch of FSBI NIIR – SONIIR, Samara, Russia. E-mail: dmyl@soniir.ru
6 Evgeny N. Maslov, Ph.D., Leading Researcher of the Branch of the Federal State Budgetary Institution NIIR – SONIIR, Samara, Russia. E-mail: maslov@soniir.ru

with MIMO, taking into account the need to provide high-speed data transmission of multiple access and simultaneous sensing/radaring stochastic of radio channel with time-frequency dispersing (ISAC/DFRC).

Results obtained: *The technologicalability of the SC is defined as the ability to most fully ensure the established quality indicators and the required communication scenarios, with maximum unification of the signal structure and algorithms for its processing. A methodology for researching the technological capabilities of SC in terms of the effectiveness of their application in 6G is proposed. Estimates have been obtained and the technological capabilities of various variants of SC with multiple carrier type OFDM and with single carrier (SC), including SC type DFT-s-OFDM, have been classified. It is shown that the signal of the CP-OFDM multiple carrier technology has high OOBE and PAPR values, and the ways to improve these parameters are not technologicalability, since they are implemented through difficult and specific technical solutions. It is shown that the signal of a single broadband carrier technology DFT-s-OFDM, by definition, has a low PAPR index and, through the spectral precoding procedure, provides flexibility to software control of the parameters of the signal structure in accordance with various communication scenarios in 6G systems using typical transmitters DFT-s-OFDM.*

Scientific novelty: *According to the proposed methodology for studying the technological capabilities of SC, it was concluded that, in accordance with the criteria of established requirements in promising 6G networks, the technologicalability of using SC CP-OFDM is inferior to the technologicalability of using SC DFT-s-OFDM, which, thanks to the procedure of spectral preliminary coding, has the flexibility of adapting (SDR) its unified structure to a wide range of application, accoding to the required communication scenarios.*

Keywords: *Functional and requirements of 6G, technologicalability of signal constructions, comparison technologicalability's of application in 6G CP-OFDM and DFT-s-OFDM.*

Введение

Планируется, что технологической основой информационной базы эффективной цифровой экономики России будут сети беспроводной связи шестого поколения (6G). Для конструктивного обеспечения разработок устройств телекоммуникаций и систем указанных сетей необходимо детальное исследование проблем и особенностей их построения. В первую очередь, разработчики оборудования должны быть обеспечены рекомендациями и стандартами, определяющими структуру рабочего радиосигнала указанной сети, в полной мере отвечающего условиям и задачам её функционирования. Таким образом, анализ технологических возможностей радиосигналов, перспективных для применения в сетях 6G, представляет собой научную задачу, актуальную для формирования практических рекомендаций по созданию сигнальной базы отечественной системы беспроводной связи указанного поколения.

Постановка цели исследования

Целью проведенного анализа являлось исследование технологических возможностей различных сигнальных конструкций (СК) – комбинаций способов модуляционного и помехоустойчивого кодирования радиосигналов для выявления типов, способных наиболее полно обеспечить функциональность системы связи 6G.

Методология исследования

Современные реалии характеризуются появлением новых пользовательских приложений, таких как видео высокой четкости, мультимедиа с эффектом присутствия и т.п., основанных на применении расширенной мобильной широкополосной связи (eMBB). Также наблюдается смещение тренда информационного обслуживания в сторону обеспечения интернета вещей (NB-IoT) и всеобъемлющего интернета (IoE), – т.е. в направлении организации автоматического обмена данными роботов (D2D) и беспилотных транспортных средств (V2X) [1].

Соответственно потребностям новых приложений, консорциум 3GPP (The 3rd Generation Partnership Project), начав в 2015 году в рамках ITU (International Telecommunication Union)[7] продвижение спецификаций проектов 5G/6G NR, определил следующие основные направления применения радиосигналов указанной системы:

- ❖ расширенная мобильная широкополосная связь (eMBB);
- ❖ сверхнадежная связь с низкой задержкой (URLLC);
- ❖ массовая связь межмашинного типа (mMTC).

Также стандартами консорциума 3GPP, несмотря на принципиальные различия технических характеристик обслуживаемых приложений, для унификации и удешевления используемого оборудования отмечалась целесообразность обеспечения совместимости технологий формирования сигналов действующих в настоящее время (3G HSPA/UMTS, 4G LTE/VoLTE) и перспективных систем беспроводной связи (5G/6G NR). Заметим, что в настоящее время стандарты 3GPP по системам 6G NR находятся в стадии разработки.

Эффективность работы указанных выше приложений критически зависит от пропускной способности канала связи и требует от перспективных типов

7 International Telecommunication Union (ITU). IMT Vision – Framework and Overall Objectives of the Future Development of IMT for 2020 and Beyond. – Geneva, Switzerland. : ITU-R, 2015. – p. 21.

радиосигналов обеспечения передачи данных на сверхвысоких скоростях и при критически ультрамалых задержках.

По определению указанные свойства радиосигнала, в первую очередь обеспечиваются выбором диапазона рабочих частот. В дополнение к диапазону миллиметровых длин волн [2], 6G впервые будет использовать терагерцовый (ТГц) диапазон или даже видимый свет, обеспечивающие использование сверхширокой полосы пропускания сигналов, превышающей десятки ГГц. Благодаря этому сеть 6G будет обладать беспрецедентной скоростью беспроводной передачи данных (до десятков Тбит/с) с ультрамалыми задержками.

Однако указанные диапазоны частот рабочих волн имеют известные особенности характеристик распространения сигналов [3], включая наличие селективных замираний или деградации некоторых областей полосы частот рабочего диапазона, снижающие эффективность работающих в этих условиях радиосистем и затрудняющие их реализацию.

Соответственно установленным задачам и условиям определим параметры СК радиосигнала, имеющие принципиально важное значение для его применения в сети 6G.

Оценивая технологические возможности перспективных типов радиосигналов, в первую очередь необходимо отметить их способность гибко адаптироваться к стохастическим изменениям радиоканала и противостоять деструктивному воздействию мультипликативных искажений, аддитивных шумов и помех.

Для организации принципиально необходимого для обеспечения указанной адаптации сканирования канала связи и одновременной передачи по каналу информационных данных, желательно использовать один и тот же сигнал (ISAC/DFRC).

Форма сигнала и схема модуляции должны обеспечивать надежную работу системы в условиях канала с частотно-временным рассеянием (многолучевость, эффект Допплера).

Для обеспечения требуемой скорости и минимизации задержки передачи данных должны быть достигнуты высокие показатели спектральной эффективности и скорости обработки сигнала[8], в том числе за счет низкой вычислительной сложности алгоритмов обработки.

Новые формы сигналов должны обеспечивать хорошую совместимость с технологией системы много входов – много выходов (MIMO), являющейся эффективным средством повышения скорости передачи данных в ограниченной полосе, т.е. создающей возможность использования запаса пропускной способности, как для повышения устойчивости связи в условиях стохастического радиоканала со множеством препятствий и помех, так и для организации множественного доступа.

Для обеспечения высокой спектральной плотности каналов большого числа разнообразных потребителей, СК должна обладать низким уровнем побочных, внеполосных излучений (OOBE).

Для обеспечения высокой энергоэффективности канального сигнала, пригодного для применения в недорогих передающих устройствах с простыми усилителями мощности, обладающими существенной нелинейностью и ограниченным энергоресурсом, структура СК должна иметь низкий показатель пик-фактора (PAPR).

При этом желательно, чтобы СК имела унифицированную структуру для нисходящего, восходящего и прямого каналов.

Таким образом, установлено, что вследствие достаточной противоречивости выявленных требований, возможно не существует варианта СК, обеспечивающего их одновременное выполнение. Однако, возможен поиск её настраиваемой структуры, обеспечивающей в широком спектре вариантов использования, включая eMBB, mMTC и URLLC, достаточный компромисс, например, между требованиями спектральной и энергетической эффективности и т.п.

Предваряя анализ, отметим, что решение задачи оценки скорости и соответствующей задержки передачи данных в зависимости от ширины рабочей полосы частот радиоканала используемого диапазона, является общеизвестным. Поэтому далее, на этом аспекте анализа и оценки перспективных типов радиосигналов останавливаться не будем, также как и на оценке влияния на величину задержки передачи данных скорости работы вычислительных средств, используемых для реализации алгоритмов обработки. Основное внимание уделим вопросам анализа аспектов технологии модуляции и формирования перспективного радиосигнала. При этом под технологичностью СК будем понимать её способность наиболее полно обеспечить установленные показатели качества и требуемые сценарии связи при максимальной унификации структуры сигнала и алгоритмов его обработки.

Результаты исследования сигналов множественной несущей

Партнерский проект 3GPP преемственно предполагает использование в 5G/6G NR многочастотного сигнала множественной несущей, полученного посредством ортогонального мультиплексирования

8 3rd Generation Partnership Project (3GPP). Study on requirements for NR beyond 52.6 GHz. Technical Report (TR) 38.807, Jan. 2020, version 16.0.0. https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3522.

с частотным разделением и циклическим префиксом (CP-OFDM)[9]:

$$\hat{d}(n \cdot T_0 / N) = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} D_k \cdot e^{j2\pi \frac{k}{N} n},\ n \in [1,N], \qquad (1)$$

где: N – размерность обратного дискретного преобразования Фурье (ОДПФ); $\{D_k\}_{k=0}^{N-1}$ – «частотные» представления комплексных символов данных PSK/QAM модуляции; $e^{j2\pi \frac{k}{N} n}$ – частотный фактор k-го коэффициента Фурье для символа D_k; $T_0 = 1 / (f_{k+1} - f_k)$ – интервал ортогональности сигналов N поднесущих множественной несущей; $n \cdot T_0/N = t_n$ – моменты котельниковских отсчетов.

После завершения формирования согласно (1) отсчетов информационного сигнала на интервале ортогональности T_0, на каждом такте сигнала CP-OFDM формирование отсчетов полного символьного интервала $T_c = T_o + T_{зи}$ завершается генерацией L отсчетов сигнала активного защитного интервала (циклического префикса) $T_{зи} = L \cdot T_o/N$, по правилам:

$$\hat{d}(t_n) = \hat{d}(t_n - T_o), \text{ или } \hat{d}(t_n) = -\hat{d}(t_n - T_o),$$
$$\text{для } t_n = n \cdot T_o/N \text{ и } n \in [N+1, N+L].$$

Введение CP обеспечивает противодействие СК межсимвольной интерференции (ISI), порожденной каналом с рассеянием.

Согласно представленной структуре, CP-OFDM сигнал обладает высокой спектральной эффективностью и за счет введения CP обладает необходимыми корреляционными свойствами, используемыми для синхронизации и когерентного фазирования процесса передачи данных, а также для организации сканирования и адаптивной коррекции канала. Отметим, что для повышения качества сканирования и коррекции в состав СК CP-OFDM могут быть введены пилот-сигналы, ортогональные сигналам информационных поднесущих и существенно упрощающие реализацию указанных функций сканирования и частотно-фазовой коррекции канала.

Наконец, ортогональная структура СК CP-OFDM, за счет разделения каналов передачи данных, технологически, хорошо сочетается с процедурой частотно-временного кодирования и пространственной обработки сигнала согласно технологии MIMO.

Однако, такие недостатки сигнала CP-OFDM, как высокие показатели OOBE и PAPR, подвигают разработчиков на поиск решений, улучшающих указанные параметры. Рассмотрим процедуры таких решений подробнее.

Известно, что высокий показатель OOBE сигнала CP-OFDM является следствием наличия в нём резких межсимвольных переходов, обусловленных скачками фаз сигналов поднесущих при их модуляции и соответственно длинными «хвостами» спектральных представлений множественных поднесущих, ортогональных в нулях, но пульсирующих за пределами их группового прямоугольного спектра.

На (рис.1) классифицированы способы снижения показателя OOBE сигнала CP-OFDM.

Ограничение группового спектра сигнала CP-OFDM посредством фильтрации впервые использовалось в технологии LTE для улучшения параметров сигнала в режиме пакетной передачи данных.

Согласно процедурам фильтрации спектра F-OFDM[10] и универсальной фильтрации UFMC[11], для подавления внеполосного излучения применяются поддиапазоные фильтры, а согласно процедуре FBMC-OQAM[12] сигнал каждой поднесущей фильтруется индивидуально гребенчатым фильтром.

В отличие от схем частотной обработки спектра, процедуры оконной обработки осуществляются во временной области. В варианте W-OFDM[13] процедура свёртки сигнала с непрямоугольным окном применяется для сглаживания переходов между последовательными OFDM символами, а в варианте WCC-FBMC-OQAM[14] круговая (периодическая) свертка используется для удаления «хвостов» гребенчатой фильтрации.

В одном ряду с рассмотренными способами «сглаживания» модуляционных скачков находится также и способ управления непосредственно формой модулирующего импульса. Так, согласно процедуре NOFDM[15] осуществляется коррекция прямоугольной формы импульсов модуляции, а в варианте P-OFDM[16]

9 3rd Generation Partnership Project (3GPP). TS 38.211 V15.7.0. In Technical Specification Group Radio Access Network. Physical Channels and Modulation (Release 15). – Newport Beach, CA, USA, 2019.

10 Demir A.F., Elkourdi M., Ibrahim M., Arslan H. Waveform Design for 5G and Beyond. In 5G Networks. Fundamental Requirements, Enabling Technologies and Operations Management. – Hoboken, NJ, USA. : John Wiley&Sons Inc, 2018. – pp. 51–76;
Farhang-Boroujeny B., Moradi H. OFDM Inspired Waveforms for 5G // IEEE Commun. Surv. Tutor. – 2016, 18. – pp. 2474–2492;
Abdoli J., Jia M., Ma J. Filtered OFDM: A new waveform for future wireless systems // In Proc. 2015 IEEE 16th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC). – IEEE, 2015. – pp. 66–70;
Zhang X., Jia M., Chen L., Ma J., Qiu J. Filtered-OFDM-enabler for flexible waveform in the 5th generation cellular networks // In Proc. 2015 IEEE Global Communications Conference (GLOBECOM). – IEEE, 2015. – pp. 1–6.

11 Schaich F., Wild T. Waveform contenders for 5G OFDM vs. FBMC vs. UFMC // In Proc. 2014 6th International Symposium on Communications, Control and Signal Processing (ISCCSP). – IEEE, 2014. – pp. 457–460.

12 Schaich F. Filterbank based multi carrier transmission (FBMC) evolving OFDM: FBMC in the context of WiMAX // In Proc. 2010 European Wireless Conference (EW). – IEEE, 2010. – pp. 1051–1058.

13 Huawei and HiSilicon. Waveform evaluation updates for case 4. 3rd Generation Partnership Project (3GPP) RAN1 (R1) 166091, Aug. 2016. https://www.3gpp.org/ftp/tsg_ran/wg1_rL1/TSGR1_86/Docs/.

14 Abdoli M. J., Jia M., Ma J. Weighted circularly convolved filtering in OFDM/OQAM // In Proc. 2013 IEEE 24th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC). – IEEE, 2013. – pp. 657–661.

15 Kozek W., Molisch A. F. Nonorthogonal pulseshapes for multicarrier communications in doubly dispersive channels // IEEE Journal on Selected Areas in Communications. – 1998. – vol. 16. – no. 8. – pp. 1579–1589.

16 Zhao Z., Schellmann M., Wang Q., Gong X., Boehnke R., Xu W. Pulse shaped OFDM for asynchronous uplink access // In Proc. 2015 49th Asilomar Conference on Signals, Systems and Computers. – IEEE, 2015. – pp. 3–7.

Рис. 1. Способы снижения внеполосного излучения (OOBE) сигнала CP-OFDM

форма импульсов проектируется (в том числе и для случая использовании гребенчатого фильтра – FB-OFDM[17]), в целях обеспечения более резкого затухания спектра модулированного сигнала за пределами рабочей полосы.

Рассмотренные варианты обеспечивают снижение уровня внеполосного излучения сигнала технологии CP-OFDM.

Однако при этом, как при использовании линейной свертки со взвешивающим окном, так и при управлении формой импульса модуляции, значительная часть циклического префикса активного защитного интервала символа занимается отсчетами расширения границ символов, что снижает показатель устойчивости СК CP-OFDM к межсимвольной интерференции (ISI). В случае же обработки спектра множественного сигнала фильтрами, особенно гребенчатым, вследствие неравномерности характеристик АЧХ и ГВЗ фильтров, происходит нарушение ортогональности сигналов OFDM-поднесущих, что приводит к увеличению из взаимных помех (ICI).

Радикальным вариантом использования для снижения OOBE неортогональности сигналов поднесущих является подход, направленный на повышение компактности спектра сигнала множественной несущей посредством уменьшения частотного разноса его поднесущих, вплоть до значения менее ширины полосы каждого парциального сигнала. Так, для сигналов поднесущих применяется обобщенное мультиплексирование с частотным разделением GFDM[18], мультиплексирование с частотным разделением и перекрытием парциальных спектров OVFDM[19], спектрально-эффективное (с перекрытием) мультиплексирование с частотным разделением SEFDM [4]. Представленные технологии обеспечивают существенное снижение OOBE при контролируемом уровне ICI, но при этом, за счет нарушения ортогональности парциальных каналов передачи данных существенно усложняется их обработка при демодуляции и соответственно затрудняется использование таких сигналов в системах MIMO.

Отдельный класс исследований направлен на изучение возможностей использования при формировании многочастотного сигнала для улучшения его параметров преобразований, отличных от классического БПФ/ОБПФ (FFT/IFFT). К данному классу относятся технологии: FRFT-OFDM[20] на основе дробного преобразования Фурье; AFT-OFDM[21] на основе афинного преобразования Фурье; DWTOFDM[22] – мультиплексирование с частотным разделением

17 Yu X., Guanghui Y., Xiao Y., Zhen Y., Jun X., Bo G. FB-OFDM: A novel multicarrier scheme for 5G // In Proc. 2016 IEEE European Conference on Networks and Communications (EuCNC). – IEEE, 2016, – pp. 271–276.

18 Michailow N., Matthé M., Gaspar I. S., Caldevilla A. N., Mendes L. L., Festag A., Fettweis G. Generalized frequency division multiplexing for 5th generation cellular networks // IEEE Transactions on Communications. – 2014. – vol. 62. – no. 9. – pp. 3045–3061.

19 Li D. Overlapped multiplexing principle and an improved capacity on Additive White Gaussian Noise Channel // IEEE Access. – 2017. – vol. 6. – pp. – 6840–6848.

20 Martone M. A multicarrier system based on the fractional Fourier transform for time-frequency selective channels // IEEE Transactions on Communications. – 2001. – vol. 49. – no. 6. – pp. 1011–1020.

21 Erseghe T., Laurenti N., Cellini V. A multicarrier architecture based upon the affine Fourier transform // IEEE Transactions on Communications. – 2005. – vol. 53. – no. 5. – pp. 853–862.

22 Galli S., Koga H., Kodama N. Advanced signal processing for PLCs: Wavelet – OFDM // In Proc. 2008 IEEE International Symposium on Power Line Communications and Its Applications. – IEEE, 2008. – pp. 187–192.

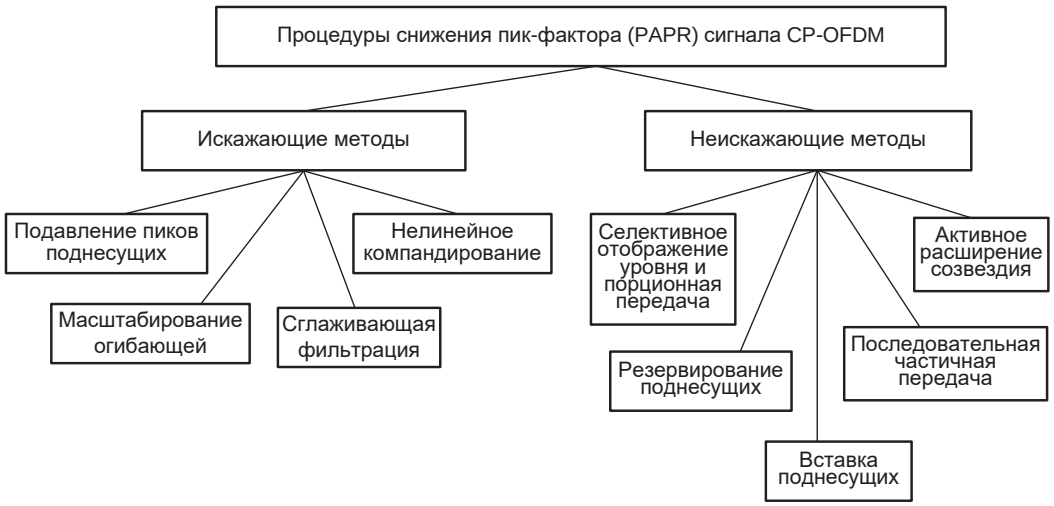


Рис. 2. Способы снижения пик-фактора (PAPR) сигнала CP-OFDM

на основе дискретных вейвлет-преобразований; LVDM [5] – мультиплексирование с частотным разделением по Лагранжу и Вандермонду, и также – SNMC[23] – множественная неортогональная несущая на основе функций Слепиана (вытянутых волновых сфероидальных функций PSWF).

Схемы реализации указанных способов обработки сигналов с множественной несущей достаточно сложны, причем эффективность их применения нуждается в дальнейших исследованиях.

Проблема большого пик-фактора (PAPR) сигнала CP-OFDM связана с высокой вероятностью совпадения текущих фаз множественных сигналов поднесущих за время достаточно протяженного символьного интервала. Указанная особенность сигнальной конструкции многочастотного сигнала является системной, поэтому радикально устранить её как причину возникновения высокого PAPR невозможно. На (рис. 2) показано, что известные методы снижения PAPR разделяются на искажающие и неискажающие. Искажающие методы снижения пик-фактора изменяют форму сигнала, например, посредством ограничения уровня его амплитуды или посредством сглаживающей фильтрации. Поскольку указанные методы достаточно просты, они широко известны и часто используются на практике.

Однако искажающие методы вносят в сигнал CP-OFDM существенные нелинейные искажения, как внутриполосные – ICI, так и внеполосные – OOBE. Поэтому значительное внимание разработчики уделяют исследованию неискажающих методов. Среди них известны такие, как селективное отображение уровня и порционная передача (SLM) [6], последовательная частичная передача (PTS)[24], резервирование поднесущих (TR)[25], вставка поднесущих (TI)[26] и активное расширение созвездия (ACE)[27].

В рамках исследования возможностей неискажающих методов, в ходе поиска эффективных алгоритмов управления фазами сигналов множественных поднесущих в целях снижения вероятности их совпадения[28], определенное внимание уделялось исключению совпадения абсолютных значений фаз сигналов, устанавливаемых в моменты их модуляции. На практике, требуемые смещения модуляционных фаз обеспечиваются случайным выбором начальных фаз опорных колебаний, используемых при формировании и при демодуляции множественного сигнала. Отметим, что штатным вариантом является также использование поворота абсолютных значений фаз модуляции сигнала QAM на некоторый угол относительно точек типового созвездия. При этом, по данным ГОСТ-Р 58912[29] при повороте созвездия на угол порядка $\pi/4$, за счет разноса координат точек созвездия и повышения тем самым их различимости при демодуляции CP-OFDM, также может быть достигнут энергетический выигрыш по помехоустойчивости

23 Yang X., Wang X., Zhang J. A new waveform based on Slepian basis for 5G system // In Proc. 2016 IEEE Wireless Days Conference (WD). – IEEE, 2016. – pp. 1–4.

24 Nghia T. V. Optimization Scheme of Partial Transmit Sequences Technique for Peak-to-Average Power Ratio Reduction of OFDM Signals and its FPGA Implementation // Digital Signal Processing. – 2017. – no. 4. – pp. 57–62.

25 Wattanasuwakull T., Benjapolakul W. PAPR Reduction for OFDM Transmission by using a method of Tone Reservation and Tone Injection // IEEE ICICS. – 2015. – pp. 273–277.

26 Tuna C., Jones D. L. Tone Injection With Aggressive Clipping Projection for OFDM PAPR // IEEE ICASSP. – 2010. – pp. 3278-3281.

27 Dhuness K., Maharaj B.T. Analysis Of An Offset Modulation Transmission // EURASIP Journal on Wireless Communications and Networking. – 2013, 19 (2013).

28 Tellambura C. Improved Phase Factor Computation for the PAPR Reduction of an OFDM Signal Using PTS // IEEE Commun. Lett. – Apr. 2001. – vol. 5. – no. 4. – pp. 135–137.

29 ГОСТ-Р 58912 – 2020. Телевидение вещательное цифровое. Система эфирного наземного цифрового телевизионного вещания второго поколения DVB-T2. Общие технические требования. – М. : Стандартинформ, 2020. – 76 с.

до 7,6 дБ. Поэтому, согласно стандарту 3GPP[30] этот способ улучшения модуляции использован в рассмотренных выше технологиях FBMC-OQAM и WCC-FBMC-OQAM. Однако, указанные меры не оказывают существенного влияния на вероятность совпадения текущих фаз множественных сигналов поднесущих за время символьного интервала между моментами модуляции, т.е. на величину показателя PAPR.

Более эффективное влияние на снижение показателя PAPR оказывает разнос моментов модуляции сигналов поднесущих во времени. Примером применения такой технологии является векторная OFDM (V-OFDM)[31], согласно которой данные модуляции N поднесущих символа OFDM делятся на K групп и используются для модуляционной установки фаз сигналов K векторов длиной N/K. «Частотные» представления модулированных векторов преобразуются посредством N/K-мерного ОБПФ во временные отсчеты и перемежаются, образуя результирующий выходной символ, вновь длиной N. При этом, моменты модуляции фаз отдельных OFDM поднесущих оказываются псевдослучайным образом разнесены во времени, что несколько снижает вероятность последующего совпадения текущих фаз. К недостаткам представленного способа снижения PAPR относится то, что спектр перемеженного сигнала не локализован, вследствие чего возрастают межканальные помехи ICI поднесущих и существенно усложняются реализации частотного эквалайзера и демодулятора.

Таким образом, многие неискажающие методы базируются на технологии расширенного скремблирования поднесущих множественного сигнала и требуют значительного усложнения алгоритмов обработки, кроме того снижается пропускная способность системы, поскольку определенная часть информационной ёмкости канала задействуется для передачи служебной информации, предназначенной для управления процедурами снижения пиковой мощности.

Например, SLM предполагает формирование нескольких эквивалентных представлений символов, для TR требуется часть поднесущих оставить немодулированнными, а TI предполагает добавление поднесущих с управляемой мощностью.

Специфическая проблема возникает при использовании сигнала со множественной несущей в широкополосных каналах миллиметрового или терагерцового диапазона. Известно, что при увеличении частоты несущей растет показатель спектральной плотности фазовых флуктуаций сигнала (PHN), вследствие чего разница его значений на границах широкой полосы рабочих частот может быть весьма значительной. Так, по данным [7], разница PHN между OFDM поднесущими на частотах 1 и 28 ГГц составляет значение около 20 дБ. Кроме того, по мере повышения несущей частоты уменьшается интервал когерентности канала с рассеянием, что ограничивает совокупное время, отведенное для измерения канала и осуществления передачи. В результате, применение в широкополосных каналах сигнала множественной несущей с длинным символом и с плотным расположением поднесущих приводит к недопустимому росту числа ошибок и к значительному ухудшению производительности системы. Таким образом, в высокоскоростных URLCC-системах с ультранизкой задержкой передачи данных возможно использование только многочастотных СК с увеличенным частотным разносом поднесущих и укороченным символьным интервалом. Однако, для передачи низкоскоростного трафика данных системы интернета вещей (IoT) все же целесообразно использовать узкополосные (в смысле общей полосы и плотности поднесущих) OFDM конструкции. Для решения описанных выше проблем, консорциум 3GPP стандартизировал переменный коэффициент разнесения OFDM поднесущих, введя так называемую масштабируемую нумерологию (SN). Стандартизация SN гарантирует согласование структуры сигнала множественной несущей соответственно задачам его применения. Так, для перспективных диапазонов 5G/6GNR миллиметровых волн спектральный разнос между ортогональными поднесущими варьируется, начиная со значения 15 кГц для LTE и заканчивая интервалом 30, 60 или 120 кГц[32].

По результатам выполненного анализа установлено, что во многих случаях вследствие мероприятий по снижению OOBE и PAPR многочастотного сигнала, либо нарушается ортогональность сигналов поднесущих, что приводит к возрастанию уровня их взаимных помех (ICI), либо снижается эффективность циклического префикса, что приводит к возрастанию уровня межсимвольных помех (ISI). Очевидно, что в этих условиях объективным критерием оптимальности выбора параметров сигнала многочастотной системы является коэффициент битовых ошибок (BER), снижающийся с уменьшением PAPR и OOBE, но увеличивающийся из-за роста ICI и ISI.

В процессе поиска компромиссных решений, разработчиками была предложена эффективная процедура снижения параметра OOBE OFDM сигнала без увеличения показателя PAPR и ухудшения

30 3rd Generation Partnership Project (3GPP). TS 36.211 V13.3.0. In Technical Specification Group Radio Access Network. Physical Channels and Modulation (Release 13). – New Orleans, LA, USA, 2016.

31 Xia X.-G. Precoded and vector OFDM robust to channel spectral nulls and with reduced cyclic prefix length in single transmit antenna systems // IEEE Transactions on Communications. – 2001. – vol. 49. – no. 8. – pp. 1363–1374.

32 3rd Generation Partnership Project (3GPP). TS 38.211 V16.3.0. 5G, NR. Physical channels and modulation (Release 16). ETSI TS 138 211 V16.3.0 (2020-11).

характеристик BER, получившая название технологии спектрального прекодирования данных модуляции SP-OFDM[33].

Согласно указанной технологии существенное снижение взаимных помех сигналов различных пользователей системы обеспечивается подавлением сигналов соответствующих поднесущих в частотной области (FDCS) при использовании в области данных дополняющего нулями кодирования (DDCS).

Результаты исследования сигналов с одной несущей

В ходе исследований технологии SP-OFDM рассматривались различные процедуры обеспечения спектрального прекодирования данных модуляции OFDM. В результате чего было установлено, что наиболее эффективным средством обеспечения гибкого управления свойствами формируемого сигнала согласно требуемым сценариям связи и низкого показателя PAPR, является процедура прямого дискретного преобразования Фурье (DFT)[34].

Рассмотрим структуру сигнала DFT-s-OFDM подробнее:

$$\hat{d}\,(n \cdot T_0 / N) = \frac{1}{\sqrt{MN}} \sum_{k=0}^{N-1} \left[c_k \left(\sum_{m=0}^{M-1} d_m \cdot e^{-j2\pi \frac{k}{M} m} \right) \right] e^{j2\pi \frac{k}{N} n},$$

$$n \in [1,N], \qquad (2)$$

где: $\{\dot{D}_m\}_{m=0}^{M-1}$ – комплексные символы данных PSK/QAM модуляции; $e^{-j2\pi \frac{k}{M} m}$ – k-й частотный фактор прямого дискретного преобразования Фурье (ДПФ) размерности M; $\{c_k\}_{k=0}^{N-1}$ – оператор формирования спектра (FDSS); $e^{j2\pi \frac{k}{N} n}$ – k-й частотный фактор обратного дискретного преобразования Фурье (ОДПФ) размерности $N \geq M$; $T_o = 1/(f_{k+1} - f_k)$ – интервал ортогональности N спектральных представлений формируемого сигнала; $n \cdot T_0 / N = t_n$ – моменты котельниковских отсчетов.

На каждом такте формируемого сигнала N информационных отсчетов интервала ортогональности T_o, полученные согласно (2) посредством OFDM, дополняются L отсчетами циклического префикса $T_{зи} = L \cdot To / N$: $\hat{d}(t_n) = \hat{d}(t_n - T_o)$ или $\hat{d}(t_n) = -\hat{d}(t_n - T_o)$, для $t_n = n \cdot To / N$ и $n \in [N+1, N+L]$, образуя в совокупности набор $N+L$ отсчетов полного символьного интервала: $T_c = T_o + T_{зи}$ соответственно.

Как следует из рассмотрения выражения (2), на первой стадии формирования сигнала DFT-s-OFDM, посредством ДПФ $m \in [0, M-1]$, на k-х OFDM-частотах вычисляется широкополосный спектр импульсного сигнала высокоскоростной несущей. Тем самым, обработка исходного временно́го сигнала d_m переносится в частотную область, где далее, посредством оператора FDSS c_k, формируется спектр сигнала с заданными характеристиками. На заключительной стадии формирования, согласно (2), посредством ОДПФ вычисляются отсчеты сигнала широкополосной несущей с требуемыми параметрами.

Известно, что сигнал одиночной широкополосной несущей по определению обладает низким значением PAPR и, следовательно, способен обеспечить эффективную работу недорогих передающих устройств с существенной нелинейностью усилительного тракта и ограниченным энергоресурсом.

Также, в отличие от сигналов со множественной несущей, сигнал одной широкополосной несущей устойчив к частотно-зависимым изменениям спектральной плотности фазовых флуктуаций (PHN) и доплеровским смещениям канальной частоты.Указанные преимущества обусловили не только широкое применение такого сигнала в системах сотовой связи предыдущих и современных поколений 4G LTE (UL), но и определяют целесообразность его применения в перспективных системах 5G/6G NR.

На (рис. 3) представлены некоторые способы формирования сигналов с одной несущей.

Согласно процедуре SC-QAM/SC-FDE[35] генерация сигнала одной несущей с квадратурно-амплитудной модуляцией, занимающего всю полосу пропускания канала, выполняется на передаче путем прямого цифрового синтеза его временных отсчетов.

33 Huang X., Zhang J. A., Guo Y. J. Out-of-Band Emission Reduction and a Unified Framework for Precoded OFDM // IEEE Communications Magazine. – 2015. – vol. 53. – no. 6. – pp. 151–159.

34 3rd Generation Partnership Project (3GPP). TS 38.211 V15.7.0. In Technical Specification Group Radio Access Network. Physical Channels and Modulation (Release 15). – Newport Beach, CA, USA, 2019.

35 Pancaldi F., Vitetta G. M., Kalbasi R., Al-Dhahir N., Uysal M., Mheidat H. Single Carrier Frequency Domain Equalization // IEEE Signal Processing Magazine. – 2008. – vol. 25. – no. 5. – pp. 37–56.

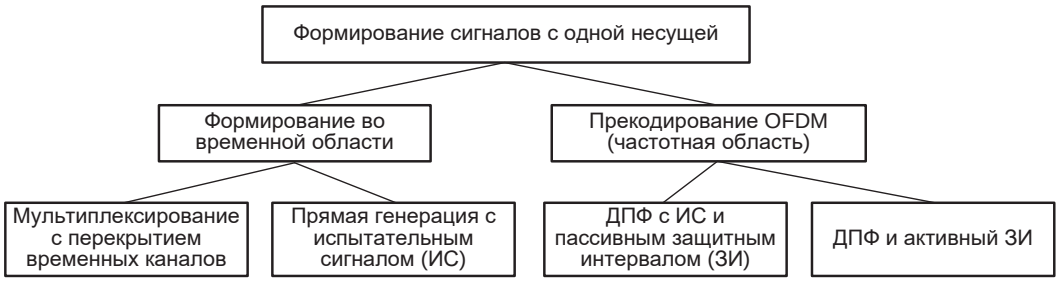


Рис. 3. Способы формирования сигналов с одной несущей

При этом, для обеспечения работы на приемной стороне частотного эквалайзера (FDE), в сигнал также периодически добавляются фиксированные последовательности отсчетов испытательного сигнала (UW) и нулей (ZT). В течение времени тестирования по результатам оценки CHIRP-сигнала UW эквалайзер получает данные о частотной характеристике канала и затем выравнивает ее (ZF, MMSE).

Технология OVTDM[36] использует для формирования одночастотного сигнала временное мультиплексирование с перекрытием импульсных реакций канала, обеспечивая тем самым работу системы на скорости выше предела Найквиста. Однако сложность приемника и необходимость проведения дополнительных детальных исследований по оценке степени увеличения пропускной способности на этой основе, в настоящее время ограничивают применение указанной технологии.

Согласно технологии ZT/UW-DFT-s-OFDM[37], в случае применения для формирования сигнала одной несущей прекодирования OFDM по типу ДПФ (DFT), также возможно использование для выравнивания и оценки характеристик канала вместо префиксного защитного интервала (ЗИ), специального ЛЧМ испытательного сигнала (UW) и нулей (ZT) пассивного ЗИ.

Однако, как и в случае SC-QAM/SC-FDE, замена отсчетов циклического префикса уникальной комбинацией ZT/UW приводит к снижению способности сигнала противодействовать воздействию межсимвольной интерференции (ISI) и к потере унификации его структуры.

Отметим, что представленная выражением (2) типовая технология синтеза сигнала DFT-s-OFDM с активным ЗИ в виде циклического префикса (CP), не только обеспечивает противодействие СК ISI, но и является достаточной для формирования требуемых свойств сигнала посредством процедуры FDSS в рамках его унифицированной структуры, т.е. при фиксированных прочих параметрах. Напомним, что согласно определенным выше требованиям, СК перспективного для 6G сигнала должна обеспечивать: одновременно сканирование канала и передачу данных (ISAC/DFRC), совместимость с MIMO, низкие показатели OOBE и PAPR.

Процедура спектрального прекодирования сигнала DFT-s-OFDM с CP обеспечивает:

- низкий показатель OOBE, посредством введения в его спектр интервалов защитного частотного разделения[38];
- совместимость с MIMO, за счет использования для множественной передачи данных каналов, сформированных на принципах SC-FDMA[39].

В случае ухудшения показателя PAPR сигнала DFT-s-OFDM при использовании многопозиционной QAM и пилот-сигналов, обеспечивающих когерентность её демодуляции, применение спектрального прекодирования OFDM типа полиномиальной отмены (PCC) [8] или интерполяции совокупности символов[40] позволяет компенсировать указанный негативный эффект.

Для обеспечения функционирования системы ISAC/DFRC, посредством спектрального прекодирования одночастотный сигнал DFT-s-OFDM может быть преобразован в форму линейной комбинации CHIRP-сигналов [9], используемых как для оценки характеристик канала, так и для передачи данных.

Отметим, что согласно данным источников, во всех рассмотренных случаях, в рамках унифицированной структуры сигнала DFT-s-OFDM, его свойства, отвечающие требованиям случая конкретного применения, согласно (2) определяются оператором формирования спектра (FDSS) $\{c_k\}_{k=0}^{N-1}$.

Так согласно [8], для спектра исходного сигнала $d_r : D_r = \sum_{r=0}^{\frac{M}{2^q}-1} d_r \times e^{-j2\pi\frac{k}{M}r}$, где $q \in \{0, 1, 2, \ldots\}$ – порядок полинома PCC, k-е компоненты оператора FDSS c_k^q, осуществляющего кодирование полиномиальной отмены, определяются как: $c_k^q = \sum_{u=0}^{2^q-1} (-1)^u d_r \times e^{-j2\pi\frac{k}{M}u}$.

А согласно [9], для формирования CHIRP-сигнала с линейной формой изменения во времени мгновенной частоты и параметром девиации $D = M$, в (2) используются указанные компоненты c_k вида: $c_k = \sqrt{\frac{\pi}{D}} \cdot (C(x_1) + C(x_2) + j\,S(x_1) + j\,S(x_2)) \times e^{-j\frac{2\pi k}{2D} - j\pi k}$, где $C(\cdot)$ и $S(\cdot)$ – интегралы Френеля с косинусной и синусной функциями соответственно, а $x_1 = (D/2 + 2\pi k)/\sqrt{\pi D}$ и $x_2 = (D/2 - 2\pi k)/\sqrt{\pi D}$.

Таким образом, процедура спектрального прекодирования данных модуляции является отличительной особенностью СК DFT-s-OFDM и определяет способность данной технологии обеспечить выполнение требований применения указанного сигнала в сетях 6G, сообразно различным сценариям связи. Спектральное прекодирование осуществляется средствами программируемого радио (SDR) путем гибкого управления оператором FDSS в рамках унифицированной структуры СК, что обеспечивает возможность использования всех модификаций сигнала в типовых DFT-s-OFDM-приемопередатчиках.

36 Anderson J. B., Rusek F., Öwall V. Faster-than-Nyquist signaling // Proceedings of the IEEE. – 2013. – vol. 101. – no. 8. – pp. 1817–1830.

37 Berardinelli G., Tavares F. M., Sorensen T. B., Mogensen P., Pajukoski K. Zero-Tail DFT-spread-OFDM signals // In Proc. 2013 IEEE GlobeCom Workshops. – IEEE, 2013. – pp. 229–234.

38 Huang X., Zhang J. A., Guo Y. J. Out-of-Band Emission Reduction and a Unified Framework for Precoded OFDM // IEEE Communications Magazine. – 2015. – vol. 53. – no. 6. – pp. 151–159.

39 Myung H., Lim J., Goodman D. Single carrier FDMA for uplink wireless transmission // IEEE Veh. Technol. Mag. – 2006. – no.1. – pp. 30–38.

40 MediaTek Inc. A new DFT-s-OFDM compatible low PAPR technique for NR uplink waveforms. 3rd Generation Partnership Project (3GPP) RAN1 (R1) 1609378, Oct. 2016. https://www.3gpp.org/ftp/TSG_RAN/WG1_RL1/TSGR1_86b/Docs/.

Экспериментальное подтверждение полученных результатов

В работах [8] и [9] представлены результаты численного моделирования анализируемых типов перспективных радиосигналов. Представленные характеристики демонстрируют технологические возможности управления параметрами сигналов DFT-s-OFDM применительно к различным сценариям организации связи при сохранении заданной помехоустойчивости передачи данных, например на уровне BER $\leq 1 \cdot 10^{-4}$ при $E_b/N_0 \approx 8$ дБ AWGN. Для оценки системы ISAC/DFRC моделировались сигналы рабочей полосы порядка 2 ГГц. Для оценки показателя OOBE моделировались соседние сигналы пользователей средней полосы (порядка 10 МГц) и пользователей узкой полосы (порядка 3 МГц).

В частности, в [8] показано, что при локализованном отображении в частотную область применение PCC с полиномом первого порядка, даже к сигналам с фазовой модуляцией низкой кратности (π/2-BPSK и QPSK), снижает показатель PAPR на 2-3 дБ и улучшает показатель OOBE на 10 дБ без ухудшения показателя BER (см. рис. 4).

В [9] показано, что сигнал CHIRP-DFT-s-OFDM, обладающий по определению PAPR = 0 дБ, в случае использования частотного разнесения, обеспеченного повторением передаваемых символов посредством линейных циркулярно-сдвинутых чирпов, обеспечивает эффективное зондирование канала при улучшении показателя OOBE в указанных выше пределах, при R = 4 также практически без ухудшения показателя BER (увеличение E_b/N_0 на 1,0 дБ) (см. рис. 5).

При этом в [8] отмечается лишь незначительное увеличение вычислительной сложности алгоритма цифровой обработки. Отметим, что в обоих моделируемых случаях реконфигурация свойств СК осуществляется посредством целенаправленного введения в сигнал избыточности, т.е. за счет контролируемого снижения пропускной способности основного канала передачи данных. В итоге, поскольку во всех моделируемых случаях программное управление показателями качества и функциональным назначением сигнала связи осуществляется посредством оператора FDSS унифицированного алгоритма (2), результаты представленных экспериментов доказывают технологичность применения в 6G сигнальных конструкций DFT-s-OFDM.

Заключение

Изучены функциональные особенности новых приложений (eMBB, URLLC, mMTC) сетей 6G, в результате чего установлено, что сигнальная конструкция (СК) перспективного для указанных сетей сигнала, должна обеспечивать низкие показатели OOBE

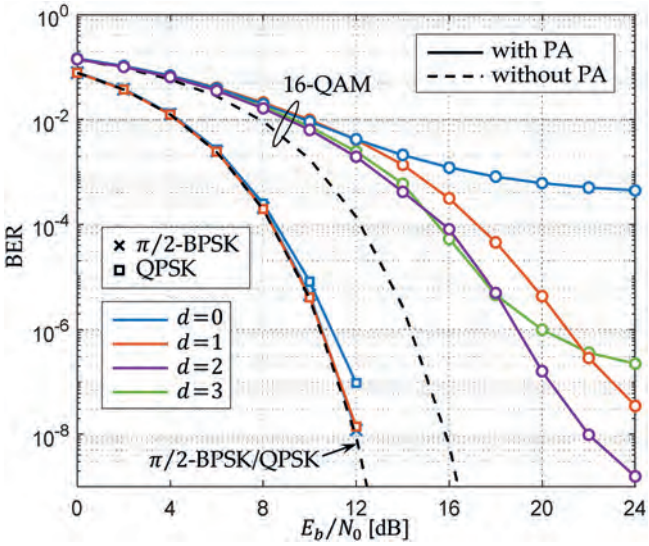
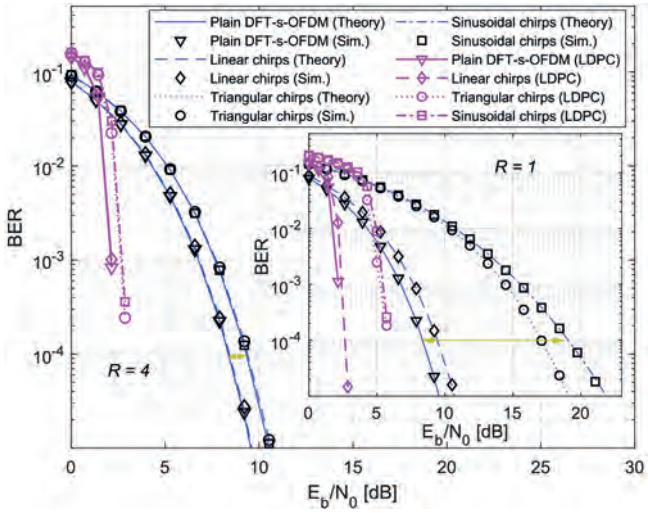


Рис. 4. Помехоустойчивость (BER) сигналов PCC-DFT-s-OFDM с PSK и 16 QAM при порядке полинома кодирования d = 0, 1, 2, 3 в канале с аддитивным белым гауссовым шумом (AWGN) с учетом влияния нелинейности усилителя мощности (PA) и без него [8]



Plain DFT-s-OFDM (Theory)	**Обычный DFT-s-OFDM (теория)**
Plain DFT-s-OFDM (Sim.)	**Обычный DFT-s-OFDM (моделирование)**
Linear chirps (Theory)	**Линейные CHIRP (теория)**
Linear chirps (Sim.)	**Линейные CHIRP (моделирование)**
Triangular chirps (Theory)	**Треугольные CHIRP (теория)**
Triangular chirps (Sim.)	**Треугольные CHIRP (моделирование)**
Sinusoidal chirps (Theory)	**Синусоидальные CHIRP (теория)**
Sinusoidal chirps (Sim.)	**Синусоидальные CHIRP (моделирование)**
Plain DFT-s-OFDM (LDPC)	**Обычный DFT-s-OFDM (LDPC)**
Linear chirps (LDPC)	**Линейные CHIRP (LDPC)**
Triangular chirps (LDPC)	**Треугольные CHIRP (LDPC)**
Sinusoidal chirps (LDPC)	**Синусоидальные CHIRP (LDPC)**

Рис. 5. Помехоустойчивость (BER) некодированных и LDPC-кодированных обычного DFT-s-OFDM сигнала и сигналов CHIRP-DFT-s-OFDM с вариантами числа повторений R = {1, 4}, в канале с аддитивным белым гауссовым шумом (AWGN) [9]

и PAPR, технологическую совместимость с MIMO и одновременное с передачей данных сканирование канала по типу ISAC/DFRC.

Определена технологичность СК, как её способность наиболее полно обеспечить установленные показатели качества и требуемые сценарии связи, при максимальной унификации структуры сигнала и алгоритмов его обработки. Предложена методология исследования технологических возможностей СК с точки зрения эффективности их применения в 6G.

Выполнен системный анализ технологических возможностей различных вариантов СК с множественной несущей типа OFDM и с одной несущей (SC), включая СК типа DFT-s-OFDM. Получены соответствующие оценки, рассмотренные СК классифицированы.

Показано, что сигнал множественной несущей технологии CP-OFDM имеет высокие показатели OOBE и PAPR, а способы улучшения этих параметров не технологичны, поскольку реализуются посредством сложных и специфических технических решений. Указанные обстоятельства ограничивают применение сигнала CP-OFDM в сетях 6G.

Также показано, что сигнал одиночной широкополосной несущей технологии DFT-s-OFDM по определению обладает низким показателем PAPR и посредством процедуры спектрального прекодирования обеспечивает гибкость программного управления параметрами сигнальной конструкции сообразно различным сценариям связи в системах 6G, использующих типовые приемопередатчики DFT-s-OFDM.

Результаты получены в ходе исследования технологических решений систем, сетей и устройств радиотелекоммуникаций и могут быть использованы при разработке рекомендаций для создания перспективной отечественной системы связи 5GA/6G, обеспечивающей сверхвысокие скорости передачи данных и ультрамалые задержки [10]. Актуальность создания указанной системы подтверждается сведениями о наличии зарубежных разработок по применению подобных систем, в том числе и в военных целях [11]. В России, обладающей значительными территориями, в некоторых случаях подобные сети позиционируются как элементы протяженных сетецентрических систем [12], построенных с использованием сквозных цифровых технологий [13], в частности для применения в Арктическом регионе РФ с использованием КВ-радиосвязи [14] или тропосферных станций [15]. В этом плане значительное внимание уделяется вопросам организации каналов связи [16] и управления [17] мобильного транспортного домена сетей 5G/6G. При этом подразумевается построение трехмерной (частотно-временной и пространственной) архитектуры сетей 6G [18]. Таким образом, результат определения структуры СК, оптимальной по критерию максимальной спектрально-энергетической эффективности и соответствия требуемым параметрам эксплуатации сетей 5G/6G весьма важен для отечественных разработчиков, поскольку позволяет оптимизировать структуру сигнала информационной системы в целом, включая обеспечение требований информационной безопасности [19].

Литература

1. *Тонг В., Чжу П. Путь от 5G к 6G глазами разработчиков. От подключенных людей и вещей к подключенному интелекту; под ред. В. Тонг, П. Чжу / Вэнь Тонг, Пейин Чжу; пер. с англ. В. С. Яценкова. – М. : ДМК Пресс, 2022. – 624 с.*
2. *Лучин Д.В. Тенденции и перспективы развития радиосистем субтерагерцового диапазона. В сборнике: Актуальные проблемы радиоэлектроники и телекоммуникаций; под редакцией А.И. Данилина / Д.В. Лучин. – Самара : Материалы Всероссийской научно-технической конференции АПРиТ, 2022. – С. 8–11.*
3. *Tripathi S., Sabu N. V., Gupta A. K., Dhillon H. S. Millimeter-wave and Terahertz Spectrum for 6G Wireless // Computer Communications and Networks. – 20 Feb. 2021.*
4. *Liu X., Xu T., Darwazeh I. Coexistence of orthogonal and nonorthogonal multicarrier signals in beyond 5G scenarios // In Proc. 2020 2nd 6G Wireless Summit (6G SUMMIT). – IEEE, 2020. – pp. 1–5.*
5. *Tourki K., Zakaria R., Debbah M. Lagrange Vandermonde Division Multiplexing // In Proc. 2020 IEEE International Conference on Communications (ICC). – IEEE, 2020. – pp. 1–6.*
6. *Munir M., Youssef M. I., Abosha A. M. Low-Complexity Selective Mapping Technique for PAPR Reduction in Downlink Power Domain OFDM-NOMA // EURASIP Journal on Advances in Signal Processing. – 2023, 10.*
7. *Buritica A. From Waveforms to MIMO: 5 Things for 5G New Radio // Microwave Journal. – 14 May 2019.*
8. *Cho L., Kuo Y. M., Wu Y. S., Hsu C. Y. Polynomial Cancellation Coded DFT-s-OFDM for Low-PAPR uplink signaling // Electronics (Switzerland). – November 2019. – 8(11):1349.*
9. *Sahin A., Hosseini N., Hosseinali J., Shams S., Hoque M., Matolak D. W. DFT-spread-OFDM Based Chirp Transmission // IEEE Communications Letters. – March 2021. – vol.25. – Issue 3.*
10. *Антонова В. М., Клыгин Д. С., Кондрашова Д. А., Бабаханов С. А. Влияние 5G на нашу жизнь // Colloquium-Journal. – 2021. – № 34-1 (121). – С. 9–12.*
11. *Milicevic Z. M., Bojkovic Z. S. Review of 5G and 6G applications for mobile wireless communication in the military environment // Military Technical Courier. – 2024. – V. 72. – № 1. – pp. 435–451.*
12. *Gulyaev Y. V., Oleinikov A. Ya., Makarenko S. I. Russian approach to interoperability formalization of network-centric systems // In Proceedings of 2021 IV International Conference on Control in Technical Systems (CTS). – IEEE, 2021. – pp. 72–75.*

13. *Рыжков А. В., Шварц М. Л. Предпосылки создания когерентной сети связи общего пользования - основы сквозных цифровых технологий // T-Comm: Телекоммуникации и транспорт. – 2021. – Т. 15. – № 7. – С. 14–22.*
14. *Лучин Д. В., Гавлиевский С. Л., Маслов Е. Н. Масштабируемая телематическая система для арктических регионов РФ с использованием КВ-радиосвязи // Электросвязь. – 2019. – № 9. – С. 22–31.*
15. *Лучин Д. В., Климов Д. А. Тропосферные станции НИИР обеспечат интернетом жителей крайнего севера // Электросвязь. – 2021. – № 9. – С. 13–15.*
16. *Айметдинова У. А., Веденькин Д. А., Али Аль-Муфти, Мисбахов Р. Ш., Морозов О. Г., Морозов Г. А., Кузнецов А. А. Анализ метода двухчастотной инициализации каналов связи транспортного домена сетей 5G/6G // Научно-технический вестник Поволжья. – 2023. – № 9. – С. 140–143.*
17. *Айметдинова У. А., Булдакова К. Э., Али Аль-Муфти, Василец С. А., Василец А. А., Мисбахов Р. Ш., Морозов Г. А. Формирование узкополосного сигнала управления для мобильного транспортного домена сетей 5G/6G // Научно-технический вестник Поволжья. – 2023. – № 11. – С. 324–326.*
18. *Девяткин Е. Е., Иванкович М. В., Пастух А. С. Анализ возможности построения трехмерной архитектуры сетей 6G // Системы синхронизации, формирования и обработки сигналов. – 2021.– Т. 12. – № 6. – С. 91–99.*
19. *Макаренко С. И. Тестирование на проникновение на основе стандарта NIST SP 800-115 // Вопросы кибербезопасности. – 2022. – № 3 (49). – С. 44–57.*

References

1. *Tong V., Chzhu P. Put' ot 5G k 6G glazami razrabotchikov. Ot podkljuchennyh ljudej i veshhej k podkljuchennomu intellektu; pod red. V. Tong, P. Chzhu / Vjen' Tong, Pejin Chzhu; per. s angl. V.S. Jacenkova. – M. : DMK Press, 2022. – 624 c.*
2. *Luchin D. V. Tendencii i perspektivy razvitija radiosistem subteragercovogo diapazona. V sbornike: Aktual'nye problemy radiojelektroniki i telekommunikacij; pod redakciej A. I. Danilina / D. V. Luchin. – Samara : Materialy Vserossijskoj nauchno-tehnicheskoj konferencii APRiT, 2022. – S. 8–11.*
3. *Tripathi S., Sabu N. V., Gupta A. K., Dhillon H. S. Millimeter-wave and Terahertz Spectrum for 6G Wireless // Computer Communications and Networks. – 20 Feb. 2021.*
4. *Liu X., Xu T., Darwazeh I. Coexistence of orthogonal and nonorthogonal multicarrier signals in beyond 5G scenarios // In Proc. 2020 2nd 6G Wireless Summit (6G SUMMIT). – IEEE, 2020. – pp. 1–5.*
5. *Tourki K., Zakaria R., Debbah M. Lagrange Vandermonde Division Multiplexing // In Proc. 2020 IEEE International Conference on Communications (ICC). – IEEE, 2020. – pp. 1–6.*
6. *Munir M., Youssef M. I., Abosha A. M. Low-Complexity Selective Mapping Technique for PAPR Reduction in Downlink Power Domain OFDM-NOMA // EURASIP Journal on Advances in Signal Processing. – 2023, 10.*
7. *Buritica A. From Waveforms to MIMO: 5 Things for 5G New Radio // Microwave Journal. – 14 May 2019.*
8. *Cho L., Kuo Y. M., Wu Y. S., Hsu C. Y. Polynomial Cancellation Coded DFT-s-OFDM for Low-PAPR uplink signaling // Electronics (Switzerland). – November 2019. – 8(11):1349.*
9. *Sahin A., Hosseini N., Hosseinali J., Shams S., Hoque M., Matolak D. W. DFT-spread-OFDM Based Chirp Transmission // IEEE Communications Letters. – March 2021. – vol.25. – Issue 3.*
10. *Antonova V. M., Klygin D. S., Kondrashova D. A., Babahanov S. A. Vlijanie 5G na nashu zhizn' // Colloquium-Journal. – 2021. – № 34-1 (121). – S. 9–12.*
11. *Milicevic Z. M., Bojkovic Z. S. Review of 5G and 6G applications for mobile wireless communication in the military environment // Military Technical Courier. – 2024. – V. 72. – № 1. – pp. 435–451.*
12. *Gulyaev Y. V., Oleinikov A. Ya., Makarenko S. I. Russian approach to interoperability formalization of network-centric systems // In Proceedings of 2021 IV International Conference on Control in Technical Systems (CTS). – IEEE, 2021. – pp. 72–75.*
13. *Ryzhkov A. V., Shvarc M. L. Predposylki sozdanija kogerentnoj seti svjazi obshhego pol'zovanija - osnovy skvoznyh cifrovyh tehnologij // T-Comm: Telekommunikacii i transport. – 2021. – T. 15. – № 7. – S. 14–22.*
14. *Luchin D. V., Gavlievskij S. L., Maslov E. N. Masshtabiruemaja telematicheskaja sistema dlja arkticheskih regionov RF s ispol'zovaniem KV-radiosvjazi // Jelektrosvjaz'. – 2019. – № 9. – S. 22–31.*
15. *Luchin D. V., Klimov D. A. Troposfernye stancii NIIR obespechat internetom zhitelej krajnego severa // Jelektrosvjaz'. – 2021. – № 9. – S. 13–15.*
16. *Ajmetdinova U. A., Veden'kin D. A., Ali Al'-Mufti, Misbahov R. Sh., Morozov O. G., Morozov G. A., Kuznecov A. A. Analiz metoda dvuhchastotnoj inicializacii kanalov svjazi transportnogo domena setej 5G/6G // Nauchno-tehnicheskij vestnik Povolzh'ja. – 2023. – № 9. – S. 140-143.*
17. *Ajmetdinova U. A., Buldakova K. Je., Ali Al'-Mufti, Vasilec S. A., Vasilec A. A., Misbahov R. Sh., Morozov G. A. Formirovanie uzkopolosnogo signala upravlenija dlja mobil'nogo transportnogo domena setej 5G/6G // Nauchno-tehnicheskij vestnik Povolzh'ja. – 2023. – № 11. – S. 324–326.*
18. *Devjatkin E. E., Ivankovich M. V., Pastuh A. S. Analiz vozmozhnosti postroenija trehmernoj arhitektury setej 6G // Sistemy sinhronizacii, formirovanija i obrabotki signalov. – 2021.– T. 12. – № 6. – S. 91–99.*
19. *Makarenko S. I. Testirovanie na proniknovenie na osnove standarta NIST SP 800-115 // Voprosy kiberbezopasnosti. – 2022. – № 3 (49). – S. 44–57.*

АНАЛИЗ СУЩЕСТВУЮЩИХ ПОДХОДОВ К СИНТЕЗУ ПСЕВДО-ДИНАМИЧЕСКИХ SBOX

Прудников В. А.[1]

DOI: 10.21681/2311-3456-2024-4-57-64

Целью исследования *является анализ существующих на текущий момент подходов к синтезу псевдо-динамических sbox, для подтверждения актуальности проблемы синтеза sbox, удовлетворяющих широкому спектру взаимоисключающих требований.*

Методы исследования: *анализ и систематизация существующих подходов к синтезу криптографических операций sbox и псевдо-динамических sbox.*

Результатом исследования является вывод о том, что на текущий момент проблема синтеза sbox, как основного нелинейного элемента современных блочных шифров и псевдослучайных функций, удовлетворяющих взаимоисключающим требованиям, является актуальной. Существует ряд способов решения обозначенной проблемы, подразумевающих подбор sbox в соответствии с требованиями, реализация нелинейного элемента псевдослучайной функции или криптоалгоритма в качестве ARX-функции, применение динамических sbox и синтез псевдо-динамических sbox, в основе которых могут быть как фиксированные нелинейные элементы, так и ARX-конструкции. К операциям sbox, вне зависимости от их вида, предъявляется около десятка требований, напрямую влияющих на криптографическую стойкость псевдослучайных функций, перестановок и криптоалгоритмов. Следовательно, проблема синтеза sbox, удовлетворяющих широкому спектру взаимоисключающих параметров является базовой. Синтез псевдо-динамических операций sbox на основе специально подобранных ARX-функций, обладающих разностными и линейными свойствами эквивалентных sbox, аналогичным случайно сформированным фиксированным нелинейным элементам той же размерности, в псевдослучайных функциях семейства pCollapser, потенциально позволяет обеспечить оптимальное использование векторных инструкций процессора и параллелизм обработки информации.

Практическая значимость *заключается в обосновании актуальности применения нового подхода к синтезу перспективного криптографического преобразования – псевдо-динамического sbox, удовлетворяющего широкому спектру взаимоисключающих требований, для задач криптографической защиты информации.*

Ключевые слова: *криптография, криптографические примитивы, sbox, псевдо-динамические sbox, ARX-функции, псевдослучайные функции.*

ANALYSIS OF EXISTING APPROACHES TO THE SYNTHESIS OF PSEUDO-DYNAMIC SBOX

Prudnikov V. A.[2]

The purpose of the research *is to analyze currently existing approaches to the synthesis of pseudo-dynamic substitution operations, to confirm the relevance of the problem of synthesizing substitution operations that satisfy a wide range of mutually exclusive requirements.*

Research methods: *analysis and systematization of existing approaches to the synthesis of cryptographic operations sbox and pseudo-dynamic sbox.*

The result of the research *is the conclusion that at the moment the problem of synthesizing substitution operations as the main nonlinear element of modern block ciphers and pseudo-random functions that satisfy mutually exclusive requirements is relevant. There are a number of ways to solve this problem, implying the selection of substitution operations in accordance with the requirements, the implementation of a nonlinear element of a pseudo-random function or a cryptoalgorithm as an ARX function, the use of dynamic substitutions in ciphers and the synthesis of pseudo-dynamic substitutions, which can be based on either fixed substitution operations, and ARX-constructions. Substitution operations, regardless of their type, are subject to about a dozen requirements that directly affect the cryptographic strength of pseudorandom functions, permutations and cryptoalgorithms. Consequently, the problem of synthesizing replacements that satisfy a wide range of mutually exclusive parameters is basic. Synthesis of pseudo-dynamic substitution operations*

1 Прудников Вадим Александрович, ассистент кафедры информационной безопасности телекоммуникационных систем Института компьютерных технологий и информационной безопасности ФГАОУ ВО «Южный федеральный университет», Таганрог, Россия. E-mail: prudnikov@sfedu.ru. ORCHID: 0000-0002-5011-727X.

2 Vadim A. Prudnikov, Assistant Professor, Department of Information Security of Telecommunication Systems, Institute of Computer Technologies and Information Security, Southern Federal University, Taganrog, Russia. E-mail: prudnikov@sfedu.ru. ORCHID: 0000-0002-5011-727X.

based on specially selected ARX functions that have differential and linear properties of equivalent substitutions, similar to randomly fixed substitution operations of the same dimension, in pseudo-random functions of the pCollapser family, potentially allows for optimal use of processor vector instructions and parallelism of information processing.

***The practical significance** lies in substantiating the relevance of using a new approach to the synthesis of a promising cryptographic transformation - pseudo-dynamic sbox, satisfying a wide range of mutually exclusive requirements for problems of cryptographic information protection.*

***Keywords:** cryptography, cryptographic primitives, sbox, pseudo-dynamic sbox, ARX functions, pseudo-random functions.*

Введение

Блок криптографической подстановки (sbox) – это нелинейный элемент, осуществляющий отображение n-битного сообщения на входе в m-битное сообщение на выходе. Sbox обладают множеством криптографических свойств: нелинейность; разностные характеристики; сбалансированность; корреляционный иммунитет; глобальный лавинный критерий; алгебраический иммунитет; критерий распространения; порядок прозрачности.

Обозначенные параметры криптографического элемента sbox оказывают ключевое влияние на устойчивость криптоалгоритмов и псевдослучайных функций (PRF) к различным методам криптоанализа.

Криптографические операции sbox являются основным нелинейным элементом множества современных блочных шифров и псевдослучайных функций. Их устойчивость к различным методам криптоанализа напрямую зависит от типа и качества используемых операций sbox.

Одной из основных задач рассматриваемого нелинейного элемента является обеспечение устойчивости к статистическим методам криптоанализа, в частности к линейному и разностному. Подбор операций sbox для криптоалгоритмов или псевдослучайных функций не является тривиальной задачей, основная проблема – анализ множества синтезируемых нелинейных элементов для отбора структур, соответствующих взаимоисключающим критериям, которые определяют sbox, максимально приближенный к идеальному. При генерации нелинейного элемента необходимо соблюдать множество жестких требований для обеспечения стойкости к статистическим атакам. Синтез криптоустойчивых sbox необходим как для разрабатываемых алгоритмов, так и для использующихся в настоящее время.

Проблема синтеза операций sbox, удовлетворяющих широкому спектру взаимоисключающих требований по устойчивости к различным методам криптоанализа и потреблению как программных, так и аппаратных ресурсов, является актуальной и ей уделяется значительное внимание.

Существует множество подходов решения проблемы синтеза sbox. Большинство из них заключается в применении различных методик при генерации фиксированных нелинейных элементов, обладающих требуемыми криптографическими свойствами. Иным способом решения задачи является применение конструкций, потенциально способных заменить операции sbox в шифрах и псевдослучайных функциях, к ним относятся ARX-конструкции (структуры, включающие в свой состав операции сложения по модулю слова, циклического сдвига и XOR), динамические sbox, позволяющие потенциально нивелировать возможность применения статистических атак на криптоалгоритм, псевдо-динамические sbox, включающие в свой состав либо фиксированные sbox, либо специально подобранные ARX-функции, и позволяющие объединить преимущества как классических sbox, так и динамических, что даёт ряд преимуществ при их аппаратной и программной реализации в составе псевдослучайных функций.

Анализ существующих подходов к синтезу нелинейного элемента sbox

Проанализируем первый вариант решения проблемы – синтез криптографических операций sbox с использованием различных алгоритмов, позволяющих получить элемент, обладающий криптографическими свойствами, приближенными к идеальным.

В работе[3] описан реверсивный генетический алгоритм, использование которого позволяет быстро генерировать большое число стойких биективных sbox размерностью от 8 бит до 16, которые имеют неоптимальные свойства и более сложную алгебраическую структуру, а также не обладают линейной избыточностью. В статье[4] представлен метод генерации sbox размерностью 8 бит с нелинейностью, достигающей значения 104. Метод комбинирует специальный генетический алгоритм с полным деревом поиска. В исследовании[5] представлен метод генерации нелинейных sbox на основе градиентного спуска. Приведены критерии отбора операций sbox для криптографических симметричных примитивов,

3 Ivanov G., Nikolov N., Nikova S. Reversed genetic algorithms for generation of bijective s-boxes with good cryptographic properties // Cryptogr. Commun. – 2016. – Vol. 8. – P. 247–276. – DOI: 10.1007/s12095-015-0170-5. – URL: https://doi.org/10.1007/s12095-015-0170-5

4 Tesař P. A new method for generating high non-linearity s-boxes // Radioengineering. – 2010. – Vol. 19, no. 1. – P. 23–26. – URL: https://www.radioeng.cz/fulltexts/2010/10_01_023_026.pdf

5 Kazymyrov O., Kazymyrova V., Oliynykov R. A method for generation of high-nonlinear s-boxes based on gradient descent // IACR Cryptology ePrint Archive (2013). – 2014. – URL: http://eprint.iacr.org/2013/578

основанных на анализе свойств векторных булевых функций. Предлагается усовершенствованный метод градиентного спуска для увеличения эффективности генерации нелинейных векторных булевых функций с оптимальными криптографическими показателями. Использование предложенного метода для наиболее часто применяемых sbox, размерностью 8 бит, позволяет добиться показателей нелинейности 104. Авторами работы[6] предлагается подход к генерации операций sbox, основанный на применении четвертичных последовательностей де Брейна, позволяющих добиться значительного увеличения числа доступных экономичных sbox по сравнению с использованием двоичных последовательностей де Брейна. Исследования в [1] посвящены разработке новой реализации криптоалгоритма AES, включающего в свой состав HPAC-SBOX (Hybrid Prediction and Adaptive Chaos – гибридное прогнозирование и адаптивный хаос), который объединяет алгоритмы обучения с прогнозированием и адаптивные хаотические логистические операции sbox. В [2] сравнивается эффективность подходов к генерации операций sbox в соответствии с их значениями нелинейности. Рассмотрены преимущества и недостатки представленных подходов. В [3] представлена разработка алгоритма генерации sbox с использованием генетического алгоритма. В алгоритме генерации обработано значение нелинейности, которое является одним из наиболее важных критериев оценки операций sbox. Качество сгенерированных блоков sbox определено с помощью тестов производительности. В [4] предлагается алгоритм генерации операций sbox, основанный на 4D гиперхаотической системе и улучшенной оптимизации роя частиц. Улучшена хаотическая система Лоренца и предложена 4D гиперхаотическая система с более высоким показателем Ляпунова и более сложной динамикой. Идея алгоритма имитационного отжига введена в алгоритм оптимизации роя частиц, что еще больше повышает эффективность алгоритма оптимизации и устраняет проблему, заключающуюся в том, что алгоритм оптимизации роя частиц легко поддается локальному оптимальному решению. Алгоритм использован для оптимизации нелинейности блоков sbox и повышения их производительности. В [5] представлена новая разновидность стохастического алгоритма генерации sbox, суть которого заключается в постепенном построении вектора значений булевой функции. Поиск новых значений выполняется случайным образом, основанном на ограничениях на дифференциальный спектр генерируемого sbox. В [6] представлен новый подход к генерации sbox, устойчивых к атакам по анализу мощности. На предварительном этапе создаётся sbox с базовыми криптографическими свойствами. Затем, на основе полученного sbox осуществляется генерация новых, с использованием генетического алгоритма на определенном подмножестве набора линейных комбинаций координатных функций исходного sbox. Работа [7] посвящена новому генетическому алгоритму, предназначенному для улучшения свойств sbox, созданных структурой Фейстеля. Однородность бумеранга определяет устойчивость блочных шифров к атакам бумеранга и является одним из параметров sbox. Стоит отметить, что операции sbox, созданные структурой Фейстеля, обладают недостаточной однородностью бумеранга. Авторами предложен новый генетический алгоритм для улучшения свойств подобных sbox, позволяющий генерировать несколько биективных sbox размерностью 8 бит с дифференциальной однородностью 6, нелинейностью 108 и однородностью бумеранга 10. В [8] представлен новый метод генерации криптостойких sbox размерностью 8 бит, путём применения матрицы смежности к полю Галуа GF(28).

Указанные подходы не удовлетворяют всем взаимоисключающим требованиям. В частности, размерность сгенерированной sbox может не позволить эффективно применять её в программной или аппаратной реализации в силу потребления большого объёма ресурсов.

Иной способ решения заключается в применении в качестве фиксированных sbox ARX-функций. В работе[7] представлено семейство поточных шифров Salsa20, основанное на ARX-операциях. Классическая версия криптоалгоритма включает 20 раундов преобразований и три вида операций над 32-битными словами: сложение по модулю 2^{32}, операция XOR, циклический сдвиг. Salsa20 расширяет 256-битный ключ и 64-битный nonce (уникальный номер сообщения) в 270-байтовый поток. Он шифрует b-байтовый открытый текст, объединяя открытый текст с первыми b байтами потока и отбрасывая остальную часть потока. Операция дешифрования осуществляется выполнением операции XOR над зашифрованным текстом с первыми b байтами потока. В алгоритме отсутствует обратная связь от открытого или зашифрованного текста к потоку. Salsa20 генерирует поток блоками по 64 байта (512 бит). Каждый блок включает независимый хэш ключа, nonce и 64-битный номер блока, отсутствует сцепление предыдущего блока с последующим. Поток на выходе криптоалгоритма может быть доступен случайным образом, и любое количество блоков может быть вычислено

6 Соколов А. В., Мазурков М. И. Методы синтеза четверичных последовательностей де Брейна для задач криптографии // Решетневские чтения. 2012. №16. URL: https://cyberleninka.ru/article/n/metody-sinteza-chetverichnyh-posledovatelnostey-de-breyna-dlya-zadach-kriptografii

7 Bernstein, D. J. (2008). The Salsa20 Family of Stream Ciphers. In: Robshaw, M., Billet, O. (eds) New Stream Cipher Designs. Lecture Notes in Computer Science, vol 4986. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-68351-3_8.

параллельно. В Salsa20 нет предварительной обработки. В исследовании[8] представлены результаты криптоанализа над семейством поточных шифров Salsa20. Авторам удалось достичь сложности поиска ключа в $2^{247,2}$ при осуществлении анализа 8-раундовой реализации, что значительно превосходит результаты прошлых лет в 2^{251} и 2^{250}. Работа [9] посвящена новому методу поиска линейных аппроксимаций криптоалгоритмов на основе ARX-конструкций, в частности шифра ChaCha. Авторами демонстрируется получение линейных аппроксимаций для 3 и 4 раундов ChaCha. В [10] представлены улучшения в системе дифференциально-линейных атак, предназначенных для шифров на базе ARX-операций. Для демонстрации результатов работы применены к криптоалгоритмам Chaskey и ChaCha. В работе[9] представлены шифры Simon и Speck – легковесные блочные криптоалгоритмы, предназначенные для интернета вещей. Максимальный размер блока составляет 128 бит, максимальный размер ключа – 256 бит. Блок состоит из двух слов, при этом слово может иметь размер 16, 24, 32, 48 или 64 бит. Ключ обладает размерностью в 2, 3 или 4 слова. Раундовая функция включает в себя операции: циклического сдвига первого слова вправо на 8 бит, сложение второго слова с первым по модулю 2 в степени длины слова, операция XOR ключа и результата сложения, циклический сдвиг второго слова влево на 3 бита, операция XOR второго слова и результата предыдущего XOR. Количество раундов зависит от выбранных размеров слова и ключа, для максимальных размеров блока и ключа количество раундов равно 34, при минимальных значениях – 22. В статье[10] продемонстрированы результаты разностного криптоанализа над описанными шифрами. В [11] представлен новый блочный шифр на базе ARX-конструкций и MDS-матрицы на основе концепции белого ящика – WARX. В [12] представлена 64-битная операция sbox Alzette, основой которой являются ARX-функции. Особенностью преобразования является то, что оно вычисляется на современных процессорах за фиксированное время и использует всего 12 инструкций. Параллельная реализация Alzette может использовать векторные (SIMD) инструкции. Одна итерация обладает разностными и линейными характеристиками, сравнимыми со свойствами операции sbox алгоритма AES, две последующие итерации обеспечивают тот же уровень устойчивости, что и супер-sbox AES. Alzette используется для построения малоресурсного 64-битного блочного криптоалгоритма Crax, превосходящего SPECK-64/128 на коротких сообщениях на микроконтроллерах, а также 256-битного блочного шифра Trax.

Минусом подхода, подразумевающего использование ARX-операций являются, как правило, неудовлетворительные криптографические свойства создаваемых конструкций, однако, они позволяют добиться высокого быстродействия и малого потребления ресурсов при программной и аппаратной реализации.

Для противодействия статистическим методам криптоанализа неоднократно осуществлялись попытки применять вместо фиксированных sbox динамически изменяемые.

Наиболее успешной попыткой применения динамически изменяемой sbox можно назвать криптоалгоритм RC4, который считается устаревшим и ненадёжным. Основная проблема стойкости RC4 – применение всего одной динамически изменяемой sbox и медленное обновление содержимого (за одну итерацию обновляется 2 ячейки из 256)[11]. Проблема предопределена тем, что динамические операции sbox (в сравнении с фиксированными sbox) требуют на порядки больше вычислительных ресурсов.

Применение псевдо-динамических sbox (PD-sbox) на базе фиксированных нелинейных элементов потенциально позволяет решить ряд описанных выше проблем, в частности, обеспечить устойчивость к статистическим методам криптоанализа.

Описание структуры псевдо-динамической операции PD-sbox

Псевдо-динамический sbox – нелинейный элемент (функция), объединяющий свойства фиксированных (высокая скорость преобразования, эффективное использование вычислительных ресурсов) и динамических (нейтрализация статистических методов криптоанализа) операций sbox[12].

Структура псевдо-динамической операции PD-sbox включает в свой состав фиксированные sbox. Аргумент каждой фиксированной операции sbox параметризован значением состояния S_i, где i – номер фиксированной sbox (от 0 до N–1).

Текущее значение состояния $S = \{S_0, S_1, S_2, \ldots, S_{N-1}\}$ задаёт эквивалентный sbox из множества возможных, порождаемых PD-sbox. Число формируемых

8 Maitra, Subhamoy et al. «Salsa20 Cryptanalysis: New Moves and Revisiting Old Styles.» IACR Cryptol. ePrint Arch. 2015 (2015): 217. – URL: https://www.semanticscholar.org/paper/Salsa20-Cryptanalysis%3A-New-Moves-and-Revisiting-Old-Maitra-Paul/8deb80ff7f9cc16a7dd05388927b4a29f1706f62

9 Beaulieu, Ray et al. “SIMON and SPECK: Block Ciphers for the Internet of Things.” IACR Cryptol. ePrint Arch. 2015 (2015): 585. – URL: https://www.semanticscholar.org/paper/SIMON-and-SPECK%3A-Block-Ciphers-for-the-Internet-of-Beaulieu-Shors/06f11891201b321294ffff9d91e3682acb160be6

10 Abed F., List E., Lucks S., Wenzel J. Cryptanalysis of the Speck Family of Block Ciphers. Cryptology ePrint Archive, Paper 2013/568. – 2013. – URL: https://eprint.iacr.org/2013/568

11 Klein A. Attacks on the RC4 stream cipher // Designs, codes and cryptography. – 2008. – Vol. 48, no. 3. – P. 269–286. – DOI: 10.1007/s10623-008-9206-6.

12 Поликарпов С. В., Кожевников А. А. Псевдо-динамические sbox: исследование линейных свойств // Известия ЮФУ. Технические науки. – 2015. – Т. 169, № 8. – С. 19–31. – URL: http://old.izv- tn.tti.sfedu.ru/wp-content/uploads/2015/8/2.pdf.

эквивалентных sbox определено набором возможных значений состояния S, которые могут динамически изменяться в процессе обработки блоков информации, что приведет равномерному распределению вероятностных свойств между порождаемыми sbox.

Структура псевдо-динамической sbox представлена на (рис.1).

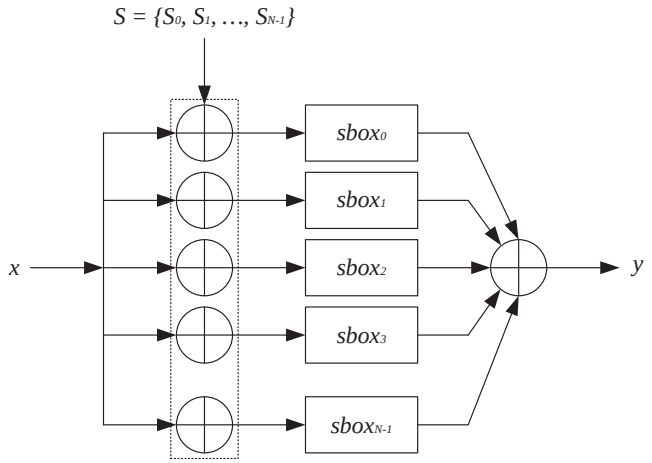


Рис. 1. Структура PD-sbox

Ниже представлено выражение, описывающее структуру псевдо-динамической операции PD-sbox:

$$Y = \oplus_{i=0}^{N-1} \text{sbox}_i (X \oplus S_i), \quad (1)$$

где sbox – фиксированная операция sbox; N – количество фиксированных подстановок; X – биты входного сообщения; Y – биты выходного сообщения; S – биты значения состояния псевдо-динамической sbox; $\oplus$ – операция сложения по модулю 2.

Входное значение каждой фиксированной sbox задаётся индивидуальным значением состояния S_i, где i – номер фиксированной sbox (от 0 до N–1). Текущее значение состояния $S = \{S_0,S_1,S_2,\ldots,S_{N-1}\}$ задаёт одну эквивалентную операцию sbox из всего множества возможных замен псевдо-динамической sbox. На (рис.2) представлена псевдо-динамическая операция sbox в виде набора эквивалентных замен[12].

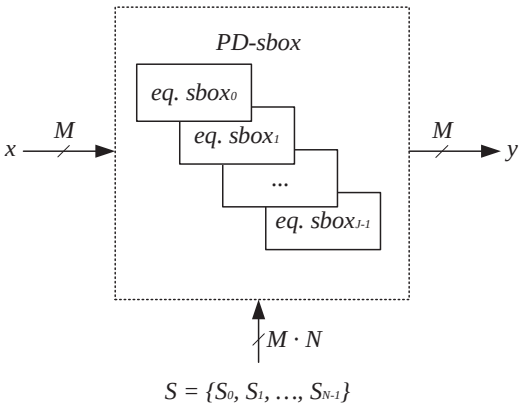


Рис.2. Псевдо-динамическая операция sbox в виде набора эквивалентных нелинейных элементов

Псевдо-динамическая операция sbox способна функционировать в двух режимах: статическом (ключезависимом) и динамическом (выходное значение зависит не только от ключа, но и от промежуточных состояний).

Статический режим работы подразумевает, что значение внутреннего состояния равно нулю или константе. При динамическом режиме работы наблюдается равновероятное изменение значений внутреннего состояния S и в таком случае дифференциальные усреднённые свойства, а также линейные, близки к идеальным (при усреднении характеристик по всем эквивалентным операциям sbox). Данная особенность потенциально позволяет нейтрализовать существующие методы дифференциального и линейного криптоанализа [13].

Анализ свойств псевдо-динамических подстановок

Исследование свойств PD-sbox представлено в следующих трудах.[13]

В работе предложена концепция применения перспективного криптографического примитива – PD-sbox, объединяющих в себе свойства фиксированных sbox (высокая скорость преобразования блока информации и эффективность использования вычислительных ресурсов) и динамических sbox (нейтрализация статистических методов криптоанализа). В работе представлены результаты предварительного криптографического анализа линейных и дифференциальных свойств PD-sbox, которые демонстрируют неэффективность аппроксимации нелинейного элемента набором линейных статистических аналогов, и существенное улучшение разностных свойств криптографического примитива при последовательном увеличении количества фиксированных sbox.

Цель исследования[14] заключалась в разработке методики определения линейных характеристик псевдо-динамических sbox для оценки возможности их применения в блочных криптоалгоритмах. В рамках исследования получены выражения, позволяющие определить линейные свойства PD-sbox. Первичный анализ выражения позволил сделать вывод, что сама структура псевдо-динамической sbox существенно усложняет определение её линейных свойств и препятствует линейному криптоанализу.

Целью в работе[15] являлся анализ линейных характеристик псевдо-динамических операций sbox

13 Поликарпов С. В., Румянцев К. Е., Кожевников А. А. Псевдо-динамические таблицы sbox: основа современных симметричных криптоалгоритмов // Научное обозрение. – 2014. – № 12. – С. 162–166. – URL: http://www.sced.ru/ru/files/7_12_1_2014/7_12_1_2014.pdf.

14 Поликарпов С. В., Румянцев К. Е., Кожевников А. А. Исследование линейных характеристик псевдо-динамических подстановок // Известия ЮФУ. Технические науки. – 2015. – Т. 166, № 5. – С. 111–123. – URL:http ://old.izv-tn.tti.sfedu.ru/wp-content/uploads/2015/5/11.pdf.

15 Поликарпов С. В., Кожевников А. А. Псевдо-динамические sbox: исследование линейных свойств // Известия ЮФУ. Технические науки. – 2015. – Т. 169, № 8. – С. 19–31. – URL: http://old.izv- tn.tti.sfedu.ru/wp-content/uploads/2015/8/2.pdf.

на основе экстраполяции линейных свойств, случайно сформированных малоразмерных PD-sbox. Определение усреднённых значений максимумов смещения позволило упростить анализ полученных результатов и найти закономерность между параметрами псевдо-динамических sbox и вероятностью достижения максимальных значений смещения случайно сформированных PD-sbox. Выявленная закономерность позволила приблизительно экстраполировать линейные свойства малоразмерных псевдо-динамических sbox на линейные свойства полноразмерных PD-sbox.

Исследованию разностных характеристик PD-sbox посвящена работа[16]. Анализ полученных данных показывает, что поочерёдное добавление в состав PD-sbox фиксированных sbox уменьшает вдвое максимальное значение центрированного коэффициента распространения разностных свойств. В свою очередь, распределение отклонений центрированного коэффициента распространения дифференциалов приближается к гауссовому распределению.

В исследовании[17] представлены результаты первоначального анализа псевдо-динамических sbox, имеющих идеальное распределение разностных свойств, при усреднении всех возможных генерируемых sbox в статическом режиме работы (при фиксированных значениях состояния). Доказано существование класса PD-sbox, имеющих идеально усредненное распределение разностных свойств в статическом режиме работы. В [14] представлены первые результаты по исследованию нелинейных свойств эквивалентных sbox, формируемых PD-sbox, состоящими из фиксированных операций sbox размерностью 4 бит. Распределение значений нелинейности для эквивалентных sbox существенно отличается от распределения значений нелинейности фиксированных sbox. Примерно 30 полученных PD-sbox формируют эквивалентные с нелинейностью больше нуля. Путём подбора составляющих PD-sbox можно добиться того, что эквивалентные sbox всегда будут нелинейными.

Развитием структуры псевдо-динамической операции sbox является применение ARX-функций в их составе [15]. Идея заключалась в том, что объединение слабых, с криптографической точки зрения, конструкций, включающих операции сложения по модулю, циклического сдвига и XOR, позволит получить эквивалентные операции sbox, обладающие характеристиками, не уступающим случайно сгенерированным операциям sbox аналогичной размерности. При этом, полученная структура обладает возможностью параллелизма при её использовании в семействе псевдослучайных функций pCollapser. Одним из основных преимуществ этого подхода является сохранение криптографической устойчивости, при значительном сокращении затрачиваемых ресурсов при программной реализации, а также потенциальное увеличение скорости работы функции, в силу использования более простых операций, в отличие от sbox. В свою очередь, применение подобранных ARX-функций для использования в структуре PD-sbox псевдослучайной функции pCollapser позволяет получить вес разностных и линейных характеристик, превосходящий аналоги, при тех же затратах ресурсов при программной реализации.

Описание структуры псевдо-динамической операции PD-sbox на основе ARX-конструкций (PD-sbox-ARX)

Развитием PD-sbox является применение в их составе специально подобранных ARX-функций вместо фиксированных sbox, несмотря на неудовлетворительные криптографические характеристики ARX-конструкций. Использование ARX-функций, в качестве основного нелинейного элемента псевдо-динамической sbox, позволяет существенно уменьшить затраты ресурсов при программной реализации и получить криптографические свойства PD-sbox, аналогичные, использующим фиксированные sbox той же размерности.

В [15] предложен вариант применения специально подобранных ARX-функций в составе псевдо-динамических операций sbox, для последующего их использования в псевдослучайной функции pCollapser, что позволяет обеспечить как параллелизм обработки информации, так и стойкость к статистическим методам криптоанализа и возможность эффективной программной реализации. Основное назначение синтезированной псевдослучайной функции – применение в качестве высокопроизводительной PRF, в режимах, не требующих наличия возможности обратного преобразования, например: AEAD, CTR, Sponge-конструкции.

Структура используемых ARX-функций приведена на (рис.3). Выбор подобной архитектуры функции обусловлен обеспечением криптографических свойств и оптимальным использованием возможностей современных процессоров и аппаратных платформ.

PD-sbox-ARX состоит из четырёх параллельно включённых в её структуру ARX-функций. Размерность входа-выхода PD-sbox соответствует размерности используемых ARX-конструкций.

16 Поликарпов С. В., Румянцев К. Е., Кожевников А. А. Псевдо-динамические таблицы sbox: исследование дифференциальных характеристик // Физико-математические методы и информационные технологии в естествознании, технике и гуманитарных науках. – М., 2014. – С. 77–89.

17 Polikarpov S., Petrov D., Kozhevnikov A. On a class pseudo-dynamic substitutions PD-sbox, with a perfect distribution of averaged differentials in static mode of work // 2017 International Conference on Cryptography, Security and Privacy. – Wuhan, 2017. – P. 17–21. – (ICCSP 2017).

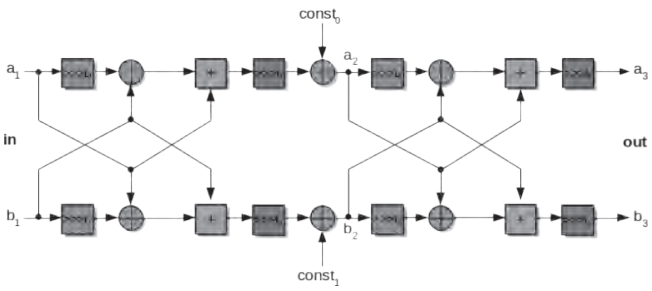


Рис. 3. Структура используемых ARX-функций

На (рис.4) представлена псевдо-динамическая sbox, включающая в свой состав четыре параллельно интегрированных ARX-функции. Размерность входа-выхода PD-sbox соответствует размерности используемых ARX-конструкций.

Выражение, описывающее значение на выходе:

$$c_i = \bigoplus_{j=0}^{3} funcARX_j\,(m_i \oplus s_j^i), \qquad (2)$$

где: i – индекс n-битного слова из входного/выходного вектора и далее индекс PD-sbox; j – индекс компонента PD-sbox ; m_i – n-битные слова из входного вектора; c_i – n-битные слова из выходного вектора; $funcARX$ – ARX-функция (компоненты PD-sbox); s_j^i – n-битные слова из входного вектора управляющего состояния (индивидуальные для каждого PD-sbox) [15].

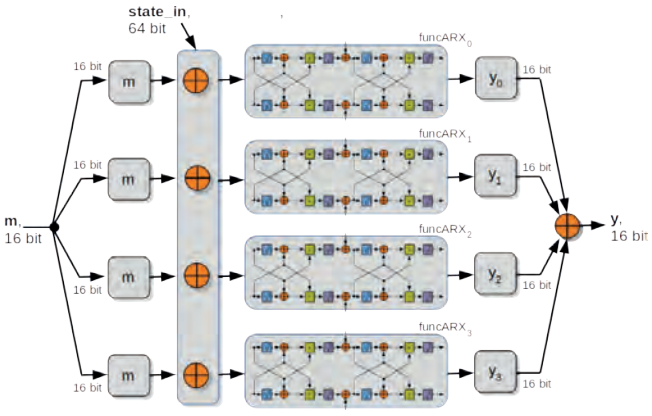


Рис. 4. Псевдо-динамическая операция sbox на основе ARX-конструкций

Выражение, описывающее индивидуальные управляющие состояния на выходе PD-sbox:

$$g_n^i = c_i \oplus funcARX_j\,(m_i \oplus s_j^i) = \bigoplus_{n=0,n\neq i}^{3} funcARX_j\,(m_i \oplus s_j^i). \quad (3)$$

PD-sbox-ARX – перспективное направление развития концепции псевдо-динамических sbox, позволяющее наглядно продемонстрировать возможность достижения криптографических характеристик эквивалентных sbox, не уступающих случайно сформированным нелинейным элементам той же размерности, а также возможность нейтрализации статистических атак при динамическом режиме работы как на сам криптографический примитив, так и на PRF или криптоалгоритм, в которых он может быть применён. Особенностью этой концепции является возможность эффективной программной реализации, которая заключается в оптимальном использовании вычислительных возможностей современных процессоров (AVX-инструкции (Advanced Vector Extensions) и параллельная обработка).

Выводы

В ходе исследования проанализированы существующие подходы к синтезу PD-sbox, а также классических sbox и их вариаций. Стоит отметить, что на текущий момент проблема синтеза sbox как основного нелинейного элемента современных блочных шифров и псевдослучайных функций, удовлетворяющих взаимоисключающим требованиям, является актуальной. Существует ряд способов решения этой проблемы, подразумевающих подбор операций sbox в соответствии с требованиями, реализация нелинейного элемента псевдослучайной функции или криптоалгоритма в качестве ARX-функции, применение динамических sbox в шифрах и синтез PD-sbox, в основе которых могут быть как фиксированные операции sbox, так и ARX-конструкции. К операциям sbox, вне зависимости от их вида, предъявляется около десятка требований, напрямую влияющих на криптографическую стойкость псевдослучайных функций, перестановок и криптоалгоритмов. Следовательно, проблема синтеза sbox, удовлетворяющих широкому спектру взаимоисключающих параметров является базовой.

Представлено описание структуры PD-sbox, а также принцип её работы. Конструкция позволяет обеспечить параллелизм обработки информации при её использовании в составе псевдослучайных функций, псевдослучайных перестановок и криптоалгоритмов, а также потенциально способна нейтрализовать существующие методы разностного и линейного криптоанализа.

Применение псевдо-динамических sbox на базе подобранных ARX-функций, обладающих разностными и линейными свойствами эквивалентных sbox, аналогичным случайно фиксированным нелинейным элементам той же размерности, в псевдослучайных функциях семейства pCollapser потенциально позволяет обеспечить оптимальное использование векторных инструкций процессора и параллелизм обработки информации. Из этого следует сделать вывод о том, что данный подход к синтезу PD-sbox является перспективным и требует проведения дополнительных исследований, посвящённых криптографическому анализу свойств нелинейного элемента, а также исследований их программной и аппаратной реализации, как в формате криптографического примитива, так и в составе псевдослучайных функций семейства pCollapser.

Литература

1. *Sankaralingam, A., Vivek, U. HPAC-sbox a novel implementation of predictive learning classifier and adaptive chaotic s-box for counterfeiting sidechannel attacks in an IOT networks // Microprocessors and Microsystems. 81. 103737. – 2021. DOI: 10.1016/j.micpro.2020.103737.*
2. *Artuğer, F., Karakuş, S., Özkaynak, F. Comparison of Nonlinearity Value of Substitution Box Generation Approaches // International Conference on Recent Academic Studies. – 2023. – Vol.1. – P. 46–49. DOI: 10.59287/icras.670.*
3. *Kökçam, A., Çavuşoğlu, Ü. A new approach to design S-box generation algorithm based on genetic algorithm // International Journal of Bio-Inspired Computation. 2021.– 2021. – Vol.17, No.1. – P. 52–62. DOI: 10.1504/IJBIC.2021.10035835.*
4. *Yang, S., Tong, X.,Wang, Z. S-box generation algorithm based on hyperchaotic system and its application in image encryption // Multimedia Tools and Applications. – 2023. – Vol.82.– P. 25559–25583. DOI: 10.1007/s11042-023-14394-1.*
5. *Marochok, S., Zajac, P. Algorithm for Generating S-Boxes with Prescribed Differential Properties // Algorithms. – 2023. – Vol.16. Issue 3. DOI: 10.3390/a16030157.*
6. *Khadem, B., Rajavzadeh, S. Construction of Side Channel Attack Resistant S-Boxes Using Genetic Algorithms Based on Coordinate Functions // Journal of Electrical and Computer Engineering Innovations (JECEI). – 2022. – Vol.10, No.1. – P. 143–152. DOI: 10.22061/jecei.2021.7801.436.*
7. *Kang, M., Wang, M. New Genetic Operators for Developing S-Boxes With Low Boomerang Uniformity // IEEE Access. – 2022. – Vol.10. – P. 10898–10906. DOI: 10.1109/ACCESS.2022.3144458.*
8. *Siddiqui, N., Yousaf, F., Murtaza, F. et al. A highly nonlinear substitution-box (S-box) design using action of modular group on a projective line over a finite field // PLoS ONE. – 2020. – Vol.15(11). DOI: 10.1371/journal.pone.0241890.*
9. *Coutinho, M., Neto, T. Improved Linear Approximations to ARX Ciphers and Attacks Against ChaCha // Advances in Cryptology – EUROCRYPT 2021. – 2021. – Vol.12696 – P. 711–740. DOI: 10.1007/978-3-030-77870-5_25.*
10. *Beierle, C., Leander, G., Todo, Y. Improved Differential-Linear Attacks with Applications to ARX Ciphers // Journal of Cryptology. – 2022. – Vol.35. DOI: 10.1007/s00145-022-09437-z.*
11. *Liu, J., Rijmen, V., Hu, Y. et al. WARX: efficient white-box block cipher based on ARX primitives and random MDS matrix // Science China Information Sciences. – 2022. – Vol.65. DOI: 10.1007/s11432-020-3105-1.*
12. *Beierle, C., Biryukov, A., Cardoso, D. S. et al. Alzette: A 64-Bit ARX-box (Feat. CRAX and TRAX) // Advances in Cryptology – CRYPTO 2020. 40th Annual International Cryptology Conference, CRYPTO 2020. – 2020. – P. 419–448. DOI: 10.1007/978-3-030-56877-1_15.*
13. *Поликарпов С. В., Прудников В. А., Румянцев К. Е. Исследование свойств миниверсии псевдо-случайной функции pCollapser // Известия ЮФУ. Технические науки. – 2023. – Февраль. – Т. 230, No 6. – С. 148–162.*
14. *Прудников В. А. Исследование нелинейных свойств псевдодинамической sbox PD-SBOX 6x4x4 // Сборник статей V Всероссийской научно-технической конференции молодых ученых, аспирантов, магистрантов и студентов «Фундаментальные и прикладные аспекты компьютерных технологий и информационной безопасности». – Таганрог, 2019. – С. 96–99.*
15. *Поликарпов С. В., Румянцев К. Е., Прудников В. А. Высокопроизводительная псевдослучайная функция pCollapserARX256-32x2 // РусКрипто'2022. – 2022. – URL: https:// www.ruscrypto.ru/ resource/archive/rc2022/ files /02_polikarpov_ rumyantsev_ prudnikov.pdf.*

References

1. *Sankaralingam, A., Vivek, U. HPAC-sbox a novel implementation of predictive learning classifier and adaptive chaotic s-box for counterfeiting sidechannel attacks in an IOT networks // Microprocessors and Microsystems. 81. 103737. – 2021. DOI: 10.1016/j.micpro.2020.103737.*
2. *Artuğer, F., Karakuş, S., Özkaynak, F. Comparison of Nonlinearity Value of Substitution Box Generation Approaches // International Conference on Recent Academic Studies. – 2023. – Vol.1. – P. 46–49. DOI: 10.59287/icras.670.*
3. *Kökçam, A., Çavuşoğlu, Ü. A new approach to design S-box generation algorithm based on genetic algorithm // International Journal of Bio-Inspired Computation. 2021.– 2021. – Vol.17, No.1. – P. 52–62. DOI: 10.1504/IJBIC.2021.10035835.*
4. *Yang, S., Tong, X.,Wang, Z. S-box generation algorithm based on hyperchaotic system and its application in image encryption // Multimedia Tools and Applications. – 2023. – Vol.82.– P. 25559-25583. DOI: 10.1007/s11042-023-14394-1.*
5. *Marochok, S., Zajac, P. Algorithm for Generating S-Boxes with Prescribed Differential Properties // Algorithms. – 2023. – Vol.16. Issue 3. DOI: 10.3390/a16030157.*
6. *Khadem, B., Rajavzadeh, S. Construction of Side Channel Attack Resistant S-Boxes Using Genetic Algorithms Based on Coordinate Functions // Journal of Electrical and Computer Engineering Innovations (JECEI). – 2022. – Vol.10, No.1. – P. 143–152. DOI: 10.22061/jecei.2021.7801.436.*
7. *Kang, M., Wang, M. New Genetic Operators for Developing S-Boxes With Low Boomerang Uniformity // IEEE Access. – 2022. – Vol.10. – P. 10898–10906. DOI: 10.1109/ACCESS.2022.3144458.*
8. *Siddiqui, N., Yousaf, F., Murtaza, F. et al. A highly nonlinear substitution-box (S-box) design using action of modular group on a projective line over a finite field // PLoS ONE. – 2020. – Vol.15(11). DOI: 10.1371/journal.pone.0241890.*
9. *Coutinho, M., Neto, T. Improved Linear Approximations to ARX Ciphers and Attacks Against ChaCha // Advances in Cryptology – EUROCRYPT 2021. – 2021. – Vol.12696 – P. 711–740. DOI: 10.1007/978-3-030-77870-5_25.*
10. *Beierle, C., Leander, G., Todo, Y. Improved Differential-Linear Attacks with Applications to ARX Ciphers // Journal of Cryptology. – 2022. – Vol.35. DOI: 10.1007/s00145-022-09437-z.*
11. *Liu, J., Rijmen, V., Hu, Y. et al. WARX: efficient white-box block cipher based on ARX primitives and random MDS matrix // Science China Information Sciences. – 2022. – Vol.65. DOI: 10.1007/s11432-020-3105-1.*
12. *Beierle, C., Biryukov, A., Cardoso, D. S. et al. Alzette: A 64-Bit ARX-box (Feat. CRAX and TRAX) // Advances in Cryptology – CRYPTO 2020. 40th Annual International Cryptology Conference, CRYPTO 2020. – 2020. – P. 419–448. DOI: 10.1007/978-3-030-56877-1_15.*
13. *Polikarpov S. V., Prudnikov V. A., Rumjancev K. E. Issledovanie svojstv miniversii psevdo-sluchajnoj funkcii pCollapser // Izvestija JuFU. Tehnicheskie nauki. – 2023. – Fevral'. – T. 230, No 6. – S. 148–162.*
14. *Prudnikov V. A. Issledovanie nelinejnyh svojstv psevdodinamicheskoj sbox PD-SBOX 6x4x4 // Sbornik statej V Vserossijskoj nauchno-tehnicheskoj konferencii molodyh uchenyh, aspirantov, magistrantov i studentov «Fundamental'nye i prikladnye aspekty komp'juternyh tehnologij i informacionnoj bezopasnosti». – Taganrog, 2019. – S. 96–99.*
15. *Polikarpov S. V., Rumjancev K. E., Prudnikov V. A. Vysokoproizvoditel'naja psevdosluchajnaja funkcija pCollapserARX256-32x2 // RusKripto'2022. – 2022. – URL: https:// www.ruscrypto.ru/ resource/archive/rc2022/ files /02_polikarpov_ rumyantsev_ prudnikov.pdf.*

ВЫЧИСЛЕНИЯ НАД ПОЛИНОМАМИ В ПОСТКВАНТОВЫХ СХЕМАХ ПОДПИСИ

Иваненко В. Г.[1], Иванова И. Д.[2], Иванова Н. Д.[3]

DOI: 10.21681/2311-3456-2024-4-65-70

Цель исследования: *ускорение операции проверки подписи в постквантовых криптографических системах путем применения к вычислениям над полиномами быстрых алгоритмов.*

Методы исследования: *сравнительный анализ принятых к стандартизации постквантовых алгоритмов, математическое моделирование операции проверки подписи, оптимизация путем синтеза быстрых алгоритмов.*

Результаты исследования: *на основании коммуникационных затрат, стойкости к атакам полным перебором, используемых парадигм и примитивов, и производительности на маломощных устройствах определены области применения схемы подписи Falcon, вследствие чего обоснована важность оптимизации данного алгоритма. Приведено математическое описание задачи, обосновывающей криптостойкость алгоритма Falcon, и определены ресурсоемкие операции над полиномами, применяемые в данной задаче. Рассмотрены алгоритмы, использующиеся для оптимизации операции проверки подписи в эталонной реализации схемы Falcon, и приведено обоснование их неэффективности при внедрении Falcon в маломощные устройства. Предложен метод оптимизации путем синтеза быстрых алгоритмов вычисления числового теоретического преобразования и быстрого алгоритма приведения целого числа по модулю. На основании данного метода разработана реализация оптимизационного алгоритма на языке Си.*

Практическая значимость: *предложенный метод оптимизации не использует архитектурные особенности среды, на которой тестируется данный алгоритм подписи, и не требует хранения дополнительных предвычисленных значений, благодаря чему может иметь широкое применение в различных областях. Разработанная реализация оптимизационного алгоритма на основе предложенного метода оптимизации может быть внедрена в эталонную реализацию схемы Falcon.*

Ключевые слова: *теория решеток, Falcon, оптимизация, NTT, мультипликативная группа, приведение по модулю, алгоритм Монтгомери.*

OPTIMIZATION OF COMPUTATIONS OVER POLYNOMIALS IN POST-QUANTUM SIGNATURE SCHEME

Ivanenko V. G.[4], Ivanova I. D.[5], Ivanova N. D.[6]

The purpose: *accelerating the signature verification in post-quantum cryptographic systems by applying fast algorithms to calculations over polynomials.*

Research methods: *comparative analysis of post-quantum algorithms accepted for standardization, mathematical modeling of the signature verification, optimization by synthesizing fast algorithms.*

Results: *the areas of application of the Falcon signature scheme are determined based on communication costs, resistance to brute-force attacks, the paradigms and primitives used, and performance on low-power devices, as a result the importance of optimization is justified. A mathematical description of the problem that substantiates the Falcon cryptographic strength is given, and resource-intensive operations used in this problem are determined. The algorithms used to optimize the signature verification in the Falcon reference implementation are considered, and the rationale for their ineffectiveness for Falcon in low-power devices is given. An optimization method by synthesizing fast algorithms for calculating the Number Theoretic Transform and a fast reduction algorithm is proposed. Based on this method, an implementation of the optimization algorithm in C language has been developed.*

1 Иваненко Виталий Григорьевич, доктор технических наук, профессор Института Интеллектуальных Кибернетических Систем (ИИКС) Национального исследовательского ядерного университета «МИФИ», г. Москва, Россия. E-mail: VGIvanenko@mephi.ru

2 Иванова Ирина Дмитриевна, магистрант кафедры «Криптология и кибербезопасность» Национального исследовательского ядерного университета «МИФИ», г. Москва, Россия. E-mail: iid.ivanova@yandex.ru, ORCID 0000-0003-3022-8973

3 Иванова Нина Дмитриевна, аспирант кафедры «Управление и защита информации» Российского университета транспорта (МИИТ), г. Москва, Россия. E-mail: IvanovaND.Nina@yandex.ru, ORCID 0000-0001-5942-8050

4 Vitaly G. Ivanenko, Dr.Sc., Associate Professor of the Institute of Intelligent Cybernetic Systems of the National Research Nuclear University «MEPhI», Moscow, Russia. E-mail: VGIvanenko@mephi.ru

5 Irina D. Ivanova, master's student of the Cryptology and Cybersecurity Department at NRNU MEPhI, Moscow, Russia. E-mail: iid.ivanova@yandex.ru, ORCID 0000-0003-3022-8973

6 Nina D. Ivanova, assistant of the Department of Management and Information Security, Russian University of Transport (MIIT), Moscow, Russia. E-mail: IvanovaND.Nina@yandex.ru, ORCID 0000-0001-5942-8050

Practical value: *the proposed optimization method does not use the architectural features of the environment and does not require storing additional precomputed values, due to which it can be widely used in various fields. The developed implementation of the optimization algorithm based on the proposed optimization method can be embedded in the Falcon reference implementation.*

Keywords: *lattice theory, Falcon, NTT, multiplicative group, reduction, Montgomery multiplication.*

Введение

В 1994 году был опубликован квантовый алгоритм Шора[7], в котором предлагается решение задач факторизации и дискретного логарифмирования за полиномиальное время. Это открытие ознаменовало, что в случае реализации алгоритма Шора на квантовом компьютере криптографические схемы, основанные на данных задачах, потеряют свою криптографическую стойкость [1, 2]. В частности использование алгоритма Шора злоумышленником может привести к резкой необходимости увеличения длин ключей в асимметричных схемах до критического уровня, не пригодного для их успешной эксплуатации в реальных информационных системах. Таким образом, изобретение достаточно мощного квантового компьютера повлечет за собой практически полное разрушение секретности и как следствие – глобальный финансовый кризис из-за разрушения банковской сферы и компрометации всех каналов связи [3].

С целью противодействия данной угрозе в 2016 году NIST был открыт прием заявок на участие в конкурсе по стандартизации постквантовых алгоритмов. В июне 2022 года по результатам третьего раунда конкурса к стандартизации были предложены три алгоритма цифровой подписи, среди которых две схемы – Falcon и CRYSTALS-Dilithium – используют криптографию на основе теории решеток.

Следует отметить, что хотя на настоящий момент еще не был создан квантовый компьютер, способный использовать алгоритм Шора, важно уже сейчас разрабатывать план интеграции стандартизованных постквантовых криптографических схем в существующие информационные системы. С этой целью в данной работе проводится сравнительный анализ финалистов NIST среди схем цифровых подписей, использующих криптографию на основе теории решеток, на примере алгоритма Falcon рассматриваются механизмы в устройстве постквантовых цифровых подписей, замедляющие выполнение ими операций создания и проверки подписей, и предлагается метод их оптимизации.

Сравнительный анализ финалистов конкурса NIST

Сравнение алгоритмов Falcon и CRYSTALS-Dilithium проводилось по трем аспектам:

- компромисс между коммуникационными затратами и криптостойкостью цифровой схемы;
- применяемые цифровой схемой криптографические примитивы и парадигмы;
- практическая применимость цифровой схемы.

Коммуникационные затраты криптографической схемы характеризуются длиной открытого ключа и подписи. Хотя с увеличением размеров ключей и подписей иногда удается повысить криптостойкость алгоритма, на практике важным является достижение компромисса между уровнем безопасности и коммуникационными затратами. В работе [4] предлагается оценивать стойкость постквантовых алгоритмов как объем затрат, требуемых квантовому злоумышленнику для проведения успешной атаки полным перебором ключей. Среди подписей-финалистов конкурса NIST у Falcon наименьшие размеры подписей, однако, как показывают эксперименты в работе [4], в сравнении с CRYSTALS-Dilithium данная схема также обладает большей стойкостью к атакам полным переборам.

Применяемые схемами криптографические примитивы и парадигмы не только обосновывают криптостойкость данных алгоритмов, но и являются причиной сложности их реализации [5]. В Falcon применяется парадигма «хеширование и подпись», в соответствии с которой для построения подписей применяется односторонняя функция с потайным входом, использующая нормальное распределение. В то же время схема подписи CRYSTALS-Dilithium применяет протокол Фиата-Шамира с прерываниями[8], использующий одностороннюю функцию на основе задачи нахождения короткого целочисленного решения. Проведение дополнительных раундов генерации подписи в данном алгоритме позволяет использовать равномерный закон распределения.

Хотя представленные на конкурсе NIST реализации цифровых подписей являются по большей части демонстрацией работы алгоритмов и не заявлены как эталонные, при оценке практической применимости Falcon и CRYSTALS-Dilithium можно также использовать их показатели производительности на маломощных устройствах [6].

7 Shor P. Algorithms for quantum computation: discrete logarithms and factoring. DOI:10.1109/SFCS.1994.365700

8 Lyubashevsky V. Fiat-Shamir with Aborts: Applications to Lattice and Factoring-Based Signatures. DOI:10.1007/978-3-642-10366-7_35

Результаты проведенного сравнительного анализа представлены в табл. 1.

Таблица 1.

Сравнительный анализ схем подписи Falcon и CRYSTALS-Dilithium

Параметры сравнения	Falcon	CRYSTALS-Dilithium
Коммуникационные затраты и криптостойкость схемы подписи		
Размеры подписей	На всех уровнях стойкости размеры подписей меньше, чем у CRYSTALS-Dilithium	На всех уровнях стойкости размеры подписей меньше, чем у Falcon
Соотношение коммуникационных затрат и криптографической стойкости	Близок к «идеальному» [4] криптографическому алгоритму (низкие коммуникационные затраты при высоком уровне стойкости)	Показатели уступают Falcon
Криптографические примитивы и парадигмы		
Применяемая для уменьшения размеров ключей и подписей парадигма	Хеширование и подпись (поддерживает восстановление сообщения по подписи)	Протокол Фиата-Шамира с прерываниями
Применяемое распределение вероятностей	Нормальное распределение (сложнее реализуется)	Равномерное распределение (проще реализуется)
Практическая применимость		
Время генерации ключей в реализации, представленной на конкурсе NIST	Требуется больше времени, чем Dilithium	Сравнительно быстро
Время выполнения подписи и проверки в реализации, представленной на конкурсе NIST	Требуется больше времени, чем Dilithium	Сравнительно быстро
Время выполнения подписи и проверки в реализации алгоритма для маломощных устройств [6]	Сравнительно быстро	Требуется больше времени, чем Falcon
Потребление памяти в реализации алгоритма для маломощных устройств [6]	Сравнительно небольшое потребление	Требуется больше ресурсов, чем Falcon

Сложность реализации схемы подписи Falcon обуславливает ее криптостойкость и компактность ее подписей. Данный алгоритм основывается на NTRU-подобных схемах, среди которых – схема шифрования NTRUEncrypt, которая была официально утверждена для использования в сфере финансов комитетом Accredited Standards Committee X9 [7]. Ввиду данных факторов важной является оптимизация данной схемы подписи с целью расширения сфер ее применения.

Операции над полиномами в постквантовых алгоритмах

Алгоритм Falcon основывается на задаче нахождения короткого целочисленного решения (Short Integer Solution, SIS). По условию данной задачи необходимо решить следующую систему уравнений:

$$\begin{cases} \|\vec{x}\| \le \beta \\ f_A(\vec{x}) := A\vec{x} = \vec{0} \in \mathbb{Z}_q^n, \end{cases} \quad (1)$$

где матрица $A = [a_1]...[a_m]$ состоит из случайных векторов из $\mathbb{Z}_q^n$, а $\vec{x}$ – ненулевой вектор из $\mathbb{Z}_q^m$.

В Falcon для создания подписей вместо $f_A(\vec{x})$ применяется односторонняя функция с потайным входом, основанная на NTRU-решетках [8]. При этом данная функция использует операцию умножения полинома на полином, которая технически требует значительных ресурсов при высоких степенях полиномов. В качестве механизма, упрощающего операцию умножения, может применяться числовое теоретическое преобразование (Number Theoretic Transform, NTT) [9]. Очевидно, что полином может быть записан как вектор, содержащий значения коэффициентов при степенях полинома. Потому NTT работает следующим образом:

1. Предполагается, что входной вектор является последовательностью из n неотрицательных целых чисел.
2. В мультипликативной группе $\mathbb{Z}_q$ определяется ω – примитивный корень единицы степени n.
3. Коэффициенты прямого преобразования $\tilde{a} = NTT(a)$ тогда определяются аналогично дискретному преобразованию Фурье как:

$$\tilde{a}_i = \sum_{j=0}^{n-1} a_j \omega^{ij} \bmod q, \quad (2)$$

где a_k – k-ый коэффицент исходного вектора a, $\tilde{a}$ – результирующий вектор, а индекс i проходит по всем координатам вектора $\tilde{a}$ от 0 до $n-1$.

4. Коэффициенты прямого преобразования $a = NTT(\tilde{a})$ определяются как:

$$a_i = \frac{1}{n} \sum_{j=0}^{n-1} \tilde{a}_j \omega^{-ij} \bmod q, \quad (3)$$

где $\tilde{a}$ – вектор, являющийся результатом применения NTT, а – исходный вектор, индекс i проходит по всем координатам вектора a от 0 до $n-1$.

Преобразование NTT, применяемое для круговой свертки векторов, может быть использовано для умножения полиномов в кольце $\mathbb{Z}_q[x]/(x^n-1)$. Если вектор c является круговой сверткой векторов a и $b \in \mathbb{Z}_q[x]/(x^n-1)$, для преобразования NTT выполняется свойство:

$$NTT(c) = NTT(a) \circ NTT(b), \quad (4)$$

где $\circ$ – покомпонентное умножение векторов.

Тогда для вычисления c необходимо применить n-мерные NTT и INTT в соответствии с упомянутым свойством:

$$c = INTT\,(NTT(a) \circ NTT(b)), \quad (5)$$

где $a, b, c \in \mathbb{Z}_q[x]/(x^n-1)$.

Для умножения полиномов в кольцах $\mathbb{Z}_q[x]$ и $\mathbb{Z}_q[x]/(x^n+1)$ используются модификации NTT, основанные на линейных и отрицательно завернутых (negative wrapped) свертках соответственно. В схеме подписи Falcon операции проводятся в кольце $\mathbb{Z}_q[x]/(x^n+1)$, из-за чего применяется следующий алгоритм NTT, основанный на отрицательно завернутых свертках (будем обозначать как NTT^{ψ}):

В мультипликативной группе $\mathbb{Z}_q$ помимо примитивного корня единицы степени n также вводится ψ – примитивный корень единицы степени $2n$ (порядок q должен удовлетворять $q \equiv 1 \bmod 2n$).

Для вектора a:

$$a = (a[0],\ldots,a[n-1]),\ b = (b[0],\ldots,b[n-1]), \quad (6)$$

где $\forall i \in [0,n-1]\ a[i] \in \mathbb{Z}_q$ вводится вектор $\hat{a}$:

$$\hat{a} = (a[0], \psi a[1],\ldots,\psi^{n-1} a[n-1]), \quad (7)$$

где ψ – примитивный корень единицы степени $2n$.

Коэффициенты прямого NTT^{ψ} и обратного $INTT^{\psi}$ преобразований NTT определяются следующим образом:

$$\tilde{a}_i = \sum_{j=0}^{n-1} a_j\, \psi^j\, \omega^{ij} \bmod q,$$

$$a_i = \frac{1}{n}\, \psi^{-j} \sum_{j=0}^{n-1} \tilde{a}_j\, \omega^{-ij} \bmod q,$$

где индекс i проходит по всем координатам вектора $\tilde{a}$ от 0 до $n-1$.

Для NTT^{ψ} аналогично справедливо свойство (4), потому отрицательно завернутую свертку векторов a и $b \in \mathbb{Z}_q[x]/(x^n-1)$ можно вычислить как:

$$c = INTT^{\psi}\,(NTT^{\psi}\,(a) \circ NTT^{\psi}\,(b)). \quad (8)$$

Сложность прямого вычисления циклической (отрицательно завернутой) свертки при помощи NTT (NTT^{ψ}) составляет $O(n^2)$: два преобразования NTT (NTT^{ψ}), одно покомпонентное умножение и одно преобразование INTT ($INTT^{\psi}$). Однако, как и в случае с дискретным преобразованием Фурье, возможно также применение быстрых алгоритмов.

Двумя такими алгоритмами являются алгоритм Кули-Тьюки и Джентльмена-Санде. Общая идея алгоритма Кули-Тьюки заключается в том, что из-за симметрии и периодичности корней из единицы коэффициенты $\tilde{a} = NTT(a)$ могут быть вычислены по формулам:

$$\tilde{a}_i = \tilde{a}_i' + \tilde{a}_i''\, \omega^i \bmod q, \quad (9)$$

$$\tilde{a}_{i+\frac{n}{2}} = \tilde{a}_i' - \tilde{a}_i''\, \omega^i \bmod q, \quad (10)$$

где $\tilde{a}_i = \sum_{j=0}^{\frac{n}{2}-1} a_{2j}\,(\omega^2)^{ij}$ и $\tilde{a}_i'' = \sum_{j=0}^{\frac{n}{2}-1} a_{2j+1}(\omega^2)^{ij}$, а $i = 0,1,\ldots, n/2-1$.

Идею симметричности и периодичности корней из единицы также использует алгоритм Джентльмена-Санде. Данные алгоритмы позволяют снизить сложность вычисления NTT до $O(n \log n)$. Однако хотя оба могут применяться для ускорения прямого и обратного преобразования NTT для циклических сверток, следует отметить, что в случае использования отрицательно завернутых сверток алгоритм Кули-Тьюки можно применить лишь к прямому преобразованию NTT^{ψ}, а алгоритм Джентльмена-Санде – только к обратному преобразованию $INTT^{\psi}$ [10].

Использование данных алгоритмов позволяет понизить сложность вычислений над полиномами, однако на практике существует еще одна проблема: операции по модулю могут быть достаточно затратными при больших значениях порядка q и требовать отдельных алгоритмов ускорения [11].

Оптимизация вычислений над полиномами с помощью алгоритма K-RED

В эталонной реализации Falcon[9], представленной на конкурсе NIST, для ускорения операций умножения по модулю в составе NTT используется алгоритм приведения Монтгомери. При умножении по алгоритму Монтгомери необходимо вычислить q' такое, что:

$$r * r^{-1} - q * q' = 1, \quad (11)$$

и перевести исходные числа a и $b \in \mathbb{Z}_q$ в «область Монтгомери»:

$$\bar{a} = a * r \bmod q, \quad (12)$$

$$\bar{b} = a * r \bmod q, \quad (13)$$

где $r \in \mathbb{Z}_q$ и $(r,q) = 1$.

Как видно из формул (9) и (10), в NTT^{ψ} ($INTT^{\psi}$) алгоритм Монтгомери может быть применен для вычисления $\tilde{a}_i''\psi^{2i+1}$ (аналог $\tilde{a}_i''\omega^i$ из (9) и (10) для отрицательно завернутых сверток) [12]. Поскольку q и ψ^{2i+1} для $i = 0,1,\ldots, n/2-1$ известны изначально и могут быть предварительно переведены в область Монтгомери, значения q' и $\bar{b}$ могут храниться отдельно и не вычисляться дополнительно в процессе проверки подписи. Однако на ограниченных устройствах, для которых

9 Falcon source files (reference implementation). URL: https://falcon-sign.info/impl/vrfy.c.html

Falcon является наилучшим кандидатом на внедрение ввиду малых коммуникационных затрат, это может стать критичным [13].

В Falcon порядок мультипликативный группы для бинарного случая (уровней стойкости 1-й и 5-й соответственно) равен $q = 12289 = 3 * 2^{12} + 1$, вследствие чего при $k = 3$ к NTT может быть применен алгоритм K-RED[10].

Алгоритм K-RED позволяет ускорить приведение целого числа по модулю вида $q = k * 2^m \pm l$, где k, l – малые положительные целые числа такие, что $k \geq 3$ и $l \geq 1$. В ходе алгоритма выполняются следующие шаги:

Число v представляется в виде:

$$v = v_0 + 2m * v_1, \quad (14)$$

где $0 \leq v_0 < 2^m$.

Алгоритм возвращает:

$$kv \equiv kv_0 - v_1 \ mod \ q, \quad (16)$$

Таким образом, в алгоритме приводится не само число v, а kv, поэтому при внедрении данного алгоритма в NTT$^{\psi}$ перед вычислением $\tilde{a}_i''\psi^{2i+1}$ необходимо вычислить:

$$\psi_k^{2i+1} = \psi^{2i+1} * k. \quad (17)$$

В эталонной реализации Falcon, представленной на конкурсе NIST, для вычисления NTT$^{\psi}$ применяется функция mq_NTT. Для ускорения выполнения преобразования используется предвычисленная таблица, обращение к которой происходит как к массиву Gmb и которая содержит степени ψ. Формула (17) может быть записана как:

$$s = mq\_div\_12289(Gmb[m+i], k)$$

При этом функция mq_div_12289 производит деление первого аргумента на второй по модулю q = 12289 (порядок $\mathbb{Z}_q$ для 1-го и 5-го уровней стойкости). В то же время реализация алгоритма K-RED, вызываемого вместо алгоритма Монтгомери mq_montymul для вычисления $\tilde{a}_i''\psi^{2i+1}$, может выглядеть следующим образом:

```
static inline uint32_t K_RED(uint32_t v)
{
    v_0 = v % pow2_m;
    v_1 = (v - v_0) / pow2_m;
    return k * v_0 - v_1;
}
```

В данном объявлении функции $pow2\_m$ и k – константы, хранящие значения 2^{12} и 3 соответственно. Поскольку деление осуществляется на степень 2, на практике это означает сдвиг или отсечение разрядов числа. Данные операции реализуются на вычислительных машинах очень быстро.

Алгоритм K-RED ускоряет вычисление обратного и прямого NTT на языке Си (на котором также была представлена реализация Falcon на NIST) до 2 раз в сравнении с алгоритмом Монтгомери. Кроме того, применение алгоритма K-RED также позволяет уменьшить в 2 раза количество умножений и приведений в процессе масштабирования коэффициентов INTT$^{-\psi}$, что может привести к значительному ускорению выполнения данного алгоритма в сравнении с другими оптимизациями Falcon [12, 14, 15].

С учетом того, что алгоритм Монтгомери требует выходящих за пределы NTT значительных расходов на хранение предвычисленных значений, в будущих исследованиях планируется на практике рассмотреть все преимущества использования алгоритма K-RED в составе Falcon.

Выводы

В результате настоящего исследования предложен метод оптимизации вычислений над полиномами в схеме Falcon. В ходе сравнительного анализа было определено, что для ограниченных и маломощных устройств лучшим кандидатом на внедрение является схема Falcon, вследствие чего была обоснована важность оптимизации данного постквантового алгоритма. По итогам анализа математического аппарата, реализующего вычисления над полиномами в рассматриваемой схеме подписи, было показано, что наиболее ресурсоемкой является операция приведения по модулю. Для ускорения вычислений над полиномами в Falcon в предлагаемом методе оптимизации используется синтез алгоритмов Кули-Тьюки и Джентельмена-Санде с быстрым алгоритмом приведения целого числа по модулю – алгоритмом K-RED.

На основании предложенного метода была написана реализация оптимизационного алгоритма на языке Си, которая может быть внедрена в эталонную реализацию Falcon. В дальнейших исследованиях планируется использовать ее для экспериментального подтверждения теоретических оценок, изложенных в данной работе, и сравнения эффективности предложенного метода оптимизации на разных платформах.

10 Longa P., Naehrig M. Speeding up the Number Theoretic Transform for Faster Ideal Lattice-Based Cryptography. DOI:10.1007/978-3-319-48965-0_8

Литература

1. *Vysotskaya V. V., Chizhov I. V. The security of the code-based signature scheme based on the Stern identification protocol // Прикладная дискретная математика. 2022. № 57. С. 67–90. DOI:10.17223/20710410/57/5*
2. *Asif R. Post-Quantum Cryptosystems for Internet-of-Things: A Survey on Lattice-Based Algorithms // IoT. 2021. Vol. 2. N. 1. P. 71–91. DOI:10.3390/IOT2010005*
3. *Комарова А. В., Коробейников А. Г. Анализ основных существующих пост-квантовых подходов и схем электронной подписи // Вопросы кибербезопасности. 2019. № 2 (30). С. 58–68. DOI: 10.21681/2311-3456-2019-2-58-68*
4. *Raavi M. et al. Security Comparisons and Performance Analyses of Post-Quantum Signature Algorithms // International Conference on Applied Cryptography and Network Security. 2021. Vol. 12727. 24 p. DOI:10.1007/978-3-030-78375-4_17*
5. *Singh S. XCRYPT: Accelerating Lattice Based Cryptography with Memristor Crossbar Arrays // IEEE Micro. 2023. Vol. 43. № 5. P. 45–54. DOI:10.1109/MM.2023.3248080*
6. *Gonzalez R. et al. Verifying Post-Quantum Signatures in 8 kB of RAM // Post-Quantum Cryptography: 12th International Workshop. 2021. P. 215–233. DOI:10.1007/978-3-030-81293-5_12*
7. *Cherckesova L. et al. Post-Quantum Cryptosystem NTRUEnCrypt and Its Advantage over Pre–Quantum Cryptosystem RSA // E3S Web of Conferences. 2020. Vol. 224. P. 01037. DOI:10.1051/e3sconf/202022401037*
8. *Espitau T. et al. Shorter Hash-and-Sign Lattice-Based Signatures // Annual International Cryptology Conference. 2022. P. 245–275. DOI:10.1007/978-3-031-15979-4_9*
9. *Liang Z. et al. Number Theoretic Transform: Generalization, Optimization, Concrete Analysis and Applications // International Conference on Information Security and Cryptology. 2020. P. 415–432. DOI:10.1007/978-3-030-71852-7_28*
10. *Abdulrahman A. et al. Multi-moduli NTTs for saber on Cortex-M3 and Cortex-M4 // Cryptology ePrint Archive. 2021. 33 p. DOI:10.46586/tches.v2022.i1.127-151*
11. *Mert A. C. et al. Design and Implementation of a Fast and Scalable NTT-Based Polynomial Multiplier Architecture // 2019 22nd Euromicro Conference on Digital System Design (DSD). 2019. P. 253–260. DOI:10.1109/DSD.2019.00045*
12. *Becker H. et al. Polynomial multiplication on embedded vector architectures // Cryptology ePrint Archive. 2021. 24 p. DOI:10.46586/tches.v2022.i1.482-505*
13. *Kim Y. et al. Accelerating Falcon on ARMv8 // IEEE Access. 2022. Vol. 10. 15 p. DOI: 10.1109/ACCESS.2022.3169784*
14. *Nguyen D. T., Gaj K. Fast Falcon Signature Generation and Verification Using ARMv8 NEON Instructions // International Conference on Cryptology in Africa. 2023. P. 417–441. DOI: 10.1007/978-3-031-37679-5_18*
15. *Seo E. Y. et al. Peregrine Toward Fastest FALCON Based on GPV Framework // Cryptology ePrint Archive. 2022. 21 p.*

References

1. *Vysotskaya V. V., Chizhov I. V. The security of the code-based signature scheme based on the Stern identification protocol // Prikladnaja diskretnaja matematika. 2022. № 57. S. 67–90. DOI:10.17223/20710410/57/5*
2. *Asif R. Post-Quantum Cryptosystems for Internet-of-Things: A Survey on Lattice-Based Algorithms // IoT. 2021. Vol. 2. N. 1. P. 71–91. DOI:10.3390/IOT2010005*
3. *Komarova A. V., Korobejnikov A. G. Analiz osnovnyh sushhestvujushhih post-kvantovyh podhodov i shem jelektronnoj podpisi // Voprosy kiberbezopasnosti. 2019. № 2 (30). S. 58–68. DOI: 10.21681/2311-3456-2019-2-58-68*
4. *Raavi M. et al. Security Comparisons and Performance Analyses of Post-Quantum Signature Algorithms // International Conference on Applied Cryptography and Network Security. 2021. Vol. 12727. 24 p. DOI:10.1007/978-3-030-78375-4_17*
5. *Singh S. XCRYPT: Accelerating Lattice Based Cryptography with Memristor Crossbar Arrays // IEEE Micro. 2023. Vol. 43. № 5. P. 45–54. DOI:10.1109/MM.2023.3248080*
6. *Gonzalez R. et al. Verifying Post-Quantum Signatures in 8 kB of RAM // Post-Quantum Cryptography: 12th International Workshop. 2021. P. 215–233. DOI:10.1007/978-3-030-81293-5_12*
7. *Cherckesova L. et al. Post-Quantum Cryptosystem NTRUEnCrypt and Its Advantage over Pre–Quantum Cryptosystem RSA // E3S Web of Conferences. 2020. Vol. 224. P. 01037. DOI:10.1051/e3sconf/202022401037*
8. *Espitau T. et al. Shorter Hash-and-Sign Lattice-Based Signatures // Annual International Cryptology Conference. 2022. P. 245–275. DOI:10.1007/978-3-031-15979-4_9*
9. *Liang Z. et al. Number Theoretic Transform: Generalization, Optimization, Concrete Analysis and Applications // International Conference on Information Security and Cryptology. 2020. P. 415–432. DOI:10.1007/978-3-030-71852-7_28*
10. *Abdulrahman A. et al. Multi-moduli NTTs for saber on Cortex-M3 and Cortex-M4 // Cryptology ePrint Archive. 2021. 33 p. DOI:10.46586/tches.v2022.i1.127-151*
11. *Mert A. C. et al. Design and Implementation of a Fast and Scalable NTT-Based Polynomial Multiplier Architecture // 2019 22nd Euromicro Conference on Digital System Design (DSD). 2019. P. 253–260. DOI:10.1109/DSD.2019.00045*
12. *Becker H. et al. Polynomial multiplication on embedded vector architectures // Cryptology ePrint Archive. 2021. 24 p. DOI:10.46586/tches.v2022.i1.482-505*
13. *Kim Y. et al. Accelerating Falcon on ARMv8 // IEEE Access. 2022. Vol. 10. 15 p. DOI: 10.1109/ACCESS.2022.3169784*
14. *Nguyen D. T., Gaj K. Fast Falcon Signature Generation and Verification Using ARMv8 NEON Instructions // International Conference on Cryptology in Africa. 2023. P. 417–441. DOI: 10.1007/978-3-031-37679-5_18*
15. *Seo E. Y. et al. Peregrine Toward Fastest FALCON Based on GPV Framework // Cryptology ePrint Archive. 2022. 21 p.*

СПОСОБ УСИЛЕНИЯ РАНДОМИЗАЦИИ ПОДПИСИ В АЛГОРИТМАХ ЭЦП НА НЕКОММУТАТИВНЫХ АЛГЕБРАХ

Молдовян Д. Н.[1], Костина А. А.[2]

DOI: 10.21681/2311-3456-2024-4-71-81

Цель работы: *устранение уязвимости известных алгебраических алгоритмов ЭЦП с многократным вхождением подписи в проверочное уравнение к потенциальным атакам с использованием множества известных подписей.*

Метод исследования: *известные результаты по изучению строения четырехмерных конечных некоммутативных ассоциативных алгебр применяются для генерации параметров алгоритма ЭЦП. Устранение указанной в цели работы уязвимости реализуется путем усиления рандомизации подписи. Последняя обеспечивается за счет вычисления ЭЦП в зависимости от двух уникальных четырехмерных векторов, принадлежащим двум различным скрытым коммутативным группам четырехмерной некоммутативной алгебры, используемой в качестве алгебраического носителя. выполнение формального доказательства обеспечения почти полной рандомизации ЭЦП.*

Результаты исследования: *доказан ряд математических утверждений, лежащих в основе обоснования выбора параметров алгебраических алгоритмов ЭЦП, стойкость которых основана на вычислительной трудности решения больших систем степенных уравнений. Показано, что вычисление подписи в зависимости от двух уникальных векторов, выбираемых из различных коммутативных подалгебр, обеспечивает почти полную рандомизацию подписи, которая устраняет потенциальные атаки с использованием нескольких известных подписей, по отношению к которым являются уязвимыми известные алгебраические алгоритмы ЭЦП с многократным вхождением подписи в проверочное уравнение. На основе предложенного способа усиления рандомизации разработан алгебраический алгоритм ЭЦП, использующий в качестве алгебраического носителя четырехмерные конечные некоммутативные ассоциативные алгебры. В отличии от известных версий алгоритмов ЭЦП со скрытой группой и удвоенным проверочным уравнением используются две скрытые группы. Дана оценка стойкости к прямой атаке и к подделке подписи.*

Научная и практическая значимость *результатов статьи состоит в разработке и апробации способа усиления рандомизации подписи, перспективного для реализации на его основе практичных постквантовых алгоритмов ЭЦП, стойкость которых определяется вычислительной трудностью решения больших систем степенных уравнений. Предложен конкретный алгоритм такого типа, обладающий сравнительно малыми размерами подписи и открытого и секретного ключей.*

Ключевые слова: *конечная ассоциативная алгебра; некоммутативная алгебра; вычислительно трудная задача; скрытая группа; цифровая подпись; рандомизация цифровой подписи; постквантовая криптография*

A METHOD FOR STRENGTHENING SIGNATURE RANDOMIZATION IN SIGNATURE ALGORITHMS ON NON-COMMUTATIVE ALGEBRAS

Moldovyan D. N.[3], Kostina A. A.[4]

Purpose of work *is eliminating the vulnerability of well-known algebraic signature algorithms with multiple entry of the signature into the verification equation to potential attacks using a variety of well-known signatures.*

Research methods: *known results on the study of the structure of four-dimensional finite non-commutative associative algebras are used to generate parameters of the signature algorithm. The elimination of the said vulnerability is implemented*

1 Молдовян Дмитрий Николаевич, кандидат технических наук, научный сотрудник лаборатории проблем компьютерной безопасности Санкт-Петербургского федерального исследовательского центра Российской академии наук. ORCID: https://orcid.org/0000-0002-4483-5048. Scopus Author ID: 36634567300. E-mail: mdn.spectr@mail.ru

2 Костина Анна Александровна, научный сотрудник лаборатории проблем компьютерной безопасности Санкт-Петербургского федерального исследовательского центра Российской академии наук, Санкт-Петербург, Россия. ORCID: https://orcid.org/0009-0004-5784-7242. Scopus Author ID: 57218870628. E-mail: to.ann@inbox.ru

3 Dmitriy N. Moldovyan, Ph.D. (in Tech.) researcher of laboratory of computer security problems, St. Petersburg Federal Research Center of the Russian Academy of Sciences, St. Petersburg, Russia. ORCID: https://orcid.org/0000-0002-4483-5048. Scopus Author ID: 36634567300. E-mail: mdn.spectr@mail.ru

4 Anna A. Kostina, researcher of laboratory of computer security problems, St. Petersburg Federal Research Center of the Russian Academy of Sciences, St. Petersburg, Russia. ORCID: https://orcid.org/0009-0004-5784-7242. Scopus Author ID: 57218870628. E-mail: to.ann@inbox.ru

by strengthening the randomization of the signature. The latter is provided by calculating the digital signature depending on two unique four-dimensional vectors belonging to two different hidden commutative groups of a four-dimensional non-commutative algebra used as an algebraic support. performing a formal proof of ensuring almost complete randomization of the EDS.

Results of the study: *a number of mathematical statements underlying the justification of the choice of parameters of algebraic signature algorithms, the security of which is based on the computational difficulty of solving large systems of power equations, are proved. It is shown that the calculation of the signature depending on two unique vectors selected from various commutative subalgebras provides almost complete randomization of the signature, which eliminates potential attacks using several known signatures, against which well-known algebraic algorithms of EDS with multiple entry of the signature into the verification equation are vulnerable. Based on the proposed method of randomization enhancement, an algebraic signature algorithm has been developed using four-dimensional finite non-commutative associative algebras as an algebraic support. Unlike the known versions of the signature algorithms with a hidden group and a doubled verification equation, two different hidden groups are used. The assessment of the security to the direct attack and to forging signature attack is given.*

Practical relevance: *the significance of the results of the article consists in the development of a method for enhancing signature randomization, which is attractive for the implementation of practical post-quantum signature algorithms based on it, the security of which being determined by the computational difficulty of solving large systems of power equations. A specific algorithm of this type is proposed, which has relatively small sizes of the signature and of the public and secret keys.*

Keywords: *finite associative algebra; non-commutative algebra; computationally difficult problem; hidden group; digital signature; signature randomization; post-quantum cryptography.*

Введение

Одной из актуальных проблем в области криптографии является разработка практичных постквантовых криптосхем с открытым ключом, в том числе алгоритмов электронной цифровой подписи (ЭЦП) [1, 2]. При построении постквантовых криптосхем должны быть использованы вычислительно сложные задачи, отличные от задач дискретного логарифмирования (ЗДЛ) и факторизации (ЗФ), для решения которых на квантовом компьютере известны полиномиальные алгоритмы[5]. Например, предложены постквантовые двухключевые криптосхемы на группах [3], алгебраических решетках [4], кодах [5], хеш-функциях [6], трудно обратимых отображениях с секретной лазейкой [7, 8] и некоммутативных алгебрах [9, 10].

Стойкость алгоритмов на трудно обратимых нелинейных отображениях основана на вычислительной сложности решения систем многих степенных уравнений (в частности, квадратных и кубических) с многими неизвестными, заданных в конечных полях сравнительно малого порядка [11, 12]. Применение квантового вычислителя для решения этой задачи не дает преимуществ по сравнению с использованием обычных компьютеров, что определяет интерес к ней как к постквантовому примитиву криптоалгоритмов с открытым ключом, в том числе алгоритмов ЭЦП. Последние обладают малым размером подписи и достаточно высокой производительностью при аппаратной и программной реализации, однако их существенным недостатком является чрезвычайно большой размер открытого ключа [13, 14]. Для устранения данного недостатка недавно предложена концепция задания трудно обратимого отображения как операции экспоненцирования в векторных конечных полях [15, 16]. Однако на настоящий момент не предложены конкретные алгоритмы ЭЦП, построенные в рамках этой концепции.

В статьях [17, 18] рассматривается подход к построению алгебраических алгоритмов ЭЦП со скрытой группой, стойкость которых базируется на трудности решения больших систем степенных уравнений в конечных полях, порядок которых имеет достаточно большой размер. Этот подход обеспечивает построение алгоритмов с малым размером подписи и открытого ключа, что делает его перспективным для разработки практичных постквантовых алгоритмов ЭЦП.

Формализация цели исследования

Общей особенностью алгоритмов ЭЦП со скрытой группой, разработанных в рамках парадигмы [17, 18] является использование проверочного уравнения с многократным вхождением подгоночного элемента подписи, представляющего собой некоторый вектор $\mathbf{S}$, вычисляемый в зависимости от рандомизирующего элемента подписи, представляющего собой натуральные число, вычисляемое в зависимости от случайных натуральных чисел, подписываемого документа и секретного ключа. В некоторых алгоритмах такого типа [19, 20] используются несколько рандомизирующих элементов подписи, но их конкатенация может быть рассмотрена как единый рандомизирующий элемент в виде натурального числа e. В статье [21] показано, что многократное вхождение элемента подписи $\mathbf{S}$ в качестве множителя уравнения проверки подлинности ЭЦП требует вычисления

5 Yan S. Y. Quantum Computational Number Theory. – Springer. 2015. – 252 p.

значения $\mathbf{S}$ по формуле $\mathbf{S} = \mathbf{B}^{-1}\mathbf{G}^{n}\mathbf{H}^{d}\mathbf{A}^{-1}$ при фиксированных секретных векторных значениях $\mathbf{A}$, $\mathbf{B}$, $\mathbf{G}$ и $\mathbf{H}$, где $\mathbf{G}$ и $\mathbf{H}$ образуют базис скрытой коммутативной группы, и уникальных натуральных значениях n и d. Последние задают рандомизацию вектора $(\mathbf{G}^{n}\mathbf{H}^{d})$, который имеет уникальное значение для каждой вычисляемой подписи. Однако, число различных значений $(\mathbf{G}^{n}\mathbf{H}^{d})$ ограничено порядком скрытой группы, которая существенно меньше порядка мультипликативной группы алгебры, используемой в качестве алгебраического носителя. Это задает неустранимую неполноту рандомизации подписи в алгоритмах [17–20], которая, как показано в [21], приводит к снижению ожидаемого уровня стойкости.

Для устранения неполноты рандомизации в работе [21] предложен способ обеспечения полной рандомизации подписи в алгоритмах ЭЦП, стойкость которых основана на вычислительной сложности решения больших систем степенных уравнений. В способе [21] используется прием удвоения проверочного уравнений, вычисление подгоночного элемента подписи по формуле $\mathbf{S} = \mathbf{B}^{-1}\mathbf{G}^{n}\mathbf{H}^{d}\mathbf{V}$, где $\mathbf{V}$ – случайный обратимый вектор. Последняя формула обеспечивает достаточную полноту рандомизации, однако для обеспечения стойкости к подделке подписи на основе известной подписи и использования вектора $\mathbf{S}$ в качестве подгоночного параметра атаки в каждом из двух проверочных уравнений используются два разных множителя, вычисляемые как различные 256-битные степени некоторого известного вектора $\mathbf{J}$. Такие же множители используются в процедуре генерации ЭЦП. Необходимость выполнения дополнительных операций экспоненцирования приводит к снижению производительности процедуры генерации (верификации) ЭЦП на 50% (40%).

В данной статье решается задача повышения производительности алгоритма ЭЦП с полной рандомизацией подписи путем разработки и использования нового способа обеспечения усиленной рандомизации подписи и векторных хеш-функций.

1. Свойства используемых алгебраических носителей

В разрабатываемой схеме ЭЦП в качестве алгебраического носителя предполагается использование конечных некоммутативных ассоциативных алгебр (КНАА) размерности $m \geq 4$, заданных над простым конечным полем $GF(p)$ по так называемым таблицам умножения базисных векторов (ТУБВ), с помощью которых определяется операция векторного умножения (умножение всевозможных пар векторов, результатом которого является вектор). Определение последней детально представлено в [21]. Вектор $\mathbf{V}$ будем обозначать в виде упорядоченного набора его координат (элементов поля $GF(p)$): $\mathbf{V} = (v_0, v_1, v_2, v_3)$.

Известны различные типы КНАА, например, включающие большое множество глобальных левосторонних [22] или большое множество глобальных правосторонних единиц [22, 23]. Далее будут рассматриваться КНАА, включающие глобальную двухстороннюю единицу, которая является единственной, хотя она может иметь достаточно разнообразный вид, определяемый ТУБВ, по которой задается операция векторного умножения. Известен способ унифицированного задания КНАА с глобальной двухсторонней единицей произвольных четных размерностей $m \geq 6$ [24]. Задание разнообразных четырехмерных КНАА с глобальной двухсторонней единицей представлено в работах [24, 25].

Для построения схемы ЭЦП и оценки ее стойкости важным является знание строения КНАА как декомпозиции на множество коммутативных подалгебр. В настоящее время строение КНАА достаточно хорошо изучено для случая размерности $m = 4$ [26, 27]. В связи с этим в разрабатываемом далее алгоритме ЭЦП в качестве его носителя предполагается использование четырехмерной КНАА с глобальной двухсторонней единицей. Исследования показали, что все такие КНАА имеют одинаковое строение, независимо от вида ТУБВ, по которой они задаются. Поэтому для использования в качестве алгебраического носителя предпочтительным является случай задания таких алгебр по прореженным ТУБВ, представленным, например, в [26, 27]. Этот выбор определяется тем, что для такого случая выполнение одной операции умножения векторов сводится к осуществлению всего 8 операций умножения в поле $GF(p)$, тогда как при использовании обычной ТУБВ потребуется выполнить 16 операций умножения в поле.

Результаты исследования строения различных четырехмерных КНАА с глобальной двухсторонней единицей [26–28] обобщаются следующим образом:

1. Множество четырехмерных векторов как элементов КНАА разбивается на $\eta = p^2 + p + 1$ коммутативных подалгебр порядка p^2, которые пересекаются строго в множестве скалярных векторов $\mathbf{L} = \alpha\mathbf{E}$, где $\mathbf{E}$ – единичный вектор (глобальная двухсторонняя единица) и $\alpha \in GF(p)$. Эти подалгебры будем называть K-подалгебрами.
2. Существуют три типа указанных подалгебр:
   2.1. Подалгебры, мультипликативная группа которых имеет циклическое строение и порядок $\Omega_1 = p^2 - 1$ (обозначим такую группу как $\Gamma 1$). Число таких K-подалгебр равно

$$\eta_1 = 2^{-1}p(p-1) \qquad (1)$$

   и каждая из них изоморфна полю $GF(p^2)$.

2.2. Подалгебры, мультипликативная группа которых (группа типа Γ2) имеет двухмерное циклическое строение (т. е. их базис включает два вектора одинакового порядка $p - 1$) и порядок $\Omega_2 = (p-1)^2$. Число таких K-подалгебр равно

$$\eta_2 = 2^{-1}p(p+1). \quad (2)$$

Каждая из подалгебр данного типа содержит $2p - 1$ необратимых векторов.

2.3. Подалгебры, мультипликативная группа которых (группа типа Γ3) имеет циклическое строение и порядок $\Omega_3 = p\,(p-1)$. Число таких K-подалгебр равно

$$\eta_3 = p + 1. \quad (3)$$

Каждая из подалгебр данного типа содержит p необратимых векторов.

3. Координаты каждого из векторов $\mathbf{V} = (v_0, v_1, v_2, v_3)$, принадлежащих заданной коммутативной подалгебре, могут быть вычислены по координатам некоторого фиксированного вектора $\mathbf{C} = (c_0, c_1, c_2, c_3)$, содержащегося в подалгебре и отличного от скалярного вектора, и по уникальной паре скалярных переменных $k,t \in GF(p)$. Вид формулы, описывающей координаты v_0, v_1, v_2 и v_3 зависит от ТУБВ, по которой задается КНАА, и от типа мультипликативной группы заданной подалгебры. Например, для мультипликативных групп типа Γ1 и Γ2 имеем следующую формулу [27]:

$$\mathbf{V} = (v_0, v_1, v_2, v_3) = (k, kc_1c_0^{-1}, t, t + k(c_3 - c_2)c_0^{-1}), \quad (4)$$

4. Порядок мультипликативной группы КНАА, заданной над полем $GF(p)$, равен

$$\Omega = p(p-1)\,(p^2-1). \quad (5)$$

Два вектора $\mathbf{A}$ и $\mathbf{B}$ будем называть перестановочными, если $\mathbf{AB} = \mathbf{BA}$, и неперестановочными, если $\mathbf{AB} \neq \mathbf{BA}$. Докажем несколько утверждений, которые используются в предлагаемом способе усиления рандомизации подписи и при построении приводимой далее схемы ЭЦП.

Утверждение 1. Пусть оба вектора $\mathbf{A}$ и $\mathbf{B}$ обратимы и $\mathbf{AB} \neq \mathbf{BA}$. Тогда из равенства $\mathbf{A}^i\mathbf{B}^j = \mathbf{A}^k\mathbf{B}^t$ следует $i \equiv k \bmod \omega_\mathbf{A}$ и $j \equiv t \bmod \omega_\mathbf{B}$, где $\omega_\mathbf{A}$ ($\omega_\mathbf{B}$) – порядок вектора $\mathbf{A}$ ($\mathbf{B}$).

Доказательство. $\{\mathbf{A}^i\mathbf{B}^j = \mathbf{A}^k\mathbf{B}^t\} \Rightarrow \{\mathbf{A}^{i-k}\mathbf{B}^{j-t} = \mathbf{E}\} \Rightarrow \{\mathbf{A}^{i-k} = \mathbf{E};\ \mathbf{B}^{j-t} = \mathbf{E}\} \Rightarrow \{i \equiv k \bmod \omega_\mathbf{A};\ j \equiv t \bmod \omega_\mathbf{B}\}$.

Утверждение 2. Пусть четырехмерные векторы $\mathbf{A}$ и $\mathbf{B}$ обратимы и $\mathbf{AB} \neq \mathbf{BA}$. Тогда: 1) из равенства $\mathbf{A}^i\mathbf{B} = \mathbf{A}^k\mathbf{B}$ следует $i \equiv k \bmod \omega_\mathbf{A}$; 2) если $i \neq k \bmod \omega_\mathbf{A}$, то $(\mathbf{A}^i\mathbf{B})(\mathbf{A}^k\mathbf{B}) \neq (\mathbf{A}^k\mathbf{B})(\mathbf{A}^i\mathbf{B})$.

Доказательство.

1. Первое положение следует непосредственно из доказанного утверждения 1. $\mathbf{A}^i\mathbf{B}^j = \mathbf{A}^k\mathbf{B}^t$

2. Предположим противное: $(\mathbf{A}^i\mathbf{B})(\mathbf{A}^k\mathbf{B}) = (\mathbf{A}^k\mathbf{B})(\mathbf{A}^i\mathbf{B})$. Тогда имеем $\mathbf{A}^i\mathbf{B}\,\mathbf{A}^k = \mathbf{A}^k\mathbf{B}\mathbf{A}^i \Rightarrow \mathbf{A}^{i-k}\mathbf{B} = \mathbf{B}\mathbf{A}^{i-k}$. Также очевидно, что $\mathbf{A}^{i-k}\mathbf{A} = \mathbf{A}\mathbf{A}^{i-k}$. Последние два равенства означают, что векторы $\mathbf{B}$ и $\mathbf{A}$ содержатся в K-подалгебре, содержащей вектор $\mathbf{A}^{i-k}$ (см. утверждения 2 и 3 в [26] или утв. 2 в [27]), откуда следует $\mathbf{AB} = \mathbf{BA}$, что противоречит условию $\mathbf{AB} \neq \mathbf{BA}$. Полученное противоречие доказывает положение 2.

Утверждение 3. Пусть векторы $\mathbf{A}$, $\mathbf{B}$ и $\mathbf{C}$ обратимы и отличны от скалярных векторов, причем $(\mathbf{AC})\mathbf{B} \neq \mathbf{B}(\mathbf{AC})$. Тогда из неравенства $i \neq k \bmod \omega_\mathbf{B}$, следует $(\mathbf{AB}^i\mathbf{C})(\mathbf{AB}^k\mathbf{C}) \neq (\mathbf{AB}^k\mathbf{C})(\mathbf{AB}^i\mathbf{C})$.

Доказательство. Предположим противное: $(\mathbf{AB}^i\mathbf{C})(\mathbf{AB}^k\mathbf{C}) = (\mathbf{AB}^k\mathbf{C})(\mathbf{AB}^i\mathbf{C})$. Тогда имеем $\mathbf{B}^i\mathbf{CAB}^k = \mathbf{B}^k\mathbf{CAB}^i \Rightarrow \mathbf{B}^{i-k}(\mathbf{CA}) = (\mathbf{CA})\mathbf{B}^{i-k}$. Последнее равенство означает, что векторы $\mathbf{B}^{i-k}$ и $(\mathbf{CA})$ содержатся в одной K-подалгебре. Очевидно, что векторы $\mathbf{B}^{i-k}$ и $\mathbf{B}$ содержатся в этой же подалгебре, из чего (см. утв. 2 и 3 в [26]) следует $(\mathbf{AC})\mathbf{B} = \mathbf{B}(\mathbf{AC})$, что противоречит условию $(\mathbf{AC})\mathbf{B} \neq \mathbf{B}(\mathbf{AC})$. Полученное противоречие доказывает утверждение 3.

Утверждение 4. Пусть векторы $\mathbf{A}$ и $\mathbf{B}$ обратимы и $\mathbf{AB} \neq \mathbf{BA}$. Тогда для всех пар натуральных значений i и k, таких, что $i \neq k \bmod \omega_\mathbf{B}$ векторы $\mathbf{AB}^i\mathbf{A}$ и $\mathbf{AB}^k\mathbf{A}$ принадлежат различным K-подалгебрам.

Доказательство. Справедливость утверждения 4 следует непосредственно из доказанного утверждения 3.

Утверждение 5. Пусть векторы $\mathbf{A}$, $\mathbf{B} \neq \mathbf{A}$ и $\mathbf{F}$ обратимы и отличны от скалярных векторов, причем $\mathbf{AB} = \mathbf{BA}$, $\mathbf{AF} \neq \mathbf{FA}$ и $\mathbf{BF} \neq \mathbf{FB}$. Тогда векторы $\mathbf{FA}$ и $\mathbf{FB}$ неперестановочны, т.е. $(\mathbf{FA})(\mathbf{FB}) \neq (\mathbf{FB})(\mathbf{FA})$.

Доказательство. Предположим противное: $(\mathbf{FA})(\mathbf{FB}) = (\mathbf{FB})(\mathbf{FA})$. Тогда имеем $\mathbf{AFB} = \mathbf{BFA} \Rightarrow \mathbf{B}^{-1}\mathbf{AF} = \mathbf{FAB}^{-1} \Rightarrow (\mathbf{B}^{-1}\mathbf{A})\mathbf{F} = \mathbf{F}(\mathbf{B}^{-1}\mathbf{A})$. Следовательно, векторы $\mathbf{F}$ и $(\mathbf{B}^{-1}\mathbf{A})$ принадлежат одной и той же K-подалгебре (см. утв. 2 и 3 в [26]). Вектор $\mathbf{A}$, очевидно, тоже принадлежит той же подалгебре, т. е. $\mathbf{AF} = \mathbf{FA}$, что противоречит условию $\mathbf{AF} \neq \mathbf{FA}$. Полученное противоречие доказывает утверждение 5.

Утверждение 6. Пусть дано разрешимое уравнение $\mathbf{A} = \mathbf{XBX}^{-1}$ с неизвестным вектором $\mathbf{X}$, где векторы $\mathbf{A}$ и $\mathbf{B} \neq \mathbf{A}$ обратимы и отличны от скалярных векторов. Тогда указанное уравнение имеет количество решений, равное порядку мультипликативной группы K-подалгебры, содержащей вектор $\mathbf{B}$, и каждое решение $\mathbf{X}_i$ принадлежит уникальной $\mathbf{K}$-подалгебре.

Доказательство. Разрешимость уравнения $\mathbf{A} = \mathbf{XBX}^{-1}$ означает существование некоторого

решения $\mathbf{X}_0$. Каждый обратимый вектор $\mathbf{V}$ K-подалгебры, содержащей вектор $\mathbf{B}$, задает уникальное решение $\mathbf{X} = \mathbf{X}_0\mathbf{V}$. Действительно, имеем $(\mathbf{X}_0\mathbf{V})\mathbf{B}(\mathbf{X}_0\mathbf{V})^{-1} = \mathbf{X}_0\mathbf{V}\mathbf{B}\mathbf{V}^{-1}\mathbf{X}_0^{-1} = \mathbf{X}_0\mathbf{B}\mathbf{V}\mathbf{V}^{-1}\mathbf{X}_0^{-1} = \mathbf{X}_0\mathbf{B}\mathbf{X}_0^{-1} = \mathbf{A}$. Таким образом, имеем столько уникальных решений, сколько имеется обратимых векторов в рассматриваемой K-подалгебре. Докажем, что других решений нет. Пусть имеется решение $\mathbf{X}_i$. Тогда имеем: $\{\mathbf{X}_i\mathbf{B}\mathbf{X}_i^{-1} = \mathbf{X}_0\mathbf{B}\mathbf{X}_0^{-1}\} \Rightarrow \{(\mathbf{X}_0^{-1}\mathbf{X}_i)\mathbf{B} = \mathbf{B}(\mathbf{X}_0^{-1}\mathbf{X}_i);\ \mathbf{X}_i = \mathbf{X}_0(\mathbf{X}_0^{-1}\mathbf{X}_i)\}$. Последние два равенства показывают, что любое решение $\mathbf{X}_i$ представимо в виде произведения решения $\mathbf{X}_0$ на вектор $(\mathbf{X}_0^{-1}\mathbf{X}_i)$, который перестановочен с $\mathbf{B}$, т. е. содержится в мультипликативной группе K-подалгебры, содержащей вектор $\mathbf{B}$.

Пусть имеются решения $\mathbf{X}_i$ и $\mathbf{X}_j \neq \mathbf{X}_i$. При фиксированном решении $\mathbf{X}_0$ имеем $\mathbf{X}_i = \mathbf{X}_0(\mathbf{X}_0^{-1}\mathbf{X}_i)$ и $\mathbf{X}_j = \mathbf{X}_0(\mathbf{X}_0^{-1}\mathbf{X}_j)$, где $\mathbf{X}_0^{-1}\mathbf{X}_i$ и $\mathbf{X}_0^{-1}\mathbf{X}_j$ принадлежат одной и той же K-подалгебре, а значит являются перестановочными. В силу утверждения 5 векторы $\mathbf{X}_i$ и $\mathbf{X}_j$ принадлежат разным K-подалгебрам, т. е. каждое решение содержится в уникальной K-подалгебре.

Утверждение 7. Пусть в уравнении $\mathbf{A} = \mathbf{X}\mathbf{G}\mathbf{X}^{-1}$ с неизвестными векторами $\mathbf{X}$ и $\mathbf{G}$ вектор $\mathbf{A}$ обратим и отличен от скалярного вектора, причем указанное уравнение имеет решения. Тогда решения с различными значениями переменной $\mathbf{G}$ не пересекаются по переменной $\mathbf{X}$.

Доказательство. Согласно утверждению 6 при фиксированном $\mathbf{G}$ имеется множество различных решений $(\mathbf{X}_i,\ \mathbf{G})$, отличающихся значениями $\mathbf{X}_i$. Пусть пары векторов $(\mathbf{X}_1,\ \mathbf{G}_1)$ и $(\mathbf{X}_2,\ \mathbf{G}_2)$ являются двумя различными решениями, в которых $\mathbf{G}_1 \neq \mathbf{G}_2$. Тогда предположение о равенстве $\mathrm{X}_1 = \mathrm{X}_2$ приводит к равенствам $\mathbf{X}_1\mathbf{G}_1\mathbf{X}_1^{-1} = \mathbf{X}_2\mathbf{G}_2\mathbf{X}_2^{-1}$ и $\mathbf{G}_1 = \mathbf{G}_2$, что противоречит условию $\mathbf{G}_1 \neq \mathbf{G}_2$.

Утверждение 8. Количество различных значений вектора $\mathbf{G}$, при которых уравнение $\mathbf{A} = \mathbf{X}\mathbf{G}\mathbf{X}^{-1}$ имеет решения равно $\approx p^2$, где $\mathbf{A}$ – обратимый вектор, отличный от скалярных векторов; p – порядок поля $GF(p)$, над которым задана четырехмерная КНАА с глобальной двухсторонней единицей.

Доказательство. Для каждого обратимого вектора $\mathbf{X}$ имеется некоторое $\mathbf{G} = \mathbf{X}^{-1}\mathbf{A}\mathbf{X}$. Согласно утверждению 6 при фиксированном $\mathbf{G}$ уравнение $\mathbf{A} = \mathbf{X}\mathbf{G}\mathbf{X}^{-1}$ имеет количество решений, равное порядку мультипликативной группы K-подалгебры, содержащей вектор $\mathbf{G}$, т.е. $\approx p^2$ различных значений $\mathbf{X}$, удовлетворяющих последнему уравнению. С учетом утверждения 7 и значения порядка мультипликативой группы КНАА, равного $\approx$p4, приходим к выводу, что формула $\mathbf{G} = \mathbf{X}^{-1}\mathbf{A}\mathbf{X}$ генерирует $\approx p^4/p^2 \approx p^2$ различных значений $\mathbf{G}$ при условии, что $\mathbf{X}$ пробегает все обратимые значения КНАА.

2. Способ усиления рандомизации

Для усиления рандомизации подписи в алгебраических алгоритмах со скрытой группой предлагается использование двух различных скрытых коммутативных групп, относящихся к разным K-подалгебрам, содержащих мультипликативную группу типа $\Gamma 1$. Пусть такие группы зафиксированы выбором двух обратимых неперестановочных векторов $\mathbf{G}$ и $\mathbf{P}$, порядок которых равен $\omega_\mathbf{G} = \omega_\mathbf{P} = p2 - 1$.Тогда в соответствии с утверждением 1 произведения всевозможных степеней векторов $\mathbf{G}$ и $\mathbf{P}$ пробегают $(p^2 - 1)^2 \approx p^4$ различных значений в четырехмерной КНАА, используемой в качестве алгебраического носителя. Действительно утверждение 1 показывает, что уникальной паре степеней $i \equiv k \bmod \omega_\mathbf{G}$ и $j \equiv t \bmod \omega_\mathrm{P}$ соответствует уникальный вектор $\mathbf{P}^j\mathbf{G}^i$.

С учетом этого предлагается следующая формула для вычисления подгоночного элемента подписи:

$$\mathbf{S} = \mathbf{D}\mathbf{P}^b\mathbf{G}^n\mathbf{F}^{-1}, \qquad (6)$$

где $\mathbf{D}$ и $\mathbf{F}$ – обратимые векторы, являющиеся элементами секретного ключа; натуральные числа $n < p^2 - 1$ и $b < p^2 - 1$ вычисляются в зависимости от рандомизирующих параметров ЭЦП. Поскольку секретные векторы $\mathbf{D}$ и $\mathbf{F}$ являются фиксированными, легко показать, что значения вектора $\mathbf{S}$ пробегают столько разных обратимых значений КНАА, сколько разных значений пробегает вектор $\mathbf{P}^b\mathbf{G}^n$, т. е. $\mathbf{S}$ потенциально принимает $\approx p^4$ различных значений. Этот способ существенно усиливает рандомизацию ЭЦП по сравнению с алгоритмами [17–20].

Атака, направленная на вычисление секретных векторов $\mathbf{D}$ и $\mathbf{F}$ по z известным подписям, предполагает составление системы скалярных уравнений, в которой число уравнений равно (или примерно равно) числу неизвестных. С учетом того, что вектор $\mathbf{P}^b\mathbf{G}^n$ принимает случайным образом почти все обратимые значения в КНАА, формулу (6) можно представить в виде $\mathbf{S} = \mathbf{D}\mathbf{V}\mathbf{F}^{-1}$, где $\mathbf{V}$ – уникальная векторная неизвестная, а $\mathbf{D}$ и $\mathbf{F}$ – фиксированные неизвестные, т.е. присутствующие в квадратном векторном уравнении, соответствующим каждой из z известных подписей. Таким образом, для z подписей имеем систему из z квадратных векторных уравнений с $z + 2$ векторными неизвестными. При любом числе подписей число неизвестных больше числа уравнений, однако, учитывая то, что уравнения не являются линейными можно предположить, что ограниченные решения могут быть вычислены, если число уравнений на 5% или 10% будет меньше числа неизвестных, т.е. для случая $z = 0{,}95(z + 2)$ или $z = 0{,}9(z + 2)$, соответственно, откуда получаем $z = 38$ или $z = 18$. При сведении системы векторных уравнений к системе скалярных уравнений получаем систему из 152 или

Таблица 1.

Минимальное число уравнений обеспечивающее вычислительную сложность W решения системы из z квадратных уравнений

Порядок поля GF(q)	$W = 2^{80}$	$W = 2^{100}$	$W = 2^{128}$	$W = 2^{192}$	$W = 2^{256}$
q = 16	30	39	51	80	110
q = 31	28	36	48	75	103
q = 256	26	33	43	68	93

72 квадратных уравнений в поле $GF(p)$ со 160 или 80 скалярными неизвестными, соответственно.

Показанный факт получения в ходе атаки на основе известных подписей систем уравнений, в которых число неизвестных существенно превышает число уравнений можно трактовать как формальное доказательство обеспечения предложенным способом почти полной рандомизации подписи.

В табл. 1 приведены оценки[6] вычислительной сложности решения систем из z квадратных уравнений, заданных в полях различного порядка. С учетом этих данных получаем оценку стойкости предложенного механизма усиленной рандомизации $W > 2^{192}$, что позволяет утверждать, что он не будет вносить слабости к атаке на основе известных подписей.

3. Алгоритм ЭЦП на основе разработанного способа усиленной рандомизации подписи

В качестве алгебраического носителя зададим одну из известных четырехмерных КНАА, заданных над простым конечным полем $GF(p)$ по прореженным ТУБВ [25, 27]. В качестве порядка возьмем простое число $p = 2q + 1$, такое, что q является 128-битным простым числом. В предложенном способе усиленной рандомизации подписи предполагается использование генераторов $\mathbf{G}$ и $\mathbf{P}$ двух разных скрытых циклических групп, которые не перестановочны между собой. Это определяет определенную специфику процедур формирования открытого ключа, а также генерации и верификации подписи, хотя использование приемов удвоения проверочного уравнения и задания элементов открытого ключа как замаскированных элементов скрытой группы остается, как и в алгоритме-аналоге из работы [21], в котором используется одна скрытая коммутативная группа.

В предлагаемом далее алгоритме используется условие необратимости векторов, конкретный вид которого зависит от ТУБВ, по которой определяется операция умножения в КНАА, поэтому далее предполагается, что используется прореженная ТУБВ, приводимая в [27] и определяющая следующее условие обратимости (необратимости) четырехмерных векторов $\mathbf{V} = (v_0, v_1, v_2, v_3)$:

$$\lambda v_0,\ v_1 \neq v_2 v_3 \quad (\lambda v_0,\ v_1 = v_2 v_3) \tag{7}$$

6 Ding J., Petzoldt A. Current State of Multivariate Cryptography. IEEE Security and Privacy Magazine. 2017, vol. 15, no. 4, pp. 28–36.

Формирование открытого ключа

Открытый ключ формируется в виде набора, включающего 32-байтное число ψ и 8 векторов $\mathbf{Y}_1$, $\mathbf{T}_1$, $\mathbf{Z}_1$, $\mathbf{L}_1$, $\mathbf{Y}_2$, $\mathbf{T}_2$, $\mathbf{Z}_2$, $\mathbf{L}_2$, $\mathbf{U}$ и $\mathbf{Q}$ (с суммарным размером ≈672 байт) по следующему алгоритму:

1. Сгенерировать векторы $\mathbf{G}$ и $\mathbf{P}$ порядка $p^2 - 1$, такие, что $\mathbf{GP} \neq \mathbf{PG}$.

2. Сгенерировать случайные обратимые векторы $\mathbf{A}$, $\mathbf{B}$, $\mathbf{D}$, $\mathbf{F}$, $\mathbf{K}$ и $\mathbf{N}$, принадлежащие разным K-подалгебрам, отличным от подалгебр, содержащих векторы $\mathbf{G}$ и $\mathbf{P}$. В результате получаем 8 секретных векторов $\mathbf{A}$, $\mathbf{B}$, $\mathbf{D}$, $\mathbf{F}$, $\mathbf{K}$, $\mathbf{N}$, $\mathbf{G}$, и $\mathbf{P}$, которые попарно неперестановочны и имеют общий размер ≈512 байт.

3. Сгенерировать случайные натуральные числа $x < p^2 - 1$, $u < p^2 - 1$ и $w < p^2 - 1$, причем x является взаимно простым с $p^2 - 1$. Затем вычислить значение $z = \psi^{-1} \bmod (p^2 - 1)$ следующие векторы:

$$\mathbf{Y}_1 = \mathbf{AGA}^{-1};\ \mathbf{T}_1 = \mathbf{AG}^u\mathbf{P}^w\mathbf{B}^{-1};\ \mathbf{Z}_1 = \mathbf{BPB}^{-1};$$
$$\mathbf{L}_1 = \mathbf{BP}^u\mathbf{D}^{-1};\ \mathbf{U} = \mathbf{DP}^x\mathbf{D}^{-1}; \tag{8}$$

$$\mathbf{Y}_2 = \mathbf{KG}^z\mathbf{K}^{-1};\ \mathbf{T}_2 = \mathbf{KG}^u\mathbf{P}^u\mathbf{N}^{-1};\ \mathbf{Z}_2 = \mathbf{NP}^z\mathbf{N}^{-1};$$
$$\mathbf{L}_2 = \mathbf{NP}^w\mathbf{D}^{-1};\ \mathbf{Q} = \mathbf{FG}^x\mathbf{F}^{-1}; \tag{9}$$

Натуральные 32-байтные числа x, u и w и векторы $\mathbf{A}$, $\mathbf{B}$, $\mathbf{D}$, $\mathbf{G}$, $\mathbf{F}$, $\mathbf{K}$, $\mathbf{N}$ и $\mathbf{P}$ являются элементами секретного ключа, имеющего общий размер ≈608 байт.

Алгоритм генерации ЭЦП

Алгоритм вычисления ЭЦП к документу M включает следующие шаги:

1. Сгенерировать случайное натуральные число $k < p^2 - 1$ и вычислить значения векторов $\mathbf{R}_1$ и $\mathbf{R}_2$ по следующим формулам:

$$\mathbf{R}_1 = \mathbf{AG}^k\mathbf{F}^{-1},\ \mathbf{R}_2 = \mathbf{KG}^k\mathbf{F}^{-1}. \tag{10}$$

3. Вычислить хеш-значение от документа M с присоединенными к нему векторами $\mathbf{R}_1$ и $\mathbf{R}_2$: $e = e_1 \| e_2 = \mathrm{H}(\mathrm{M}, \mathbf{R}_1, \mathbf{R}_2)$, где 256-битное хеш-значение e представлено в виде конкатенации двух 128-битных натуральных чисел e_1 и e_2.

4. Сгенерировать случайное натуральное число $n < (p^2 - 1)$.

5. Вычислить степень b: $b = -(w + e + u + e_1e_2x) \bmod (p^2 - 1)$.

6. Вычислить подгоночный элемент ЭЦП **S** по формуле (6): $\mathbf{S} = \mathbf{DP}^b\mathbf{G}^n\mathbf{F}^{-1}$.

7. Вычислить вспомогательный рандомизирующий элемент ЭЦП σ по формуле $\sigma = H(\mathbf{S})$, т. е. σ является хеш-значением от подгоночного элемента **S**.

8. Вычислить вспомогательный подгоночный элемент в виде целого числа s по формуле $s = (k - \sigma - u - n)x^{-1} \bmod (p^2 - 1)$.

Подписью к документу M является тройка значений $(e_1||e_2,\ s,\ \mathbf{S})$ с общим размером ≈128 байт. Вычислительная сложность алгоритма генерации подписи примерно равна трем операциям возведения четырехмерных векторов в 256-битную степень или ≈9200 операций умножения в поле $GF(p)$.

Алгоритм верификации ЭЦП

Подпись $(e_1||e_2,\ s,\ \mathbf{S})$ к документу M выполняется по открытому ключу и включает следующие шаги:

1. Вычислить значения векторов $\mathbf{R}_1$ и $\mathbf{R}_2$ по следующим формулам:

$$\mathbf{R}_1' = \mathbf{Y}_1^{\sigma}\mathbf{T}_1\mathbf{Z}_1^{e}\mathbf{L}_1\mathbf{U}^{e_1e_2}\mathbf{SQ}^{s};$$
$$\mathbf{R}_2' = \mathbf{Y}_2'^{\sigma\psi}\mathbf{T}_2\mathbf{Z}_2^{e\psi}\mathbf{L}_2\mathbf{U}^{e_1e_2}\mathbf{SQ}^{s}. \qquad (11)$$

2. Вычислить хеш-функцию от документа M с присоединенными векторами $\mathbf{R}_1$ и $\mathbf{R}_2$: $\varepsilon_1||\varepsilon_2 = H(M, \mathbf{R}_1, \mathbf{R}_2)$, где 256-битное хеш-значение представлено в виде конкатенации двух 128-битных натуральных чисел ε_1 и ε_2.

3. Если выполняются равенства $\varepsilon_1 = e_1$ и $\varepsilon_2 = e_2$, то ЭЦП принимается как подлинная, иначе подпись отвергается как ложная.

Вычислительную сложность процедуры верификации ЭЦП можно грубо оценить как 4 операции возведения четырехмерных векторов в 256-битную степень, для чего надо осуществить ≈12300 операций умножения по модулю p. Покажем корректность работы предложенной схемы ЭЦП как то, что корректно сгенерированная ЭЦП $(e_1||e_2,\ \mathbf{S})$ проходит процедуру верификации как подлинная подпись к документу M.

Доказательство корректности схемы ЭЦП

По первому уравнению в формулах (11) вычисляем значение вектора $\mathbf{R}_1'$:

$$\mathbf{R}_1' = (\mathbf{AGA}^{-1})^{\sigma}\mathbf{AG}^{u}\mathbf{P}^{w}\mathbf{B}^{-1}(\mathbf{BPB}^{-1})^{e}\mathbf{BP}^{u}\mathbf{D}^{-1}(\mathbf{DP}^{x}\mathbf{D}^{-1})^{e_1e_2}$$
$$(\mathbf{DP}^{b}\mathbf{G}^{n}\mathbf{F}^{-1})\,(\mathbf{FG}^{x}\,\mathbf{F}^{-1})^{s} = \mathbf{AG}^{\sigma+u}\,\mathbf{P}^{w+e+u+xe_1e_2+b}\,\mathbf{G}^{n+xs}\,\mathbf{F}^{-1} =$$
$$= \mathbf{AG}^{\sigma+u}\,\mathbf{P}^{0}\,\mathbf{G}^{n+x(k-\sigma-u-n)\,x^{-1}}\,\mathbf{F}^{-1} = \mathbf{AG}^{\sigma+u}\,\mathbf{G}^{n+k-\sigma-u-n}\,\mathbf{F}^{-1} =$$
$$= \mathbf{AG}^{k}\,\mathbf{F}^{-1} = \mathbf{R}_1;$$

По второму уравнению (11) вычисляем значение вектора $\mathbf{R}_2'$ и значение $\varepsilon_1||\varepsilon_2 = H(M, \mathbf{R}_1', \mathbf{R}_2')$ и сравниваем $\varepsilon_1||\varepsilon_2$ со значением $e_1||e_2 = H(M, \mathbf{R}_1, \mathbf{R}_2)$:

$$\mathbf{R}_2' = (\mathbf{KG}^{z}\mathbf{K}^{-1})^{\sigma\psi}\,\mathbf{KG}^{u}\mathbf{P}^{u}\mathbf{N}^{-1}\,(\mathbf{NP}^{z}\mathbf{N}^{-1})^{e\psi}\,\mathbf{NP}^{w}\mathbf{D}^{-1}$$
$$(\mathbf{DP}^{x}\mathbf{D}^{-1})^{e_1e_2}\,(\mathbf{DP}^{b}\mathbf{G}^{n}\mathbf{F}^{-1})\,(\mathbf{FG}^{x}\mathbf{F}^{-1})^{s} =$$
$$= \mathbf{KG}^{z\sigma\psi+u}\mathbf{P}^{u+ze\psi+w+xe_1e_2+b}\,\mathbf{G}^{n+xs}\,\mathbf{F}^{-1} =$$
$$= \mathbf{KG}^{\sigma+u}\mathbf{P}^{0}\,\mathbf{G}^{n+x(k-\sigma-u-n)\,x^{-1}}\,\mathbf{F}^{-1} =$$
$$= \mathbf{KG}^{\sigma+u}\mathbf{G}^{n+k-\sigma-u-n}\mathbf{F}^{-1} = \mathbf{KG}^{k}\mathbf{F}^{-1} = \mathbf{R}_2;$$

Два последних равенства показывают, что проверяемая подпись прошла процедуру верификации как подлинная ЭЦП.

4. Обсуждение

Прямой атакой на предложенный алгоритм ЭЦП является вычисление секретного ключа по открытому. Поскольку каждый элемент открытого ключа зависит не от всех элементов открытого ключа, то актуальным является вопрос о вычислении секретного ключа по частям, т.е. можно ли свести решение системы квадратных векторных уравнений, составленной по формулам (8) и (9), к решению систем меньшего размера. Пара векторов $\mathbf{G}^u$ и $\mathbf{G}^x$ определяется вектором **G** и неизвестными u и x, поэтому их следует рассматривать как независимые неизвестные. Тройка векторов $\mathbf{P}^u$, $\mathbf{P}^x$ и $\mathbf{P}^w$ определяется вектором **P** и неизвестными u, x и w, поэтому их также следует рассматривать как самостоятельные неизвестные (иначе вместо системы степенных уравнений пришлось бы рассматривать систему, включающую степенные и экспоненциальные уравнения).

Также в качестве самостоятельных неизвестных следует рассматривать векторы $\mathbf{G}^z$ и $\mathbf{P}^z$. Однако при переходе от векторных уравнений к скалярным каждый из векторов $\mathbf{G}^u$, $\mathbf{G}^x$, $\mathbf{P}^u$, $\mathbf{P}^x$, $\mathbf{P}^w$, $\mathbf{G}^z$ и $\mathbf{P}^z$ будет привносить только две независимые скалярные неизвестные, поскольку его координаты могут быть выражены по формуле (4) через координаты вектора **G** (или вектора **P**) и две скалярные неизвестные $k,t \in GF(p)$. При этом степень скалярных уравнений увеличивается на единицу, однако это не так сильно влияет на сложность решения системы степенных уравнений, как число уравнений и неизвестных в системе уравнений, заданных в поле $GF(p)$.

Каждое из четырех векторных уравнений (8) включает две или три неизвестные и при переходе от одного уравнения к другому появляются два или три других неизвестных. Аналогичная ситуация имеет место и в векторных уравнениях (9). При переходе от одного из уравнений (8) к одному из уравнений (9) появляются, по крайней мере, две новые неизвестные, вовлекаемые в рассмотрение. Таким образом, система, включающая все 10 уравнений (8) и (9), не распадается на независимые системы с меньшим числом уравнений, т. е. вычисление неизвестных по частям предположительно не может быть реализовано.

Наиболее близкими к возможности раздельного вычисления неизвестных является система из пары уравнений $\mathbf{Y}_1 = \mathbf{AGA}^{-1}$ и $\mathbf{Y}_2 = \mathbf{KG}^{z}\mathbf{K}^{-1}$. Согласно утверждению 8, каждое из двух последних уравнений имеют $\approx p^2$ решений. Решения каждого из этих уравнений попадают в уникальные K-подалгебры.

Пусть $\mathbf{G}'$ и $\mathbf{G}''$ некоторые решения первого и второго уравнений соответственно, которые перестановочны (принадлежат одой K-подалгебре), т. е. $\mathbf{G}'\mathbf{G}'' = \mathbf{G}''\mathbf{G}'$. Возводя значение $\mathbf{G}'$ в степень z, можно проверить выполнимость условия $\mathbf{G}'^{z} = \mathbf{G}''$. Найдя пару значений $\mathbf{G}'$ и $\mathbf{G}''$, для которых выполняется последнее равенство, мы устанавливаем значение $\mathbf{G} = \mathbf{G}'$. Однако вычислительная трудоемкость процесса перебора составляет ≈2256 операций экспоненцирования. Кроме того, для установленных значений $\mathbf{G}$ для первого уравнения (и $\mathbf{G}^{z}$ для второго уравнения) имеются $\approx p^2$ решений, отличающихся значением вектора $\mathbf{A}$ (и $\mathbf{K}$).

Таким образом, для вычисления элементов секретного ключа по элементам открытого ключа предпочтительным с вычислительной точки зрения является решение системы уравнений следующего вида:

$$\begin{cases} \mathbf{Y}_1\mathbf{A} = \mathbf{AG};\ \mathbf{T}_1\mathbf{B} = \mathbf{AG}^{u}\mathbf{P}^{w};\ \mathbf{Z}_1\mathbf{B} = \mathbf{BP}; \\ \mathbf{L}_1\mathbf{D} = \mathbf{BP}^{u};\ \mathbf{Y}_2\mathbf{K} = \mathbf{KG}^{z};\ \mathbf{T}_2\mathbf{N} = \mathbf{KG}^{u}\mathbf{P}^{u}; \\ \mathbf{Z}_2\mathbf{N} = \mathbf{NP}^{z};\ \mathbf{L}_2\mathbf{D} = \mathbf{NP}^{w};\ \mathbf{UD} = \mathbf{DP}^{x};\ \mathbf{QF} = \mathbf{FG}^{x}.) \end{cases} \quad (12)$$

Эта система включает 10 степенных (квадратных и кубических) векторных уравнений с 15 неизвестными. При сведении решения этой системы векторных уравнений к системе скалярных уравнений координаты 8 неизвестных векторов задают 32 независимые скалярные неизвестные, а 7 векторных неизвестных ($\mathbf{G}^{u}$, $\mathbf{G}^{x}$, $\mathbf{P}^{u}$, $\mathbf{P}^{x}$, $\mathbf{P}^{w}$, $\mathbf{G}^{z}$ и $\mathbf{P}^{z}$) задают по две независимые скалярные неизвестные (координаты этих семи неизвестных выражаются по формуле (4) через координаты неизвестных $\mathbf{G}$ и $\mathbf{P}$ и пару скалярных значений $k,t \in GF(p)$.

Получаем систему из 40 степенных (квадратных, кубических и четвертой степени) скалярных уравнений с 46 скалярными неизвестными. Ожидаемая множественность решений показывает существование многих эквивалентных секретных ключей, однако нахождение одного из них можно оценить как вычислительную сложность решения системы из 40 степенных уравнений с 40 неизвестными (например, шести скалярным неизвестным присваиваем произвольные скалярные значения), заданной в поле $GF(p)$. С учетом данных табл. 1 и 129-битной разрядности p [11] получаем ожидаемую стойкость разработанного алгоритма к прямой атаке, равную $W > 2^{128}$.

В разработанном алгоритме ЭЦП реализован в полной мере предложенный в разделе 2 алгоритм усиленной рандомизации, поэтому его стойкость к атакам на основе известных подписей соответствует оценкам из раздела 2: $W > 2^{192}$.

Для получения более высокого уровня стойкости может быть использована реализация предложенного алгоритма на КНАА больших размерностей, например, $m = 6$ и $m = 10$ с ожидаемым уровнем стойкости (к прямой атаке и к подделке подписи) не менее 2192 и 2256 соответственно.

Сопоставление с алгоритмом-аналогом из статьи [21] представлено в табл. 2, из которой видно, что достоинство предложенного алгоритма состоит в более высокой производительности (на 66%). Несмотря на существенное уменьшение числа операций возведения в степень, осуществляемых в разработанном алгоритме, не было достигнуто более существенного увеличения производительности из-за того, что размер степени в нем увеличен в два раза по сравнению с алгоритмом из [21].

Для предложенного алгоритма является актуальным рассмотрение атаки по подделке подписи с использованием известных подлинных подписей. Определяющем в обеспечении стойкости к данной атаке является разнесение в проверочных уравнениях элементов открытого ключа $\mathbf{Y}_1$ (и $\mathbf{Y}_2$) и $\mathbf{U}$ по разные стороны от подгоночного элемента подписи $\mathbf{S}$ и использование вспомогательного рандомизирующего параметра σ, вычисляемого как хеш-функция от $\mathbf{S}$ (последнее требует использования вспомогательного подгоночного элемента s). Детальное рассмотрение этой атаки дает оценку стойкости $W \geq 2^{128}$ (решение системы уравнений (12) и последующее вычисление значения x (как дискретного логарифма в уравнении $(\mathbf{A}^{-1}\mathbf{Y}_1\mathbf{A})^{x} = \mathbf{F}^{-1}\mathbf{QF}$, после чего подделка подписи становится вычислительно выполнимой).

Таблица 2.

Сравнение с алгоритмом-аналогом из статьи [21]

Алгоритм	Размер открытого ключа, байт	Размер секретного ключа, байт	Размер подписи, байт	Производительность, отн. ед.	
				генерация	верификация
из статьи [23]	512	480	128	6,5	8,1
из раздела 3	672	608	128	10,8	8,1

Выводы

Предложен способ усиления рандомизации подписи в алгебраических алгоритмах ЭЦП со скрытой группой и разработан новый алгоритм, отличающийся использованием двух скрытых коммутативных групп, элементы которых не перестановочны между собой, благодаря чему обеспечивается достаточная полнота рандомизации подписи. Выполненный анализ стойкости W предложенного алгоритма к прямой атаке и к подделке подписи дал значение $W \geq 2^{128}$, которое приемлемо для многих применений. Представляет интерес реализация предложенного алгоритма на КНАА размерностей m = 6, 8 и 10, что потенциально обеспечивает существенное повышение уровня стойкости. Однако в этом случае для обоснования достигаемого уровня стойкости потребуется выполнение исследования строения таких алгебр, что представляет собой самостоятельную задачу.

Исследование выполнено за счет гранта Российского научного фонда № 24-21-00225, https://rscf.ru/project/24-21-00225/

Литература

1. *Post-Quantum Cryptography. 13th International Conference, PQCrypto 2022, Virtual Event, September 28–30, 2022, Proceedings // Lecture Notes in Computer Science. 2022. V. 13512. Springer, Cham.*
2. *Post-Quantum Cryptography. 14th International Conference, PQCrypto 2023, College Park, MD, USA, August 16–18, 2023, Proceedings // Lecture Notes in Computer Science. 2023. V. 14154. Springer, Cham.*
3. *Battarbee C., Kahrobaei D., Perret L., Shahandashti S. F. SPDH-Sign: Towards Efficient, Post-quantum Group-Based Signatures // In: Johansson, T., Smith-Tone, D. (eds) Post-Quantum Cryptography. PQCrypto 2023 / Lecture Notes in Computer Science, 2023. V. 14154. P. 113–138. Springer, Cham. https://doi.org/10.1007/978-3-031-40003-2_5*
4. *Gärtner J. NTWE: A Natural Combination of NTRU and LWE // In: Johansson, T., Smith-Tone, D. (eds) Post-Quantum Cryptography. PQCrypto 2023 / Lecture Notes in Computer Science, 2023, vol 14154, pp. 321–353. Springer, Cham. https://doi.org/10.1007/978-3-031-40003-2_12*
5. *Kosolapov Y. V., Turchenko O. Y. On the construction of a semantically secure modification of the McEliece cryptosystem. Prikladnaya diskretnaya matematika [Applied discrete mathematics]. 2019, no. 45, pp. 33–43. DOI: 10.17223/20710410/45/4*
6. *Hamlin B., Song F. Quantum Security of Hash Functions and Property-Preservation of Iterated Hashing // In: Ding, J., Steinwandt, R. (eds) Post-Quantum Cryptography. PQCrypto 2019 / Lecture Notes in Computer Science. 2019. V. 11505. P. 329–349. Springer, Cham. https://doi.org/10.1007/978-3-030-25510-7_18*
7. *Ding J., Petzoldt A., Schmidt D. S. Multivariate Cryptography // In: Multivariate Public Key Cryptosystems. Advances in Information Security. 2020. V. 80. Springer, New York, NY. https://doi.org/10.1007/978-1-0716-0987-3_2*
8. *Ding J., Petzoldt A., Schmidt D. S. The Matsumoto-Imai Cryptosystem // In: Multivariate Public Key Cryptosystems. Advances in Information Security. 2020. V. 80. P. 25–60. Springer, New York, NY. https://doi.org/10.1007/978-1-0716-0987-3_3*
9. *Moldovyan N. A., Moldovyan A. A. Digital signature scheme on the 2x2 matrix algebra // Вестник Санкт_петербургского университета. Прикладная математика. Информатика. Процессы управления. 2021. Т. 17. Вып. 3. С. 254–261. https://doi.org/10.21638/11701/spbu10.2021.303*
10. *Moldovyan N. A., Moldovyan A. A. Candidate for practical post-quantum signature scheme // Вестник Санкт-Петербургского университета. Прикладная математика. Информатика. Процессы управления. 2020. Т. 16. Вып. 4. С. 455–461. https://doi.org/10.21638/11701/spbu10.2020.410*
11. *Ikematsu Y., Nakamura S., Takagi T. Recent progress in the security evaluation of multivariate public-key cryptography // IET Information Security. 2022. P. 1–17. DOI: 10.1049/ise2.12092*
12. *Ding J., Petzoldt A., Schmidt D. S. Solving Polynomial Systems // In: Multivariate Public Key Cryptosystems. Advances in Information Security. Springer. New York. 2020. V. 80. P. 185–248. https://doi.org/10.1007/978-1-0716-0987-3_8*
13. *Cartor R., Cartor M., Lewis M., Smith-Tone D. IPRainbow // In: Cheon, J.H., Johansson, T. (eds) Post-Quantum Cryptography // Lecture Notes in Computer Science. 2022. V. 13512. P. 170-184. Springer, Cham. https://doi.org/10.1007/978-3-031-17234-2_9*
14. *Ding, J., Petzoldt, A., Schmidt, D.S. Oil and Vinegar // In: Multivariate Public Key Cryptosystems. Advances in Information Security. 2020. V. 80. P. 89–151. Springer, New York, NY. https://doi.org/10.1007/978-1-0716-0987-3_5*
15. *Молдовян А. А., Молдовян Д. Н., Молдовян Н. А. Новый подход к разработке алгоритмов многомерной криптографии // Вопросы кибербезопасности. 2023. № 2(54). С. 52–64. DOI:10.21681/2311-3456-2023-2-52-6*
16. *Moldovyan A. A., Moldovyan N. A. Vector finite fields of characteristic two as algebraic support of multivariate cryptography // Computer Science Journal of Moldova. 2024. V.32. N.1(94). P. 46–60. DOI: 10.56415/csjm.v32.04*
17. *Молдовян Д. Н., Молдовян А. А., Молдовян Н. А. Новая концепция разработки постквантовых алгоритмов цифровой подписи на некоммутативных алгебрах // Вопросы кибербезопасности. 2022. № 1(47). С. 18–25. DOI: 10.21681/2311-3456-2022-1-18-25.*
18. *Молдовян Д. Н., Молдовян А. А. Алгебраические алгоритмы ЭЦП, основанные на трудности решения систем уравнений // Вопросы кибербезопасности. 2022. № 2(48). С. 7–17. DOI: 10.21681/2311-3456-2022-2-7-17.*
19. *Молдовян А. А., Молдовян Н. А. Алгоритмы ЭЦП на конечных некоммутативных алгебрах над полями характеристики два // Вопросы кибербезопасности. 2022. № 3(49). С. 58–68. DOI: 10.21681/2311-3456-2022-3-58-68.*

20. *Moldovyan N. A. Algebraic signature algorithms with a hidden group, based on hardness of solving systems of quadratic equations // Quasigroups and Related Systems. 2022. V. 30. N. 2(48). P. 287–298. DOI: https://doi.org/10.56415/qrs.v30.24*
21. *Молдовян А. А., Молдовян Д. Н., Костина А. А. Алгебраические алгоритмы ЭЦП с полной рандомизацией подписи // Вопросы кибербезопасности. 2024. № 2(60). С. 95–102. DOI: 10.21681/2311-3456-2024-2-95-102.*
22. *Moldovyan N. A., Moldovyan A. A. Finite Non-commutative Associative Algebras as carriers of Hidden Discrete Logarithm Problem // Вестник ЮУрГУ. Серия Математическое моделирование и программирование. 2019. Т. 12, № 1. С. 66–81. DOI: 10.14529/mmp190106*
23. *Moldovyan N. A. Finite Non-commutative Associative Algebras for Setting the Hidden Discrete Logarithm Problem and Post-quantum Cryptoschemes on Its Base // Bulletin of Academy of Sciences of Moldova. Mathematics. 2019. No. 1 (89). P. 71–78.*
24 *Moldovyan A. A., Moldovyan N. A. Post-quantum signature algorithms with a hidden group and doubled verification equation. Informatsionno-upravliaiushchie sistemy [Information and Control Systems], 2023, no. 3, pp. 59–69. doi:10.31799/1684-8853-2023-3-59-69.*
25. *Moldovyan A. A., Moldovyan N. A. Post-quantum algebraic signature algorithms with a hidden group. Информационно-управляющие системы, 2023, no. 1(122), pp. 29–40. doi:10.31799/1684-8853-2023-1-29-40.*
26. *Moldovyan N. A., Moldovyan A. A. Structure of a 4-dimensional algebra and generating parameters of the hidden logarithm problem // Вестник Санкт-Петербургского университета. Прикладная математика. Информатика. Процессы управления. 2022. Т. 18. Вып. 2. С. 209–217. https//doi.org/10.21638/11701/spbu10.2022.202*
27. *Moldovyan D. N., Moldovyan A. A., Moldovyan N. A. Structure of a finite non-commutative algebra set by a sparse multiplication table // Quasigroups and Related Systems. 2022, vol. 30, no. 1, pp. 133 – 140. https://doi.org/10.56415/qrs.v30.11*
28. *Moldovyan N. A., Moldovyan A. A. Digital signature scheme on the 2x2 matrix algebra // Вестник Санкт_петербургского университета. Прикладная математика. Информатика. Процессы управления. 2021. Т. 17. Вып. 3. С. 254–261. https://doi.org/10.21638/11701/spbu10.2021.303*

References

1. *Post-Quantum Cryptography. 13th International Conference, PQCrypto 2022, Virtual Event, September 28–30, 2022, Proceedings. Lecture Notes in Computer Science. 2022. V. 13512. Springer, Cham.*
2. *Post-Quantum Cryptography. 14th International Conference, PQCrypto 2023, College Park, MD, USA, August 16–18, 2023, Proceedings // Lecture Notes in Computer Science. V. 14154. Springer, Cham.*
3. *Battarbee C., Kahrobaei D., Perret L., Shahandashti S. F. SPDH-Sign: Towards Efficient, Post-quantum Group-Based Signatures // In: Johansson, T., Smith-Tone, D. (eds) Post-Quantum Cryptography. PQCrypto 2023 / Lecture Notes in Computer Science, 2023, vol. 14154, pp. 113–138. Springer, Cham. https://doi.org/10.1007/978-3-031-40003-2_5*
4. *Gärtner J. NTWE: A Natural Combination of NTRU and LWE. In: Johansson, T., Smith-Tone, D. (eds) Post-Quantum Cryptography. PQCrypto 2023 / Lecture Notes in Computer Science, 2023, vol 14154, pp. 321–353. Springer, Cham. https://doi.org/10.1007/978-3-031-40003-2_12*
5. *Ding J., Petzoldt A., Schmidt D. S. Multivariate Cryptography // In: Multivariate Public Key Cryptosystems. Advances in Information Security. 2020. V. 80. Springer, New York, NY. https://doi.org/10.1007/978-1-0716-0987-3_2.*
6. *Hamlin B., Song F. Quantum Security of Hash Functions and Property-Preservation of Iterated Hashing. In: Ding, J., Steinwandt, R. (eds) Post-Quantum Cryptography. PQCrypto 2019 / Lecture Notes in Computer Science. 2019, vol. 11505, pp. 329–349. Springer, Cham. https://doi.org/10.1007/978-3-030-25510-7_18*
7. *Ding J., Petzoldt A., Schmidt D. S. Multivariate Cryptography. In: Multivariate Public Key Cryptosystems. Advances in Information Security. 2020, vol.. 80. Springer, New York, NY. https://doi.org/10.1007/978-1-0716-0987-3_2*
8. *Ding J., Petzoldt A., Schmidt D. S. The Matsumoto-Imai Cryptosystem. In: Multivariate Public Key Cryptosystems. Advances in Information Security. 2020, vol. 80, pp. 25-60. Springer, New York, NY. https://doi.org/10.1007/978-1-0716-0987-3_3*
9. *Moldovyan N. A., Moldovyan A. A. Digital signature scheme on the 2x2 matrix algebra. Vestnik of Saint Petersburg University. Applied Mathematics. Computer Science. Control Processes, 2021, vol. 17, iss. 3, pp. 254–261. https://doi.org/10.21638/11701/spbu10.2021.303*
10. *Moldovyan N. A., Moldovyan A. A. Candidate for practical post-quantum signature scheme. Vestnik of Saint Petersburg University. Applied Mathematics. Computer Science. Control Processes, 2020, vol. 16, iss. 4, pp. 455–461. https://doi.org/10.21638/11701/spbu10.2020.410*
11. *Ikematsu Y., Nakamura S., Takagi T. Recent progress in the security evaluation of multivariate public-key cryptography // IET Information Security. 2022, pp. 1–17. DOI: 10.1049/ise2.12092*
12. *Ding J., Petzoldt A., Schmidt D.S. Solving Polynomial Systems. In: Multivariate Public Key Cryptosystems. Advances in Information Security. Springer. New York. 2020, vol.. 80, pp. 185-248. https://doi.org/10.1007/978-1-0716-0987-3_8*
13. *Cartor R., Cartor M., Lewis M., Smith-Tone D. IPRainbow. In: Cheon, J.H., Johansson, T. (eds) Post-Quantum Cryptography // Lecture Notes in Computer Science. 2022, vol. 13512, pp. 170–184. Springer, Cham. https://doi.org/10.1007/978-3-031-17234-2_9*
14. *Ding, J., Petzoldt, A., Schmidt, D.S. Oil and Vinegar. In: Multivariate Public Key Cryptosystems. Advances in Information Security. 2020, vol. 80, pp. 89-151. Springer, New York, NY. https://doi.org/10.1007/978-1-0716-0987-3_5*
15. *Moldovyan A.A., Moldovyan D.N., Moldovyan N.A. A new approach to the development of multidimensional cryptography algorithms. Voprosykiberbezopasnosti [Cibersecurity questtions]. 2023, no. 2(54), pp. 52–64. DOI:10.21681/2311-3456-2023-2-52-6.*
16. *Moldovyan A.A., Moldovyan N.A. Vector finite fields of characteristic two as algebraic support of multivariate cryptography // Computer Science Journal of Moldova. 2024. V.32. N.1(94). P. 46–60. DOI: 10.56415/csjm.v32.04*
17. *Moldovyan D.N., Moldovyan A.A., Moldovyan N.A. A new concept for designing post-quantum signature algorithms on non-commutative algebras. Voprosykiberbezopasnosti [Cibersecurity questtions]. 2022, no. 1(47), pp. 18–25. DOI: 10.21681/2311-3456-2022-1-18-25*
18. *Moldovyan D.N., Moldovyan A.A. Algebraic Signature Algorithms Based on Difficulty of Solving Systems of Equations. Voprosykiberbezopasnosti [Cibersecurity questtions]. 2022, no. 2(48), pp. 7–17. DOI: 10.21681/2311-3456-2022-2-7-17*

19. *Moldovyan A. A., Moldovyan N. A. Signature algorithms on finite on non-commutative algebras over fields of characteristic two. Voprosykiberbezopasnosti [Cibersecurity questtions]. 2022, no. 3(49), pp. 58–68. DOI: 10.21681/2311-3456-2022-3-58-68*
20. *Moldovyan N. A. Algebraic signature algorithms with a hidden group, based on hardness of solving systems of quadratic equations // Quasigroups and Related Systems. 2022 vol. 30, no. 2(48), pp. 287–298. DOI: https://doi.org/10.56415/qrs.v30.24*
21. *Moldovyan A. A., Moldovyan D. N., Kostina A. A. Algebraic signature algorithms with complete signature randomization. Voprosy-kiberbezopasnosti [Cibersecurity questtions]. 2024, No. 2(60). P. 95–102. DOI: 10.21681/2311-3456-2024-2-95-102*
22. *Moldovyan N. A., Moldovyan A. A. Finite Non-commutative Associative Algebras as carriers of Hidden Discrete Logarithm Problem. Bulletin of the South Ural State University. Ser. Mathematical Modelling, Programming & Computer Software (Bulletin SUSU MMCS), 2019, vol. 12, no. 1, pp. 66–81. DOI: 10.14529/mmp190106*
23. *Moldovyan N. A. Finite Non-Commutative Associative Algebras for Setting the Hidden Discrete Logarithm Problem and Post-quantum Cryptoschemes on Its Base // Bulletin of Academy of Sciences of Moldova. Mathematics. 2019, no. 1 (89), pp. 71–78.*
24. *Moldovyan A. A., Moldovyan N. A. Post-quantum signature algorithms with a hidden group and doubled verification equation. Informatsionno-upravliaiushchie sistemy [Information and Control Systems], 2023, no. 3, pp. 59–69. doi: 10.31799/1684-8853-2023-3-59-69*
25. *Moldovyan A. A., Moldovyan N. A. Post-quantum algebraic signature algorithms with a hidden group. Informatsionno-upravliaiushchie sistemy [Information and Control Systems], 2023, no. 1, pp. 29–40. doi:10.31799/1684-8853-2023-1-29-40.*
26. *Moldovyan N. A., Moldovyan A. A. Structure of a 4-dimensional algebra and generating parameters of the hidden logarithm problem Vestnik of Saint Petersburg University. Applied Mathematics. Computer Science. Control Processes. 2022, vol. 18, iss. 2, pp. 209–217. https//doi.org/10.21638/11701/spbu10.2022.202*
27. *Moldovyan D. N., Moldovyan A. A., Moldovyan N. A. Structure of a finite non-commutative algebra set by a sparse multiplication table // Quasigroups and Related Systems. 2022, vol. 30, no. 1, pp. 133 – 140. https://doi.org/10.56415/qrs.v30.11*
28. *Moldovyan N. A., Moldovyan A. A. Digital signature scheme on the 2x2 matrix algebra. Vestnik of Saint Petersburg University. Applied Mathematics. Computer Science. Control Processes. 2021. V. 17. Iss. 3. P. 254–261. https://doi.org/10.21638/11701/spbu10.2021.303*

СТРУКТУРНО-ФУНКЦИОНАЛЬНЫЙ АНАЛИЗ КОНФЛИКТНОЙ СИТУАЦИИ МЕЖДУ ГОСУДАРСТВЕННОЙ СИСТЕМОЙ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ИНОСТРАННОЙ СИСТЕМОЙ ДЕСТРУКТИВНЫХ ВОЗДЕЙСТВИЙ

Стародубцев Ю. И.[1], Закалкин П. В.[2]

DOI: 10.21681/2311-3456-2024-4-82-91

Цель исследования: *определить взаимосвязь понятий «информационная инфраструктура» Российской Федерации и «киберпространство»; определить предпосылки реализации возрастающего множества деструктивных воздействий.*

Методы исследования: *системный анализ, классификация, сравнительный анализ.*

Полученные результаты: *рассмотрена система обеспечения информационной безопасности Российской Федерации, ее участники, информационная инфраструктура Российской Федерации и определена ее взаимосвязь с киберпространством. Осуществлена формализация рассмотренных элементов. Разработано графическое отображение взаимосвязи информационной инфраструктуры и киберпространства.*

Научная новизна: *Осуществлен системно-структурный анализ конфликтной ситуации, что позволило выявить объективные причины реализации множества деструктивных воздействий на объекты критической инфраструктуры.*

Ключевые слова: *киберпространство, информационная безопасность, информационная инфраструктура, атака, деструктивные воздействия.*

STRUCTURAL AND FUNCTIONAL ANALYSIS OF THE CONFLICT SITUATION BETWEEN THE STATE INFORMATION SECURITY SYSTEM AND A FOREIGN SYSTEM OF DESTRUCTIVE INFLUENCES

Starodubtsev Yu. I.[3], Zakalkin P. V.[4]

The purpose of the study: *to determine the relationship between the concepts of «information infrastructure» of the Russian Federation and «cyberspace»; to determine the prerequisites for the implementation of an increasing set of destructive influences.*

Research methods: *system analysis, classification, comparative analysis.*

The results obtained: *the information security system of the Russian Federation, its participants, the information infrastructure of the Russian Federation are considered and its relationship with cyberspace is determined. The formalization of the considered elements has been carried out. A graphical representation of the relationship between information infrastructure and cyberspace has been developed.*

Scientific novelty: *A system-structural analysis of the conflict situation has been carried out, which made it possible to identify the objective reasons for the implementation of many destructive effects on critical infrastructure facilities.*

Keywords: *cyberspace, information security, information infrastructure, attack, destructive effects.*

1 Стародубцев Юрий Иванович, Заслуженный деятель науки РФ, Заслуженный изобретатель РФ, доктор военных наук, профессор, профессор кафедры, Военная академия связи, Санкт Петербург, Россия. E-mail: prof.starodubtsev@gmail.com, https://orcid.org/0000-0001-5140-4476

2 Закалкин Павел Владимирович, кандидат технических наук, Академия Федеральной Службы Охраны Российской Федерации, Орёл, Россия. E-mail: pzakalkin@mail.ru, https://orcid.org/0000-0003-2946-2586

3 Yuri Starodubtsev, Honored Scientist of the Russian Federation, Honored Inventor of the Russian Federation, Doctor of Military Sciences, Professor, Professor of the Department, Military Academy of Communications, Saint Petersburg, Russia. E-mail: prof.starodubtsev@gmail.com, https://orcid.org/0000-0001-5140-4476

4 Pavel Zakalkin, Ph.D., Academy of the Federal Guard Service of the Russian Federation, Orel, Russia. E-mail: pzakalkin@mail.ru, https://orcid.org/0000-0003-2946-2586

Введение

Сложнейшая военно-политическая обстановка в мире привела к началу Специальной военной операции и, как следствие, к переформатированию мирового порядка. Одним из отличительных факторов данного военного конфликта является кардинально возросшая роль киберпространства при ведении военных действий. Резко возросло количество кибератак, осуществляемых противоборствующими сторонами (как открыто, так и посредством своих «прокси» группировок), появились новейшие вооружения, навигация и управление которыми осуществляется посредством киберпространства.

Исходя из новых реалий глава военного комитета НАТО адмирал Роб Бауэр заявил, что «Кибератака на одну из стран НАТО может стать поводом для применения 5-й статьи устава Североатлантического альянса»[5]. Признавая киберпространство как пространство ведения военных действий, НАТО готово в любой момент (руководствуясь своими интересами) объявить Российской Федерации войну исходя только из факта наличия атак, осуществляемых посредством киберпространства.

Рассмотрев основные руководящие документы, имеющие отношение как к военной безопасности страны, так и к информационной безопасности, было установлено, что на законодательном уровне в Российской Федерации понятие «киберпространство» не определено.

Согласно Доктрины информационной безопасности Российской Федерации[6] (далее – Доктрина) в основном используются термины «информационная инфраструктура Российской Федерации»[7], «информационная сфера»[8] и «информационное пространство». Т.е. сложилась парадоксальная ситуация, НАТО готово объявить Российской Федерации войну в киберпространстве (попутно создавая киберкомандования в странах участницах альянса), осуществляет множество скоординированных кибератак на инфраструктуру РФ, а в РФ само понятие «киберпространство» не определено.

Данное исследование в первую очередь направлено на определение взаимосвязи понятий «информационная инфраструктура Российской Федерации», «информационная сфера» и «киберпространство».

Система обеспечения информационной безопасности

На государственном уровне в Доктрине признается, что:

- противник пытается доминировать в информационном пространстве за счет технологического превосходства и повсеместного внедрения иностранного оборудования, протоколов и т.д.;
- невозможно реализовать совместное справедливое, основанное на принципах доверия, управление этим пространством (даже хотя бы на территории собственного государства);
- отсутствуют международно-правовые нормы, регулирующие межгосударственные отношения в этом пространстве.

Согласно Доктрины обеспечение устойчивого и бесперебойного функционирования информационной инфраструктуры, в первую очередь критической информационной инфраструктуры Российской Федерации[9] (КИИ) и ЕСЭ РФ, в мирное время, в период непосредственной угрозы агрессии и в военное время является национальным интересом РФ в информационной сфере. В Доктрине определяется система обеспечения информационной безопасности[10] (СОИБ). С технической точки зрения СОИБ включает подсистемы контроля, принятия решений и формирования управляющих воздействий. При этом все подсистемы функционируют на ограниченном множестве учитываемых параметров.

В графическом виде СОИБ в РФ представлена на рисунке 1.

Система обеспечения информационной безопасности

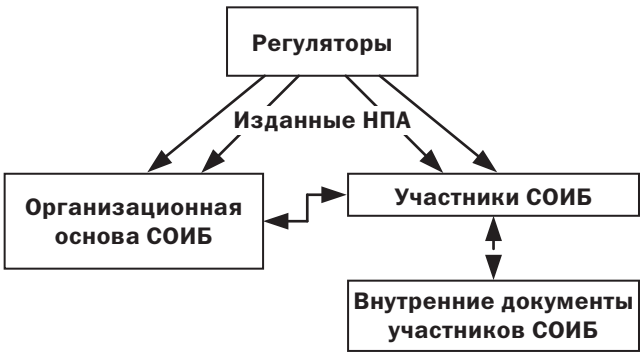


Рис. 1. Обобщенная структура системы обеспечения информационной безопасности в РФ

5 Кибератака может стать поводом для применения пятой статьи устава НАТО [Электронный ресурс] URL: https://rg.ru/2024/06/01/nato-mozhet-ispolzovat-5-iu-statiu-ustava-iz-za-kiberataki-na-strany-aliansa.html

6 Доктрина информационной безопасности российской Федерации. Утверждена Указом Президента Российской Федерации от 05.12.2016 г.

7 Информационная инфраструктура Российской Федерации – совокупность объектов информатизации, информационных систем, сайтов в сети «Интернет» и сетей связи, расположенных на территории Российской Федерации, а также на территориях, находящихся под юрисдикцией Российской Федерации или используемых на основании международных договоров Российской Федерации.

8 Информационная сфера – совокупность информации, объектов информатизации, информационных систем, сайтов в информационно-телекоммуникационной сети «Интернет», сетей связи, информационных технологий, субъектов, деятельность которых связана с формированием и обработкой информации, развитием и использованием названных технологий, обеспечением информационной безопасности, а также совокупность механизмов регулирования соответствующих общественных отношений.

9 Критическая информационная инфраструктура – объекты критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия таких объектов.

10 Система обеспечения информационной безопасности – совокупность сил обеспечения информационной безопасности, осуществляющих скоординированную и спланированную деятельность, и используемых ими средств обеспечения информационной безопасности.

В структуре СОИБ выделяются три основных элемента: регуляторы, организационная основа СОИБ и участники СОИБ.

В РФ имеется два основных регулятора в области информационной безопасности: ФСБ и ФСТЭК. Их задачи представлены в соответствующих руководящих документах[11].

Все элементы СОИБ РФ руководствуются нормативно-правовыми актами (НПА), издаваемыми регуляторами, и используют программные и программно-аппаратные средства, лицензированные ими.

СОИБ является частью системы обеспечения национальной безопасности Российской Федерации. Обеспечение ИБ осуществляется на основе сочетания законодательной, правоприменительной, правоохранительной, судебной, контрольной и других форм деятельности государственных органов во взаимодействии с органами местного самоуправления, организациями и гражданами.

СОИБ должна строится на основе разграничения полномочий органов законодательной, исполнительной и судебной власти в данной сфере с учетом предметов ведения федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, а также органов местного самоуправления, определяемых законодательством Российской Федерации в области обеспечения безопасности.

Согласно Доктрины организационная основа СОИБ состоит из элементов, представленных на рисунке 2.

11 1) Федеральный закон от 3 апреля 1995 г. N 40-ФЗ «О федеральной службе безопасности».
2) Указ Президента РФ от 16.08.2004 N 1085 (ред. от 08.11.2023) «Вопросы Федеральной службы по техническому и экспортному контролю» (Выписка).

Согласно Доктрины участники СОИБ РФ представлены на рисунке 3.

Министерства и ведомства имеют право на создание собственных внутренних документов применительно к ИБ в части их касающихся. Получается, что в РФ имеется множество участников СОИБ, в процессе своей деятельности руководствующихся НПА, изданными регуляторами, и в дополнение к этому частично использующих внутренние документы.

В формализованном виде СОИБ можно представить следующим образом:

$$\{\{NPA^{R}\},\{Org\},\{Uch\},\{NPA^{Uch}\}\} = СОИБ$$

где $\{NPA^{R}\}$ – множество НПА, изданных регуляторами; $\{Org\}$ – множество элементов, составляющих организационную основу СОИБ; $\{Uch\}$ – множество участников СОИБ; $\{NPA^{Uch}\}$ – множество внутренних документов участников СОИБ.

Вся совокупность выделенных элементов: множество НПА, изданных регуляторами, множество элементов, составляющих организационную основу СОИБ, множество участников СОИБ и множество внутренних документов участников СОИБ – направлена на обеспечение ИБ информационной инфраструктуры РФ.

Структурное представление системы обеспечения информационной безопасности

Рассмотрим СОИБ со стороны участника СОИБ. Исходя из представленных выше документов каждый из участников СОИБ может руководствоваться НПА как одного из регуляторов, так и нескольких сразу и еще при этом иметь внутреннюю документацию применительно к ИБ. Также каждый из участников СОИБ

Рис. 2. Организационная основа СОИБ РФ

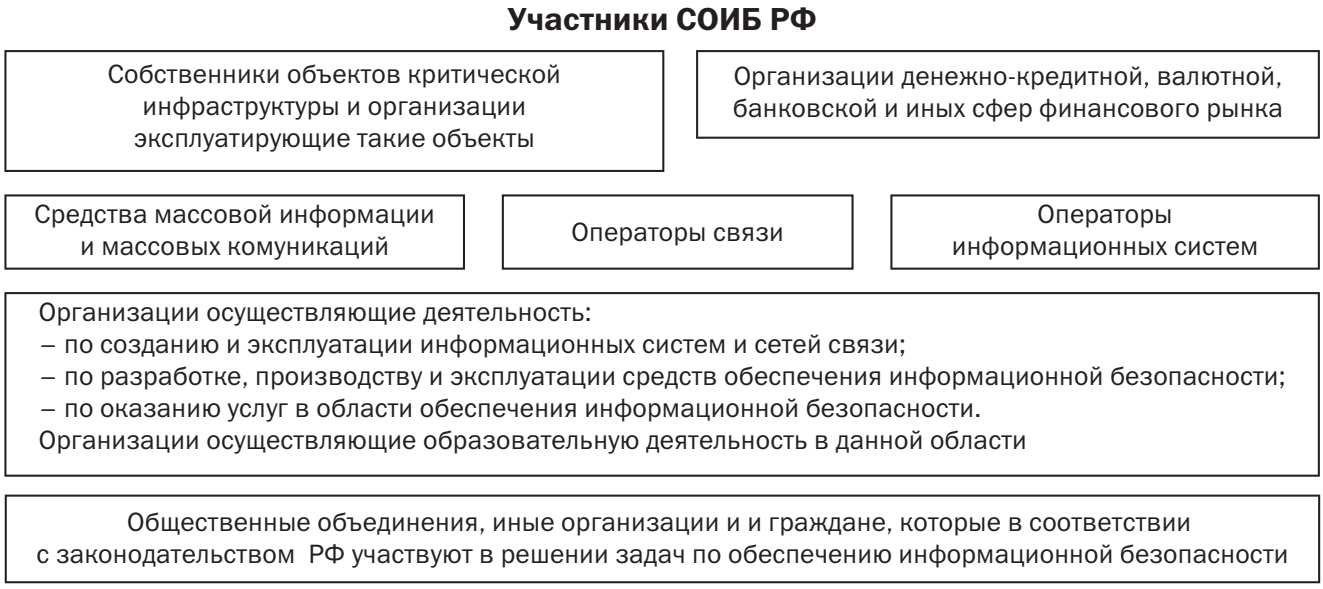


Рис. 3. Участники СОИБ РФ

в рамках своей ответственности может иметь несколько элементов информационной инфраструктуры.

В качестве примера сложившейся ситуации приведен рисунок 4. Участник СОИБ ($Uch1$) руководствуется НПА регулятора NPA^{R1} и собственной внутренней документацией применительно к ИБ (NPA^{Uch1}), имеет в зоне своей ответственности некоторое множество элементов информационной инфраструктуры Ii_1^{Uch1}, Ii_2^{Uch1}, Ii_n^{Uch1} (где n – количество элементов информационной инфраструктуры $Uch1$). При этом ответственным за элементы информационной инфраструктуры участника СОИБ может назначаться как одно лицо, так и несколько лиц, все зависит от территориальной рассосредоточенности структурных элементов участника СОИБ. Например, практически все органы государственной власти на территории РФ имеют деление, условно повторяющее административно-территориальное деление РФ. Соответственно лица ответственные за элементы информационной инфраструктуры Дальневосточного ФО и Центрального ФО будут различны.

В тоже время $Uch2$ может руководствоваться как NPA^{R1}, NPA^{R2}, так и собственной внутренней документацией применительно к ИБ (NPA^{Uch2}). Например, ФСТЭК для ряда своих НПА указывает что их действие не распространяется на высшие органы государственной власти и т.д., в таком случае используются НПА другого регулятора. $Uch2$ имеет собственное множество элементов информационной инфраструктуры Ii_1^{Uch2}, Ii_2^{Uch2}, Ii_k^{ch2} (где k – количество элементов информационной инфраструктуры NPA^{lsp}) и множество лиц, ответственных за ее эксплуатацию.

Исходя из приведенного графического представления видно, что каждый из участников СОИБ

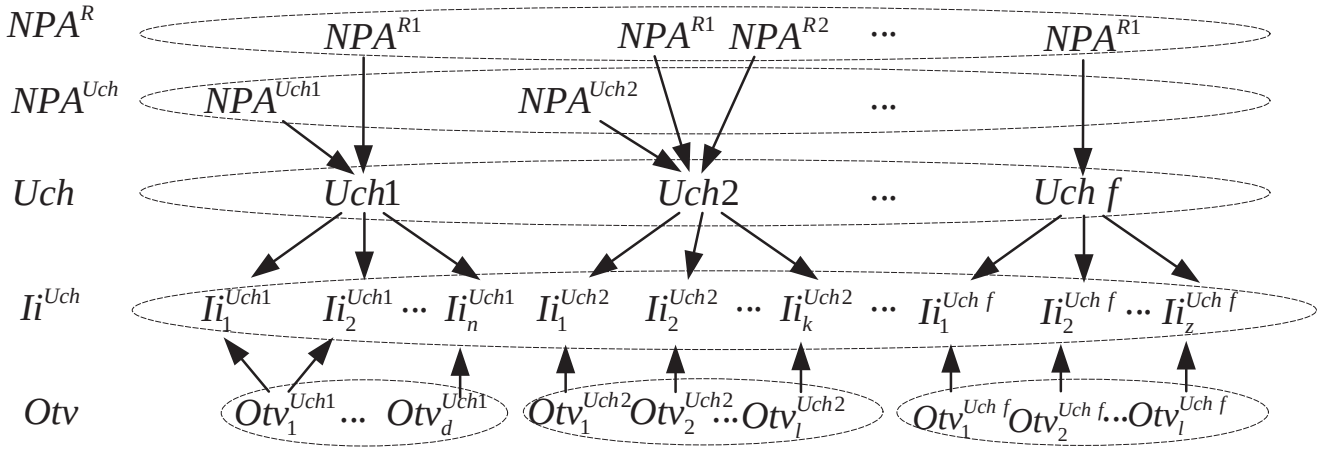


Рис. 4. Графическое представление взаимосвязи элементов СОИБ

применительно к своей инфраструктуре использует подмножество НПА (NPA^{Isp}) из общего множества НПА регуляторов, внутреннюю документацию применительно к ИБ, и при всем этом у участников имеется произвольный набор элементов информационной инфраструктуры и лиц, ответственных за обеспечение ее эксплуатации.

В формализованном виде участника СОИБ можно представить следующим образом:

$$Uch2 = \{NPA^{Isp}_{Uch2}, Ii^{Uch2}, Otv^{Uch2}\}$$

где $NPA^{Isp}_{Uch2} = \{NPA^{R1}_{Uch2}, NPA^{R2}_{Uch2}, NPA^{Uch2}\}$, при $NPA^{R1} \notin NPA^{R2}$, $NPA^{R1}_{Uch2} \cap NPA^{R1}$, $NPA^{R2}_{Uch2} \cap NPA^{R2}$; $Ii^{Uch2} = \{Ii^{Uch2}_1, Ii^{Uch2}_2, ..., Ii^{ch2}_k\}$, k – количество элементов информационной инфраструктуры; $Otv^{Uch2} = \{Otv^{Uch2}_1, Otv^{Uch2}_2, ..., Otv^{ch2}_l\}$, l – количество лиц, ответственных за функционирование информационной инфраструктуры $Uch2$.

Каждый из участников СОИБ действует в рамках НПА, изданных регуляторами, но при этом в первую очередь участник заинтересован в обеспечении безопасного функционирования собственной информационной инфраструктуры. Например, оператор связи заинтересован в безопасном функционировании элементов информационной инфраструктуры, находящейся в его ведении, но при этом функционирование инфраструктуры других операторов связи ему интересно только в рамках варианта обеспечения транзита собственного трафика через них.

Таким образом, вся информационная инфраструктура РФ не равноценно разделена между участниками СОИБ, за обеспечение ее функционирования отвечает множество лиц с различной степенью компетенции и различными техническими возможностями по обеспечению функционирования инфраструктуры.

Если вся информационная инфраструктура РФ функционирует в рамках СОИБ РФ, где определены регуляторы, организационная основа, участники, ответственные лица и т.д., вся инфраструктура защищена согласно требованиям, то возникает логичный вопрос «Откуда появляется противник, осуществляющий атаки на инфраструктуру?».

Для ответа на этот вопрос необходимо вернуться к определению термина «информационная инфраструктура», исходя из которого видно, что информационная инфраструктура РФ ограничивается только территорией РФ, а также территориями, находящимися под юрисдикцией Российской Федерации или используемых на основании международных договоров Российской Федерации. При этом абсолютно не учитывается инфраструктура зарубежных государств.

Физическая составляющая информационной инфраструктуры РФ имеет множество точек взаимодействия с инфраструктурой зарубежных государств,

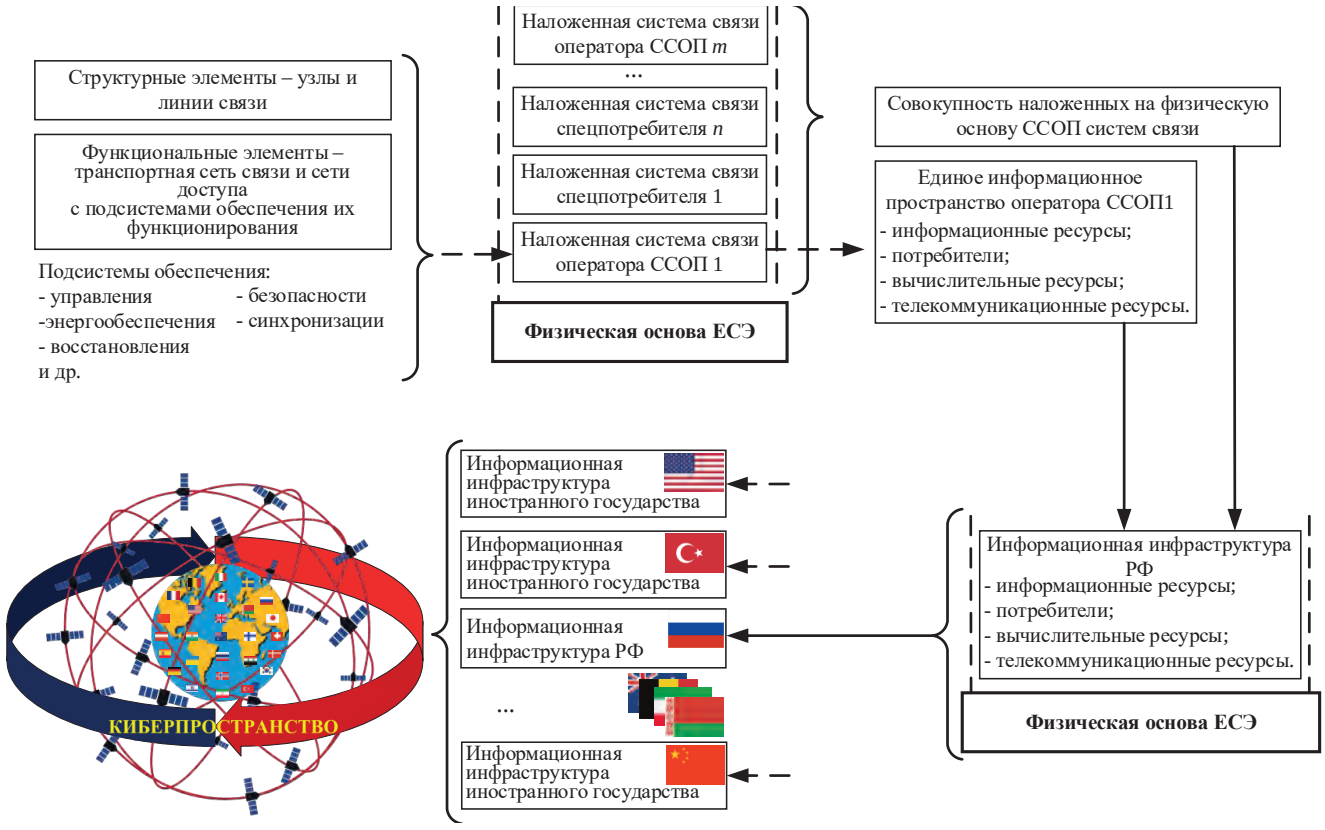


Рис. 5. Графическое отображение взаимосвязи понятий «информационная инфраструктура» и «киберпространство»

тем самым интегрируясь в одно глобальное пространство мирового масштаба, которое с различной степенью плотности покрывает все пространство нашей планеты. Поверх физической составляющей наложено множество логических структур. Графическое отображение этой ситуации представлено на рисунке 5. Наличие большого количества слабоконтролируемых связей (а также использование зарубежного оборудования, протоколов и т.д.) с инфраструктурой иностранных государств позволяет осуществлять деструктивные воздействия на информационную инфраструктуру РФ из любой точки земного шара [1–4], а заблаговременно внедренные программные закладки и зарубежное программное обеспечение облегчают эту задачу [5-6].

Взаимодействие с инфраструктурой иностранных государств является критичным для РФ, т.к. частично функционирование элементов информационной инфраструктуры возможно только в совокупности с этим пространством, и отдельно без него существенно ограничивается функционал или полностью прекращается его работа. Например, корневые сервера, отвечающие за адресацию, корневые DNS сервера и т.д. полностью контролируются зарубежными организациями [1].

Если распространить терминологию, применяемую в РФ на весь мир, то получается, что каждое государство имеет свою информационную инфраструктуру, имеющую точки взаимодействия с инфраструктурой других государств (как минимум соседних). В формализованном виде это можно представить следующим образом:

$$Ii^{MIR} = \{Ii^{RF}, Ii_1^{ig}, Ii_2^{ig}, Ii_3^{ig},..., Ii_z^{ig}\}$$

где Ii^{MIR} – общемировая информационная инфраструктура; z – общее количество мировых государств.

Терминология, принятая в различных государствах, в той или иной степени отличается, но в подавляющем большинстве общемировую информационную инфраструктуру называют киберпространством. Получается, что информационная инфраструктура РФ является составляющей киберпространства. Говоря о киберпространстве, мы подразумеваем и информационную инфраструктуру РФ (как составляющую киберпространства), а говоря о информационной инфраструктуре РФ мы подразумеваем киберпространство (как общее пространство, включающее в себя информационную инфраструктуру РФ).

Исходя из этого определение термина «информационная инфраструктура» требует корректировки. Предлагается под информационной инфраструктурой РФ понимать территориально выделенный структурный элемент киберпространства, представляющий собой взаимосвязанную совокупность объектов информатизации, информационных систем, сайтов в сети «Интернет» и сетей связи, расположенных на территории Российской Федерации, а также на территориях, находящихся под юрисдикцией Российской Федерации или используемых на основании международных договоров Российской Федерации.

Мировые информационные инфраструктуры не являются единственными составляющими киберпространства, в [1,2] указывается, что элементами киберпространства являются также и симбионты киберпространства. Т.е. устройства, которые в любой произвольный момент времени могут подключиться (или отключиться) к киберпространству для обеспечения доступа к его ресурсам и реализации отдельных системных функций в интересах других пользователей информационных услуг. К симбионтам можно отнести смартфоны, персональные компьютеры, системы навигации, IoT-устройства, АСУ ТП и т.д.

Информационная инфраструктура как элемент киберпространства

Киберпространство можно представить в виде множества, включающего в себя множество подмножеств, каждое из которых в свою очередь также состоит из множества подмножеств. Например, представив киберпространство как множество Ii^{MIR}, подмножествами данного множества будет множество информационных инфраструктур Ii^{mg} мировых государств. Каждое из множеств является множеством подмножеств, включающих в себя элементы, составляющие физическую и логическую структуру киберпространства. Которые в свою очередь включают в себя подмножества из множества участников СОИБ, организационной структуры, ответственных лиц, а также множества симбионтов в динамике, подключающихся (отключающихся) к элементам киберпространства.

При этом всякое объединение подмножеств будет являться частью подмножеств Ii^{mg}, также как и всякое пересечение всякого конечного семейства множеств из Ii^{mg} будет множеством из Ii^{mg}.

Учитывая, что физические элементы киберпространства покрывают всю поверхность нашей планеты (с различной степенью плотности) [1,2,7], а наша планета в приближенном виде имеет форму шара (обычно для описания фигуры Земли используют эллипсоид вращения или геоид), то киберпространство можно представить в виде шара. Физические элементы киберпространства могут находиться как в ближнем космосе (спутники), так и на морском дне (подводные коммуникационные кабели), то логичнее говорить о форме киберпространства, как о сферической оболочке (или сферическом слое) – области, заключенной между двумя концентрическими сферами различного радиуса.

Исходя из общей топологии[12] можно утверждать, что киберпространство является топологической структурой. Топологической структурой в множестве X называют структуру, образованную заданием множества Ω подмножеств множества X, обладающего следующими свойствами:

- всякое объединение множеств из Ω есть множество из Ω;
- пересечение всякого конечного семейства множеств из Ω есть множество из Ω.

Множества Ω называются открытыми множествами топологической структуры, определяемой посредством Ω в X.

Раз киберпространство наделено топологической структурой, следовательно, согласно общей топологии, оно является топологическим пространством.

В данном случае мы говорим только о физической структуре киберпространства, логическая структура является гораздо более сложной и многомерной, где на одном физическом элементе может пересекаться множество логических.

Киберпространство взаимоувязано и из любой его точки можно попасть в любую другую, что позволяет осуществлять атаки на элементы киберпространства (в нашем случае информационная инфраструктура), не находясь в непосредственной близости от них.

Предположим, что из информационной инфраструктуры иностранного государства (Ii^{ig}) осуществляется атака ($attack$) на элементы информационной инфраструктуры РФ (Ii^{RF}), например на элементы участников $Ii^{Uch1} = \{Ii_1^{Uch1}, Ii_3^{Uch1}\}$, $Ii^{Uch2} = \{Ii_2^{Uch2}, Ii_3^{Uch2}\}$ и $Ii^{Uch3} = \{Ii_1^{Uch3}, Ii_3^{Uch3}\}$ (Рисунок 6).

$$attack = \{aIi_1^{Uch1}, aIi_3^{Uch1}, aIi_2^{Uch2}, aIi_3^{Uch2}, aIi_1^{Uch3}, aIi_3^{Uch3}\}$$

12 Н. Бурбаки Общая топология. Основные структуры. М., 1968 г. 272 стр. с илл.

где aIi – атакованная информационная инфраструктура.

Далее необходимо ввести ограничения касаемо лиц, ответственных за элементы информационной инфраструктуры:

- ответственные лица с помощью имеющихся в их распоряжении технических средств (либо другим способами) получили уведомление об атаке на находящиеся в их ведении инфраструктуры;
- обладают высоким уровнем профессиональных компетенций, доверены, имеют в своем распоряжении достаточное количество технических средств и осведомлены о тактиках и техниках как проведения атак, так и противодействия им.

В связи с этим, далее будем считать $Otv^{Uch} = const$.

Авторский коллектив прекрасно понимает, что в реальной жизни у всех Otv^{Uch} будет различный уровень подготовки, технических и финансовых возможностей. Кроме того, во многих случаях атака может быть не зафиксирована, поскольку в системах защиты отсутствуют необходимые правила детектирования, учитывающие актуальные изменения в ландшафте киберугроз [8–10].

В данном примере целенаправленно показывается идеальный случай, когда все обнаружено и имеется достаточный ресурс для противодействия атаке.

Каждый из ответственных лиц из общего количества атакованной инфраструктуры будет видеть только атаки на инфраструктуру, за которую он ответственен, либо в отдельных случаях атаки на инфраструктуру участника СОИБ, которому он подчиняется. В этом случае общая информированность ответственного лица Inf^{Otv} будет определяться как:

$$Inf^{Otv} = \frac{ali_{vid}^{Otv}}{ali_n}$$

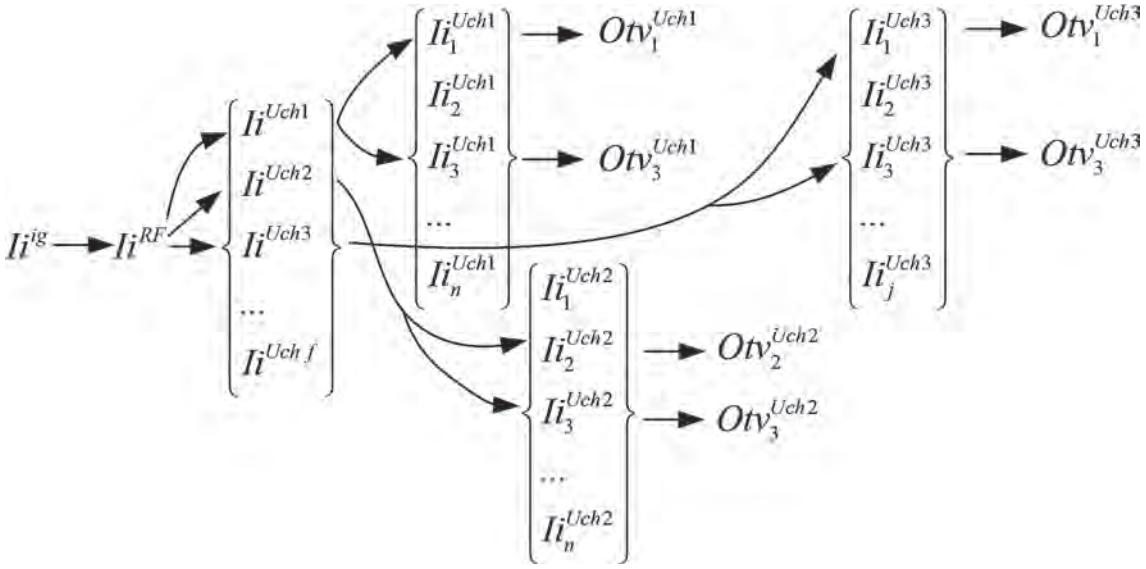


Рис. 6. Графическое отображение атаки из информационной инфраструктуры иностранного государства

где ali_{vid}^{Otv} – атакованная информационная инфраструктура, видимая ответственному лицу; ali_n – общее количество атакованной информационной инфраструктуры в рамках $attack$.

Применительно к нашему примеру (рисунок 6) информированность Otv_3^{Uch} в худшем случае будет 16%, а в лучшем (при условии, что он осведомлен о всех атаках на элементы информационной инфраструктуры участника СОИБ) – 33%.

Применение средств противодействия компьютерным атакам формализуется моделью, состоящей из процессов: регулирования настроек системы противодействия компьютерным атакам и средств администрирования безопасности информации, регулирования информационных и вычислительных ресурсов критически важной информационной системы, регулирования управляющей информации[13].

Таким образом, каждое из действий характеризуется временным промежутком, затрачиваемым на него. Каждый из ответственных лиц запускает цикл противодействия атаке основной характеристикой которого будет, временной промежуток, затрачиваемый на его исполнение. Множество ответственных лиц породит множество циклов противодействия, разрозненных по времени, целям и подчиненных интересам различных систем управления.

Учитывая, что циклы противодействия могут выполняться параллельно друг другу, то общее время, затраченное на противодействие атаке, будет определяться временем завершения последнего цикла. При этом не обязательно, что цикл, завершившийся последним, будет самым длительным во времени. В общем случае время, затраченное на общий цикл противодействия ($t_{общ}^{прот}$) определяется следующим образом:

$$t_{общ}^{прот} = \Delta t + t_{цикл}^{посл}$$

где Δt – период времени с момента обнаружения первой атаки, до момента начала работы цикла завершившегося последним; $t_{цикл}^{посл}$ – время длительности работы цикла завершившегося последним.

Обобщенная характеристика структур для действий в киберпространстве (на примере США)

Рассматривая противника (блок НАТО), в первую очередь необходимо рассмотреть США как головную структуру в области кибербезопасности и киберпространства (все остальные страны блока НАТО в подавляющем большинстве используют документы, созданные на базе руководящих документов США). Основными структурами для действий в киберпространстве является Агентство национальной безопасности (АНБ) в связке с Центральным разведывательным управлением (ЦРУ) и киберкомандование США.

АНБ осуществляет радиоэлектронную разведку и обеспечение информационной безопасности в интересах правительства США.

Радиоэлектронная разведка осуществляет сбор информации о планах, намерениях, возможностях и местонахождении террористических групп, организаций, иностранных держав, или их агентов, которые угрожают национальной безопасности США. В качестве примера систем шпионажа можно привести PRISM, обработкой больших данных занимаются множество дата-центров созданных в интересах АНБ и ЦРУ[14]. В рамках обеспечения ИБ осуществляется защита жизненно важных национальных систем США, коммуникационных сетей США и информации от кражи или нанесения ущерба противником, а также обеспечивается доступность и подлинность информации, необходимой правительственным структурам США. Обеспечение информационной безопасности и радиоэлектронной разведки необходимы для проведения разведывательных операций в киберпространстве киберкомандованием США и их партнерами.

В свою очередь киберкомандование США планирует, координирует, объединяет, синхронизирует и проводит мероприятия по руководству операциями и защите компьютерных сетей министерства обороны; готовит и осуществляет полный спектр военных операций в киберпространстве, обеспечивает свободу действий США и их союзников в киберпространстве и препятствует аналогичным действиям противника.

Таким образом, противник, осуществляя атаку, представляет из себя единую структуру – киберкомандование иностранного государства. Действует скоординированно по четкому плану, имеет высокую степень информированности, резерв сил и средств, которые может вводить их на различных этапах атаки, тем самым регулируя атакующие усилия по различным элементам.

С другой стороны, противнику противостоят разрозненные по силам, времени, планам, низкоинформированные (в рамках общей атаки противника) силы и средства, которые при этом рассосредоточены и подчинены различным системам управления.

В таблице приведены основные характеристики описываемой ситуации.

13 Климов С.М., Сычёв М. П., Астрахов А .В. «Противодействие компьютерным атакам. Методические основы». Электронное учебное издание [Электронный ресурс] URL: http://wwwcdl.bmstu.ru/iu10/comp-atak-metod.htm

14 Как АНБ и ЦРУ используют дата-центры и облака [Электронный ресурс] URL: https://habr.com/ru/companies/vdsina/articles/531972/

Таблица 1.

Основные характеристики распределенной атаки со стороны противника и СОИБ

Противник	СОИБ
Атака планируется и осуществляется одной структурой – киберкомандованием.	Защита осуществляется различными структурами (являющимися участниками СОИБ), зачастую не связанными между собой.
Единая система управления.	Множество систем управления.
Единый план, четко разбитый на этапы по времени. Возможность корректировки плана по ходу операции.	У каждого участника свой собственный план противодействия, составленный исходя из его информированности и опыта. Циклы противодействия разобщены.
Высокая степень скоординированности и информированности в рамках проведения атаки.	Низкая степень скоординированности и информированности (между участниками СОИБ), ограниченная только собственными элементами.
Единая нормативная база.	Разный набор нормативных документов у участников.

Выводы

Информационная инфраструктура РФ является структурным элементом киберпространства и регулярно подвергается деструктивным воздействиям.

Очевидна несоизмеримость организованного множества воздействий, осуществляемых по единому замыслу и плану со стороны противника на информационную инфраструктуру и разрозненными, разноплановыми и взаимоисключающими мероприятиями по защите элементов информационной инфраструктуры, реализуемых не соподчинёнными должностными лицами.

Исход конфликта между множеством возможных источников деструктивных воздействий и объектов информационной инфраструктуры в большей степени будет зависеть не от средств защиты, а от скоординированности и информированности участников конфликтной ситуации, характеристик и порядка функционирования используемого фрагмента киберпространства.

Противник пытается доминировать в киберпространстве за счет технологического превосходства и повсеместного внедрения иностранного оборудования, протоколов и т.д.

Литература

1. *Стародубцев Ю. И., Закалкин П. В., Иванов С.А. Структурно-функциональная модель киберпространства // Вопросы кибербезопасности. 2021. № 4(44). С.16–24. DOI:10.21681/2311-3456-2021-4-16-24.*
2. *Закалкин П. В. Эволюция систем управления киберпространством // Вопросы кибербезопасности. 2022. № 1(47). С. 76–86. DOI:10.21681/2311-3456-2022-1-76-86.*
3. *Белов А. С., Добрышин М. М., Шугуров Д. Е. Научно-методический подход к оцениванию качества систем обеспечения информационной безопасности // Приборы и системы. Управление, контроль, диагностика. 2022. № 11. С. 34–40.*
4. *Добрышин М. М. Выбор структуры и механизмов адаптивного управления системы обеспечения информационной безопасности // Известия Тульского государственного университета. Технические науки. 2022. № 2. С. 214–222.*
5. *Леонов Н. В. Противодействие уязвимостям программного обеспечения. Часть 1. Онтологическая модель. // Вопросы кибербезопасности. 2024. № 2(60). С.87–92. DOI: 10.21681/2311-3456-2024-2-87-92.*
6. *Левшун Д. С., Веснин Д. В., Котенко И. В. Прогнозирование категорий уязвимостей в конфигурациях устройств с помощью методов искусственного интелекта // Вопросы кибербезопасности. 2024. № 3(61). С.33–69 DOI: 10.21681/2311-3456-2024-3-33-39.*
7. *Иванов М. В., Калашников И. В., Нурулаев М. М. Исследование структурных свойств сети интернет на основе метаграфовых моделей // Труды СПИИРАН. 2020. Т.19. № 4. С. 880–900.*
8. *Мещеряков Р. В., Исхаков С. Ю. Исследование методов формирования индикаторов компрометации от внутренних источников информационных и киберфизических систем // Вопросы кибербезопасности. 2023. № 6(58) С.35–49. DOI:10.21681/2311-3456-2023-6-35-49.*
9. *Израилов К. Е., Буйневич М. В. Метод обнаружения атак различного генезиса на сложные объекты на основе информации состояния. Часть 1. Предпосылки и схема // Вопросы кибербезопасности. 2023. № 3(55) С.90–100. DOI:10.21681/2311-3456-2023-3-90-100.*
10. *Иванов С. А. Устойчивость сетей связи общего пользования в условиях глобализации // Известия Тульского государственного университета. Технические науки. 2021. № 9. С. 86–90.*

References

1. *Starodubcev Ju. I., Zakalkin P. V., Ivanov S. A. Strukturno-funkcional'naja model' kiberprostranstva // Voprosy kiberbezopasnosti. 2021. № 4(44). S.16–24. DOI:10.21681/2311-3456-2021-4-16-24.*
2. *Zakalkin P. V. Jevoljucija sistem upravlenija kiberprostranstvom // Voprosy kiberbezopasnosti. 2022. № 1(47). S. 76–86. DOI:10.21681/2311-3456-2022-1-76-86.*
3. *Belov A. S., Dobryshin M. M., Shugurov D. E. Nauchno-metodicheskij podhod k ocenivaniju kachestva sistem obespechenija informacionnoj bezopasnosti // Pribory i sistemy. Upravlenie, kontrol', diagnostika. 2022. № 11. S. 34–40.*
4. *Dobryshin M. M. Vybor struktury i mehanizmov adaptivnogo upravlenija sistemy obespechenija informacionnoj bezopasnosti // Izvestija Tul'skogo gosudarstvennogo universiteta. Tehnicheskie nauki. 2022. № 2. S. 214–222.*
5. *Leonov N. V. Protivodejstvie ujazvimostjam programmnogo obespechenija. Chast' 1. Ontologicheskaja model'. // Voprosy kiberbezopasnosti. 2024. № 2(60). S.87–92. DOI: 10.21681/2311-3456-2024-2-87-92.*
6. *Levshun D. S., Vesenie D. V., Kotenko I. V. Prognozirovanie kategorij ujazvimostej v konfiguracijah ustrojstv s pomoshh'ju metodov iskusstvennogo intellekta // Voprosy kiberbezopasnosti. 2024. № 3(61). S.33–69 DOI: 10.21681/2311-3456-2024-3-33-39.*
7. *Ivanov M. V., Kalashnikov I. V., Nurullaev M. M. Issledovanie strukturnyh svojstv seti internet na osnove metagrafovyh modelej // Trudy SPIIRAN. 2020. T.19. № 4. S. 880–900.*
8. *Meshherjakov R. V., Ishakov S. Ju. Issledovanie metodov formirovanija indikatorov komprometacii ot vnutrennih istochnikov informacionnyh i kiberfizicheskih sistem // Voprosy kiberbezopasnosti. 2023. № 6(58) S.35–49. DOI:10.21681/2311-3456-2023-6-35-49.*
9. *Izrailov K. E., Bujnevich M. V. Metod obnaruzhenija atak razlichnogo genezisa na slozhnye ob#ekty na osnove informacii sostojanija. Chast' 1. Predposylki i shema // Voprosy kiberbezopasnosti. 2023. № 3(55) S.90–100. DOI:10.21681/2311-3456-2023-3-90-100.*
10. *Ivanov S. A. Ustojchivost' setej svjazi obshhego pol'zovanija v uslovijah globalizacii // Izvestija Tul'skogo gosudarstvennogo universiteta. Tehnicheskie nauki. 2021. № 9. S. 86–90.*

ПРИМЕНЕНИЕ ТЕХНОЛОГИЙ МАШИННОГО ОБУЧЕНИЯ ДЛЯ ОБНАРУЖЕНИЯ ВЕБ-АТАК

Лапина М. А.[1], Мовзалевская В. В.[2], Токмакова М. Е.[3], Бабенко М. Г.[4], Саджид М.[5]

DOI: 10.21681/2311-3456-2024-4-92-103

Цель исследования: *исследование применимости методов машинного обучения и их оценки в области обнаружения вторжений и атак в веб-среде.*

Методы исследования: *рассмотрены различные реализации алгоритмов машинного обучения для определения типа и атаки в веб-среде, в частности алгоритмы классификации и кластеризации. Для обнаружения атак были выбраны самые оптимальные алгоритмы машинного обучения, реализованные с помощью библиотеки Scikit-learn, после их рассмотрения и сравнительного анализа. В рамках этой работы параметрами оценки эффективности исследуемых алгоритмов являются показатели времени обучения, а также характеристики из Confusion matrix и Classification Report для алгоритмов классификации, и Homogeneity, Completeness, V-measure для алгоритмов кластеризации.*

Результат: *для рассматриваемой выборки данных был определен и реализован наиболее экономичный по времени и качеству алгоритм – метод деревьев решений. Наилучшие характеристики для решения поставленной задачи показали деревья решения точность при определении типа и подтипа атаки составляет 99.9662% и 99.9576% соответственно. Время обнаружение атаки в среднем равно 85.39 ms и 114.72 ms для типа и подтипа соответственно.*

Практическая ценность *состоит в том, что предлагается решение задачи для обнаружения и определения различных типов и под типов атаки в веб среде которые позволяют разработать оптимальную стратегию защиты интернет ресурсов и минимизировать вероятность потери, кражи или искажения данных.*

Вклад авторов: *Лапина М. А., Бабенко М. Г., Саджид М. – выбор и постановка задачи исследования; Лапина М. А., Мовзалевская В. В., Токмакова М. Е. – выбор решений, программная реализация и проведение экспериментов; Лапина М. А., Мовзалевская В. В., Токмакова М. Е., Бабенко М. Г. – обсуждения результатов экспериментов, анализ полученных результатов.*

Ключевые слова: *веб-среда, алгоритмы классификации, алгоритмы кластеризации, искусственный интеллект, интернет-безопасность, методы обнаружения угроз, информационная безопасность.*

DETECTING WEB ATTACKS USING MACHINE LEARNING ALGORITHMS

Lapina M. A.[6], Movzalevskaya V. V.[7], Tokmakova M. E.[8], Babenko M. G.[9], Sajid M.[10]

The purpose of the study: *study the applicability of machine learning methods and their evaluation in the field of intrusion and attack detection in the web environment.*

Research methods: *various implementations of machine learning algorithms for determining the type and attack in the web environment are considered classification and clustering algorithms. To detect attacks, the most optimal machine learning algorithms implemented using the Scikit-learn library were selected after their consideration and comparative*

1 Лапина Мария Анатольевна, кандидат физико-математических наук, доцент, доцент кафедры информационной безопасности автоматизированных систем Северо-Кавказского федерального университета, Ставрополь, Россия. E-mail: mlapina@ncfu.ru, ORCID: 0000-0001-8117-9142.

2 Мовзалевская Виталия Валентиновна, студентка специальности информационная безопасность автоматизированных систем Северо-Кавказского федерального университета, Ставрополь, Россия. E-mail: vitaliya1306@gmail.com, ORCID: 0009-0007-7540-3110.

3 Токмакова Марина Евгеньевна, студентка специальности информационная безопасность автоматизированных систем Северо-Кавказского федерального университета, Ставрополь, Россия. E-mail: marinatokmakova175@mail.ru, ORCID: 0009-0000-2608-7712.

4 Бабенко Михаил Григорьевич, доктор физико-математических наук, доцент, заведующий кафедрой вычислительной математики и кибернетики Северо-Кавказского федерального университета, Ставрополь, Россия. E-mail: mgbabenko@ncfu, ORCID: 0000-0001-7066-0061.

5 Саджид Мохаммад, доктор наук, доцент кафедры компьютерных наук Мусульманского университета, Алигарха, Алигарх, Индия. E-mail: sajid.cst@gmail.com, ORCID: 0000-0001-8822-5332.

6 Maria A. Lapina, Ph.D., Associate Professor, Associate Professor of the Department of Information Security of Automated Systems, North Caucasus Federal University, Stavropol, Russia. E-mail: mlapina@ncfu.ru, ORCID: 0000-0001-8117-9142.

7 Vitaliya V. Movzalevskaya, student of the specialty information security of automated systems at the North Caucasus Federal University, Stavropol, Russia. E-mail: vitaliya1306@gmail.com, ORCID: 0009-0007-7540-3110.

8 Marina E. Tokmakova, student of the specialty information security of automated systems at the North Caucasus Federal University, Stavropol, Russia. E-mail: marinatokmakova175@mail.ru, ORCID: 0009-0000-2608-7712.

9 Mikhail G. Babenko, Dr.Sc., Associate Professor, Head of the Department of Computational Mathematics and Cybernetics, North Caucasus Federal University, Stavropol, Russia. E-mail: mgbabenko@ncfu, ORCID: 0000-0001-7066-0061.

10 Mohammad Sajid, Ph.D., Associate Professor, Department of Computer Science, Muslim University, Aligarh, Aligarh, India. E mail: sajid.cst@gmail.com, ORCID: 0000-0001-8822-5332.

analysis. In this work, the parameters for evaluating the effectiveness of the studied algorithms are training time indicators, as well as characteristics from the Confusion matrix and Classification Report for classification algorithms, and Homogeneity, Completeness, V-measure for clustering algorithms.

The results obtained: *for the considered data sample, the most time-efficient and quality-efficient algorithm was determined and implemented - the decision tree method. The best characteristics for solving the problem were shown by decision trees; the accuracy in determining the type and subtype of an attack is 99.9662% and 99.9576%, respectively. The average attack detection time is 85.39 ms and 114.72 ms for the type and subtype, respectively.*

The scientific novelty *is that it offers a solution to the problem of detecting and defining various types and subtypes of attacks in the web environment, which allows developing an optimal strategy for protecting Internet resources and minimizing the likelihood of loss, theft or corruption of data.*

Contribution of the authors: *Lapina M. A., Babenko M. G., Sajid M. – selection and formulation of the research problem; Lapina M. A., Movzalevskaya V. V., Tokmakova M. E. – selection of solutions, software implementation and experiments; Lapina M. A., Movzalevskaya V. V., Tokmakova M. E., Babenko M. G. – discussions of the experimental results, analysis of the obtained results.*

Keywords: *web environment, classification algorithms, clustering algorithms, artificial intelligence, Internet security, threat detection methods, information security.*

Введение

Внедрение умных устройств в жизнь людей предоставило злоумышленникам значительно большее количество ресурсов с низким уровнем защиты, что позволило им разработать новые сценарии для проведения кибератак с использованием ботнет. Ботнет состоят из тысяч зараженных вредоносным программным обеспечения умных устройств, которые одновременно непрерывно отправляют огромные объемы данных для нанесения огромного вреда отдельным пользователям, компаниям с использованием DDoS атак [1].

Безопасность веб-сервисов является сложной задачей. В целом DDoS-атаки стали серьезной угрозой для веб-сервисов. Для выполнения DoS/DDoS-атак могут использоваться различные подходы, включая сетевые подходы, такие как лавинная рассылка через пакеты TCP SYN, ICMP или UDP, а также подходы на основе хостов, когда один или несколько хостов нацелены на определенные приложения для использования структуры своей памяти, протокола аутентификации или определенного алгоритма [2]. По данным Information Technology Intelligence Consulting, час простоя ИТ-услуг может стоить компаниям от 300 000 до 1 000 000 долларов. Учитывая эту цифру, размер понесенного финансового ущерба невообразим, когда в октябре 2020 года на тысячи IP-адресов Google была обрушена DDoS-атака. Атака была совершена тремя китайскими интернет-провайдерами и длилась шесть месяцев, достигнув ошеломляющего уровня 2,5. Тбит/с [1].

Алгоритмы машинного обучения позволяют обнаруживать и предотвращать атаки, что значительно повышает эффективность защиты сайта. По своей сути, машинное обучение можно представить как процесс вывода алгоритмов прогнозирования неизвестных данных, с использованием ранее собранной информации.

1. Постановка задачи

Задачей данного исследования является создание прогностической модели, способной различать «плохие» сетевые соединения (вторжения или атаки) и «хорошие» (обычные) соединения, а также определять конкретный тип атак для защиты компьютерной сети от неавторизованных пользователей, включая, возможно, инсайдеров. Используемая в исследовании база данных содержит стандартный набор данных для аудита, который включает в себя широкий спектр вторжений и атак, имитируемых в сетевой среде. Все, используемые в работе, алгоритмы машинного обучения были реализованы с использованием библиотеки Scikit-learn, также для метода градиентного бустинга приведена реализация CatBoost. Для моделирования использовался датасет KDD Cup 1999.

2. Обзор литературы

В табл. 1, 2 приведены свойства всех реализованных в исследовании алгоритмов машинного обучения:

- ❖ возможность работы с категориальными данными;
- ❖ сложность модели алгоритма, связанная с количеством параметров в модели;
- ❖ интерпретируемость, чем она выше у модели, тем легче понять, почему были приняты определенные решения или прогнозы;
- ❖ необходимость масштабирования данных;
- ❖ временная сложность.

Учитывая данные свойства методов, самыми оптимальными являются логическая регрессия (возможность работы с категориальными данными, низкая сложность модели, высокий уровень интерпретируемости, не требуется масштабируемость данных) и деревья решений (возможность работы с категориальными данными, низкая сложность модели,

Таблица 1.

Свойства алгоритмов машинного обучения

Методы	Высокая			
	Категориальные данные	Сложность модели	Уровень интерпретируемость	Масштабируемость данных
Алгоритмы классификации				
Случайный лес [3]	–	Высокая	Средний	Не требуется
GB (Scikit-learn) [4]	+	Высокая	Высокий	Не требуется
GB (CatBoost) [5]	+	Высокая	Средний	Не требуется
Logit model [6]	+	Низкая	Высокий	Не требуется
Наивный Байес [7]	+	Высокая	Низкий	Требуется
Деревья решений [8]	+	Низкая	Высокий	Не требуется
SVMs [9]	+	Высокая	Низкий	Не требуется
Метод k-NN [10]	+	Низкая	Высокий	Требуется
Алгоритмы кластеризации				
Метод k-средних [11]	–	Высокая	Низкий	Требуется
HCA [12]	+	Низкая	Средний	Требуется

Таблица 2.

Свойства алгоритмов машинного обучения

Методы	Временная сложность
Алгоритмы классификации	
Случайный лес	O(n)
GB	O(knm)
Logit model	O(n)
Наивный Байес	O(dk) + O(dkn)
Деревья решений	$O(n_{features} \times n^2_{samples} \log(n_{samples}))$
SVMs	$O(n_{features} \times n^2_{samples})$
Метод k-NN	O(log n)
Алгоритмы кластеризации	
Метод k-средних	O(knT)
HCA	O(n3)

высокий уровень интерпретируемости, не требуется масштабируемость данных).

3. Моделирование

В данном разделе приведены реализация, обучение и тестирование вышеописанных алгоритмов машинного обучения. Моделирование проводилось на Intel(R) Xeon(R) CPU E5-2690 v4 @ 2.60GHz, DDR3 SDRAM 256 Gb под управлением операционной системы Ubuntu 18.04.5 на языке программирования Python 3.8.8 с использованием jupyter core 4.7.1, jupyter-notebook 6.3.0, qtconsole 5.0.3, ipython 7.22.0, ipykernel 5.3.4, jupyter client 6.1.12, jupyter lab 3.0.14, nbconvert 6.0.7, ipywidgets 7.6.3, nbformat 5.1.3, traitlets 5.0.5, sklearn 0.24.1, catboost 1.2.3 на языке программирования Python.

В качестве набора данных используются данные из необработанного трафика, перехваченного утилитой tcpdump в локальной сети. Набор данных содержит 494 023 записи, из них 330 995 тренировочных и 163 028 тестовых. Набор данных взят KDD Cup 1999. Задача обученной модели – определить атаку по ее свойствам.

В машинном обучении существует много различных метрик, которые позволяют определить точность и эффективность работы обученной модели. В рамках данного исследования параметрами оценки эффективности исследуемых алгоритмов являются показатели времени обучения, а также характеристики из Confusion matrix и Classification Report для алгоритмов классификации, и Homogeneity, Completeness, V-measure для алгоритмов кластеризации.

3.1. Алгоритмы классификации

Для оценки точности работы алгоритмов классификации используются показатели времени работы модели, Confusion matrix и Classification Report, представленные в таблицах в соответствующих подразделах, а также в разделе 5.

В работе для обнаружения атак в веб-среде выбранные алгоритмы машинного обучения реализованы с помощью библиотеки Scikit-learn. Однако, для алгоритма градиентного бустинга приведена реализация CatBoost, т. к. она обеспечивает высокую производительность и предотвращение переобучения, также данная реализация заявлена как самая быстрая и оптимизированная [15], поэтому в исследовании приведено ее сравнение с Scikit-learn, самой часто реализуемой.

Для моделей классификации Случайный лес, GB (Scikit-learn), GB (CatBoost), Logit model, Наивный Байес, Деревья решений, SVMs, Метод k-NN, представлены в табл. 3. Как видно из приведенных данных в табл. 3.A (Precision), табл. 3.B (Recall) и табл. 3.C (F1-Score) алгоритм определяет все классы, причем с минимальным, по отношению к общему числу атак текущего класса, количеством ошибок. Самый маленький класс, состоящий из 10 атак, верно определился только в половине случаев. Из данных представленных в Таблицах 3.A, 3.B и 3.C наилучшие параметры precision, recall и F1-Score для классов benign, dos, probe, r2l и u2r близки к своим лучшем значениям для метода случайный лес. Точность предсказания данного практически достигает наилучших результатов. Достигается за счет использование ансамбля деревьев решений [13, 14], которые позволяют выявить ключевые факторы и более точно решить задачу классификации по сравнению с имеющимися аналогами. Однако, стоит отметить, что вычислительная сложность случайного леса больше вычислительная сложность деревья решений и требует больше вычислительных ресурсов для реализации приложений в реальном времени, чем деревья решений.

4. Алгоритмы кластеризации

Для оценки точности работы алгоритмов кластеризации используются показатели времени работы модели, Completeness, Homogeneity, V-measure, представленные в таблицах в соответствующих подразделах, в разделе 5, а также на рисунках, показывающих распределение классов в изначальных данных и по окончании работы алгоритмов.

4.1. Метод k-средних

Сначала приведены данные для определения типа атаки (5 классов), далее описано работа с определением подтипа атаки (23 класса).

Изначальное распределение классов в тренировочных данных, полученное с помощью Principal component analysis (PCA), представлено на рис. 1 (определение типа атаки).

Распределение кластеров, полученное в результате работы модели, обученной с помощью алгоритма K-средних, представлено на рис. 2 (определение типа атаки).

Ниже приведены основные метрики для оценки результатов работы модели при определении типа атаки:

- Completeness = 0.40571;
- Homogeneity = 0.8058;
- V-measure = 0.53969.

Не очень высокое значение Completeness показывает, что члены одного класса далеко не всегда относятся моделью к одному кластеру. Это наглядно представлено на рис. 3, слева фрагмент с изначальным распределением классов, а справа – фрагмент с результатом работы модели.

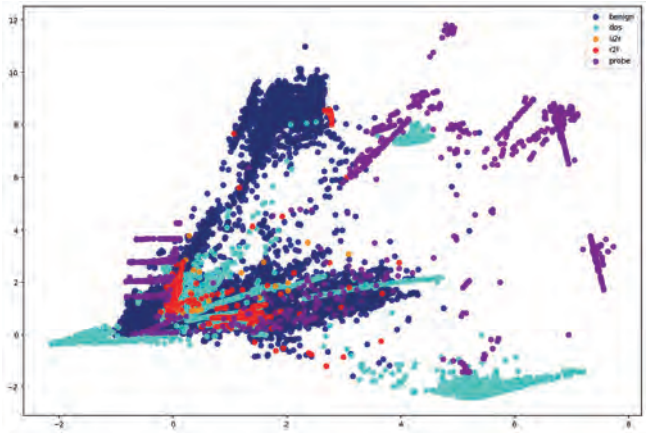


Рис. 1. Изначальное распределение кластеров в наборе данных при определении типа атаки

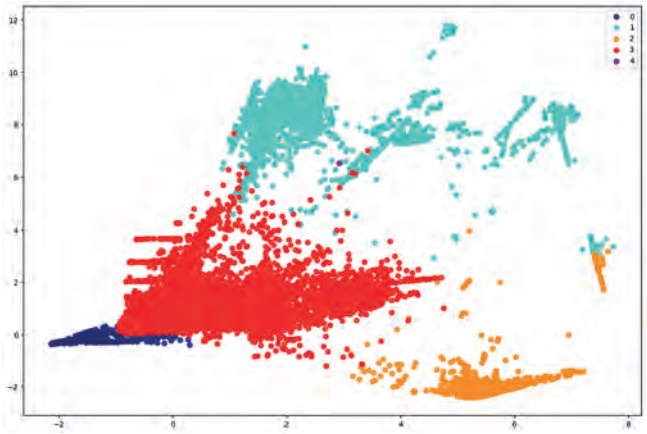


Рис. 2. Кластеры алгоритма K-means при определении типа атаки

Таблица 3.

Результат классификации атак на веб-сервисы с помощью моделей классификации Случайный лес, GB (Scikit-learn), GB (CatBoost), Logit model, Наивный Байес, Деревья решений, SVMs, Метод k-NN

A) Precision

	Метод								
	Случайный лес	GB (Scikit-learn)	GB (CatBoost)	Logit model	Наивный Байес	Деревья решений	SVMs	Метод k-NN	Support
Классы (тип атаки)									
benign	**1.00**	**1.00**	**1.00**	**1.00**	0.98	**1.00**	**1.00**	**1.00**	32041
dos	**1.00**	**1.00**	**1.00**	**1.00**	**1.00**	**1.00**	**1.00**	**1.00**	129287
probe	**1.00**	0.98	0.99	0.98	0.04	0.99	0.99	0.99	1320
r2l	**0.99**	0.75	0.96	0.93	0.23	0.98	0.98	0.96	369
u2r	**1.00**	0.00	0.50	0.75	0.00	0.38	**1.00**	0.50	10
Параметры									
macro avg	**1.00**	0.75	0.89	0.93	0.45	0.87	0.99	0.89	163027
weighted avg	**1.00**	**1.00**	**1.00**	**1.00**	0.99	**1.00**	**1.00**	**1.00**	163027

B) Recall

	Метод								
	Случайный лес	GB (Scikit-learn)	GB (CatBoost)	Logit model	Наивный Байес	Деревья решений	SVMs	Метод k-NN	Support
Классы (тип атаки)									
benign	**1.00**	0.99	**1.00**	**1.00**	0.91	**1.00**	**1.00**	**1.00**	32041
dos	**1.00**	**1.00**	**1.00**	**1.00**	0.73	**1.00**	**1.00**	**1.00**	129287
probe	**1.00**	0.98	0.99	0.97	0.97	**1.00**	0.99	0.99	1320
r2l	**0.97**	0.77	0.96	0.91	0.48	**0.97**	0.93	0.96	369
u2r	0.50	0.00	0.30	0.60	**0.80**	0.30	0.40	0.30	10
Параметры									
macro avg	**0.89**	0.75	0.85	**0.89**	0.78	0.85	0.86	0.85	163027
weighted avg	**1.00**	**1.00**	**1.00**	**1.00**	0.76	**1.00**	**1.00**	**1.00**	163027

C) F1-Score

	Метод								
	Случайный лес	GB (Scikit-learn)	GB (CatBoost)	Logit model	Наивный Байес	Деревья решений	SVMs	Метод k-NN	Support
Классы (тип атаки)									
benign	**1.00**	0.99	**1.00**	**1.00**	0.94	**1.00**	**1.00**	**1.00**	32041
dos	**1.00**	**1.00**	**1.00**	**1.00**	0.84	**1.00**	**1.00**	**1.00**	129287
probe	**1.00**	0.98	0.99	0.98	0.07	0.99	0.99	0.99	1320
r2l	**0.98**	0.76	0.96	0.92	0.31	**0.98**	0.96	0.96	369
u2r	**0.67**	0.00	0.37	**0.67**	0.01	0.33	0.57	0.37	10
Параметры									
accuracy	**1.00**	**1.00**	**1.00**	**1.00**	0.76	**1.00**	**1.00**	**1.00**	163027
macro avg	**0.93**	0.75	0.86	0.91	0.43	0.86	0.90	0.86	163027
weighted avg	**1.00**	**1.00**	**1.00**	**1.00**	0.85	**1.00**	**1.00**	**1.00**	163027

Рис. 3. Сравнение исходных данных и результатов работы модели

Показатель Homogeneity принимает довольно высокое значение, это свидетельствует о том, что каждый кластер преимущественно состоит только из членов одного класса.

Стоит отметить, что модель плохо определила классы с небольшим количеством членов, а также некоторые классы поделила между несколькими кластерами.

Оценка времени работы модели, полученная в ходе проведения экспериментов на одних и тех же данных, представлена в табл. 4 (раздел 5). Среднее время работы модели на тестовых данных составляет 0.30534 секунд.

Далее представлена работы с подтипами атак (23 класса). Изначальное распределение классов в тренировочных данных, полученное с помощью Principal component analysis (PCA), представлено на рис. 4 (определение подтипа атаки).

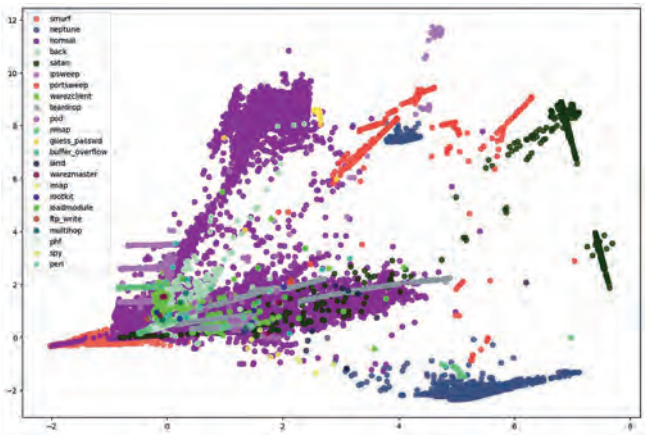


Рис. 4. Изначальное распределение кластеров в наборе данных при определении подтипа атаки

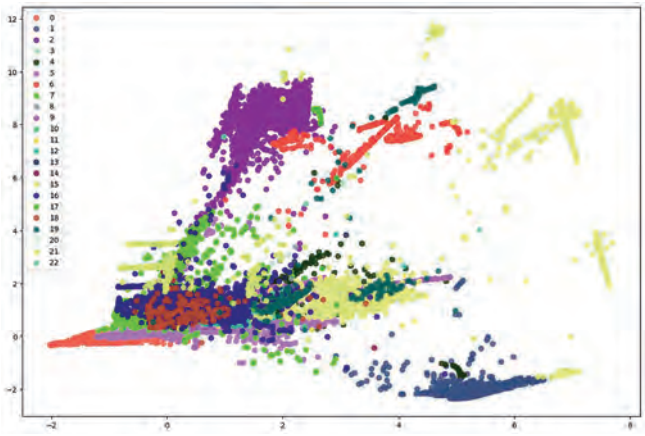


Рис. 5. Кластеры алгоритма K-means при определении подтипа атаки

Распределение кластеров, полученное в результате работы модели, обученной с помощью алгоритма K-средних, представлено на рис. 5 (определение подтипа атаки)

Ниже приведены основные метрики для оценки результатов работы модели при определении подтипа атаки:

- Completeness = 0.72072;
- Homogeneity = 0.94527;
- V-measure = 0.81786.

Достаточно высокое значение Completeness показывает, что члены одного класса практически всегда относятся моделью к одному кластеру.

Показатель Homogeneity принимает очень высокое значение, это свидетельствует о том, что каждый кластер преимущественно состоит только из членов одного класса.

Оценка времени работы модели, полученная в ходе проведения экспериментов на одних и тех же данных, представлена в табл. 5 (раздел 5). Среднее время работы модели на тестовых данных составляет 0.24645 секунд.

4.2. Иерархическая кластеризация

Во время тестирования алгоритма иерархической кластеризации было принято решение использовать только 5% от исходного набора тренировочных и тестовых данных, так как данный алгоритм требует большого количества памяти для корректной работы. Сначала приведены данные для определения типа атаки (5 классов), далее описано работа с определением подтипа атаки (23 класса).

Изначальное распределение классов в тренировочных данных, полученное с помощью Principal component analysis (PCA), представлено на рис. 6 (определение типа атаки).

Ниже приведены основные метрики для оценки результатов работы модели при определении типа атаки:

- Completeness = 0.40278;
- Homogeneity = 0.79463;
- V-measure = 0.53459.

Не высокое значение Completeness показывает, что члены одного класса далеко не всегда отнесены моделью к одному кластеру.

Показатель Homogeneity принимает довольно высокое значение, это свидетельствует о том, что каждый кластер преимущественно состоит только из членов одного класса.

Стоит отметить, что модель плохо определила классы с небольшим количеством членов, а также некоторые классы поделила между несколькими кластерами.

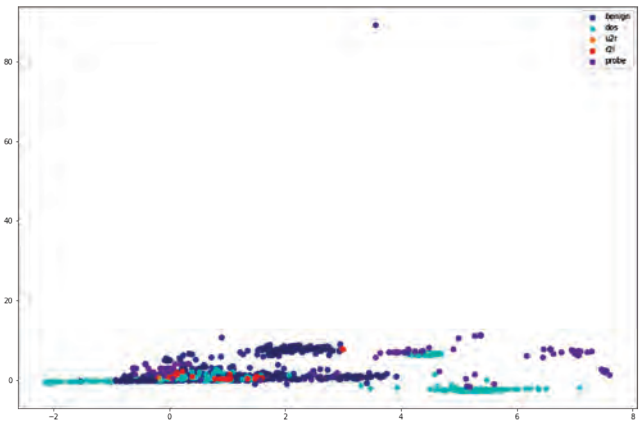


Рис. 6. Изначальное распределение кластеров в наборе данных при определении типа атаки

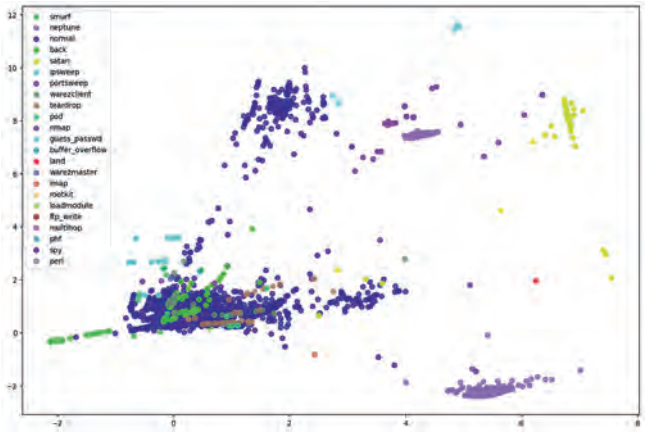


Рис. 8. Изначальное распределение кластеров в наборе данных при определении подтипа атаки

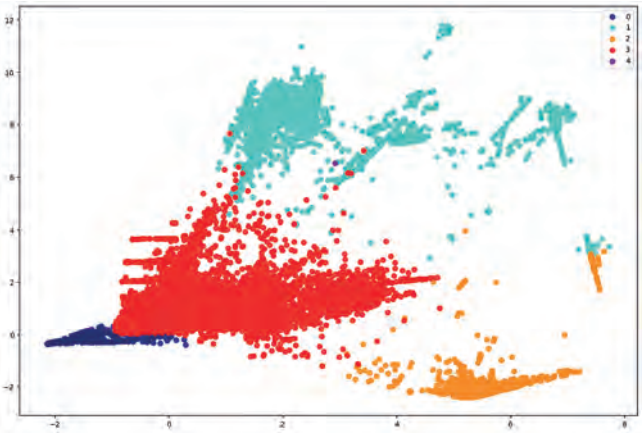


Рис. 7. Кластеры алгоритма Иерархической кластеризации при определении типа атаки

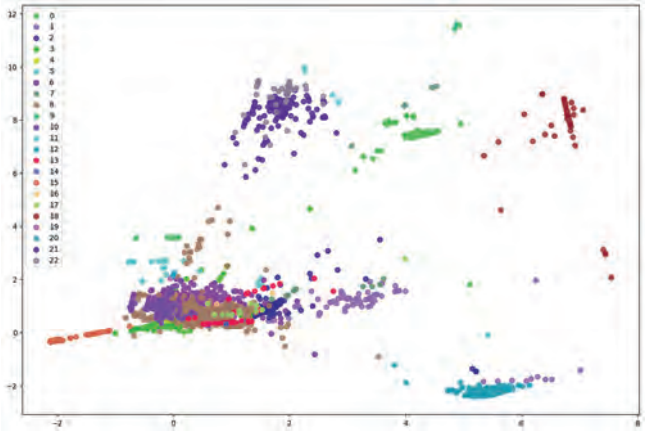


Рис. 9. Кластеры алгоритма иерархической кластеризации при определении подтипа атаки

Оценка времени работы модели, полученная в ходе проведения экспериментов на одних и тех же данных, представлена в табл. 4 (раздел 5). Среднее время работы модели на тестовых данных составляет 122.050 секунд.

Далее представлена работы с подтипами атак (23 класса). Изначальное распределение классов в тренировочных данных, полученное с помощью Principal component analysis (PCA), представлено на рис. 8 (определение подтипа атаки).

Распределение кластеров, полученное в результате работы модели, обученной с помощью алгоритма иерархической кластеризации, представлено на рис. 9. (определение подтипа атаки)

Ниже приведены основные метрики для оценки результатов работы модели при определении подтипа атаки:

- Completeness = 0.69550;
- Homogeneity = 0.95251;
- V-measure = 0.80397.

Не высокое значение Completeness показывает, что члены одного класса не всегда относятся моделью к одному кластеру.

Показатель Homogeneity принимает очень высокое значение, это свидетельствует о том, что каждый кластер преимущественно состоит только из членов одного класса.

Стоит отметить, что модель плохо определила классы с небольшим количеством членов, а также некоторые классы поделила между несколькими кластерами.

Оценка времени работы модели, полученная в ходе проведения экспериментов на одних и тех же данных, представлена в табл. 5 (раздел 5). Среднее время работы модели на тестовых данных составляет 102.074 секунд.

5. Анализ полученных данных

Проведён сравнительный анализ алгоритмов машинного обучения применительно к выборке атак и вторжений в веб-среде. Исследование продемонстрировало разную степень эффективности моделей

Таблица 4.

Время работы алгоритмов для определения типа атаки (5 классов)

Методы	Average, sec	T_{max}, sec	T_{min}, sec	σ
Алгоритмы классификации				
Случайный лес	2.82505	7.20053	2.01484	1.05204
Градиентный бустинг (Scikit-learn)	1.37482	4.23323	0.87714	0.72573
Градиентный бустинг (CatBoost)	0.88187	1.47155	0.74535	0.21805
Логическая регрессия	0.26269	0.62514	0.19481	0.08247
Наивный байесовский классификатор	0.85927	1.30261	0.80680	0.06827
Деревья решений	0.08539	0.11705	0.07151	0.01232
Метод опорных векторов	38.3194	38.3773	38.2732	0.02738
Метод k-ближайших соседей	670.8163	871.81656	650.8959	1.23631
Алгоритмы кластеризации				
Метод k-средних	0.30534	0.51908	0.23136	0.07874
Иерархическая кластеризация	122.050	283.725	96.0285	1.30705

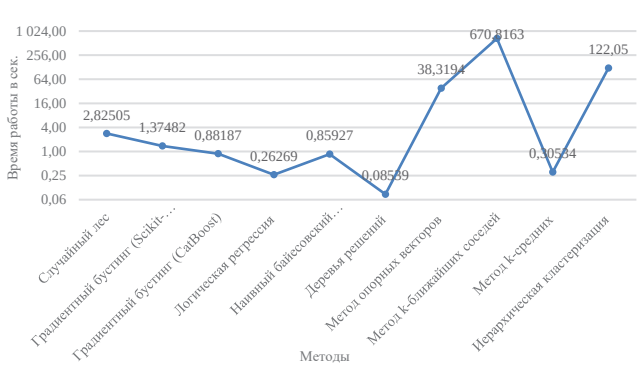


Рис.10. Время работы алгоритмов для определения типа атаки (5 классов)

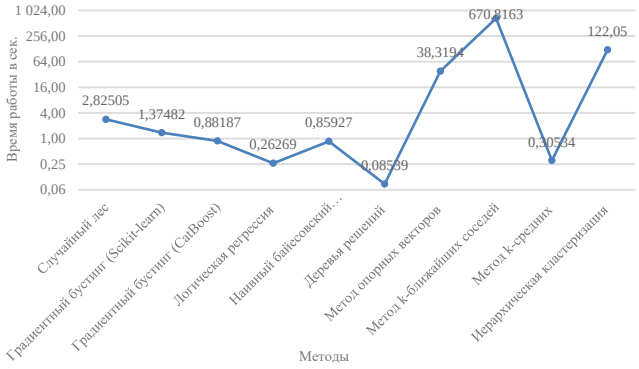


Рис.11. Время работы алгоритмов для определения подтипа атаки (23 классов)

Таблица 5.

Время работы алгоритмов для определения подтипа атаки (23 класса)

Методы	Average, sec	T_{max}, sec	T_{min}, sec	σ
Алгоритмы классификации				
Случайный лес	3.92719	4.50832	3.63689	0.2723
Градиентный бустинг (Scikit-learn)	3.24662	6.97630	2.70011	0.81519
Градиентный бустинг (CatBoost)	2.44120	5.76815	1.78189	0.87678
Логическая регрессия	0.32962	0.51410	0.27861	0.06833
Наивный байесовский классификатор	4.32658	4.89500	4.04916	0.22773
Деревья решений	0.11472	0.14774	0.10419	0.01176
Метод опорных векторов	48.88156	70.00742	43.25102	0.40573
Метод k-ближайших соседей	28.46818	31.26908	27.85873	0.35328
Алгоритмы кластеризации				
Метод k-средних	0.24645	0.34519	0.21609	0.03729
Иерархическая кластеризация	102.074	123.239	90.7761	0.53563

и скорости их работы в решении конкретной задачи определения типа и подтипа атак.

Ниже приведены показатели времени обучения каждой модели при определении типа атаки (Табл. 4, Рис. 10), а также подтипа атаки (Табл. 5, Рис. 11).

Исходя из показателей времени (Табл. 4) обучения моделей, их можно разделить на те, которые работают быстрее (случайны лес (2.82505), градиентный бустинг (Scikit-learn) (1.37482), градиентный бустинг (CatBoost) (0.88187), логическая регрессия (0.26269), наивный байесовский классификатор (0.85927), деревья решений (0.08539), метод k-средних (0.30534)) и те, которые работают медленнее (метод опорных векторов (38.3194), метод k-ближайших соседей (670.8163), иерархическая кластеризация (122.050)).

Исходя из показателей времени обучения моделей (Табл. 5), их можно разделить на те, которые работают быстрее (логическая регрессия (0.32962), деревья решений (0.11472), метод k-средних (0.24645) и те, которые работают медленнее (случайный лес (3.92719), градиентный бустинг (Scikit-learn) (3.24662), градиентный бустинг (CatBoost) (2.44120), наивный байесовский классификатор (4.32658), метод опорных векторов (48.88156), метод k-ближайших соседей (28.46818), иерархическая кластеризация (102.074)).

Также приведены показатели из матрицы несоответствия для алгоритмов классификации при определении типа атаки (Табл. 6). Из данных, представленных в табл. 6 можно сделать вывод, что алгоритм основанный на технологии случайный лес позволяет наилучшим образом определить тип атаки.

Данные точности определения подтипа атаки для каждого из алгоритмов представлены в табл. 7, опираясь на них можно сделать выводы, что случайный лес позволяет получить наибольшую точность определения подтипа атаки, но при этом не позволяет определить следующие подтипы атаки: land, spy, loadmodule, phf. Градиентный бустинг Scikit-learn не позволяет определить следующие подтипы атаки: warezmaster, land, guess_passwd, imap, ftp_write multihop, loadmodule, perl, rootkit, phf. Градиентный бустинг CatBoost не позволяет определить следующие подтипы атаки: multihop, loadmodule, rootkit, satan, phf. Деревья решений не позволяют определить следующие подтипы атаки: land, imap, spy, multihop, rootkit, phf.

Данные точности определения подтипа атаки для каждого из алгоритмов представлены в табл. 8, опираясь на них можно сделать выводы, что логическая регрессия не позволяет определить следующие подтипы атаки: spy, multihop, loadmodule, perl, rootkit, phf. Наивный байесовский классификатор не позволяет определить следующие подтипы атаки: multihop, loadmodule, rootkit, phf. Метод опорных векторов не позволяет определить следующие подтипы атаки: land, spy, multihop, perl, rootkit, phf. Метод k-ближайших соседей не позволяет определить следующие подтипы атаки: land, spy, rootkit, phf.

6. Вывод

Учитывая временные показатели, в качестве основной модели был выбран метод деревьев решений, время его работы оказалось минимальным и при определении типа атаки (0.08539), и при определении подтипа (0.11472).

При этом на рассматриваемых данных метрики качества метода деревьев решений принимают следующие значения: при определении типа атаки

Таблица 6.

Матрица несоответствия для определения типа атаки (5 классов)

Методы	benign		dos		probe		r2l	
Случайный лес	True	False	True	False	True	False	True	False
Градиентный бустинг (Scikit-learn)	32037	4	129283	4	1317	3	358	11
Градиентный бустинг (CatBoost)	31777	264	129215	72	1291	29	283	86
Логическая регрессия	32003	38	129277	10	1304	16	353	16
Наивный байесовский классификатор	31984	57	129241	46	1276	44	335	34
Деревья решений	29287	2754	93943	35344	1278	42	176	193
Метод опорных векторов	32018	23	129277	10	1315	5	359	10
Метод k-ближайших соседей	32019	22	129277	10	1303	17	345	24

Таблица 7.

Точность определения подтипа атаки (23 класса) – часть 1

Классы	Random Forest	Градиентный бустинг Scikit-learn	Градиентный бустинг CatBoost	Деревья решений
back	723/723	721/723	723/723	723/723
warezmaster	4/7	0/7	2/7	3/7
land	0/6	0/6	1/6	0/6
guess_passwd	19/20	0/20	20/20	19/20
imap	1/3	0/3	2/3	0/3
ipsweep	387/391	356/391	23/391	390/391
ftp_write	4/6	0/6	3/6	3/6
spy	0/1	1/1	1/1	0/1
multihop	1/3	0/3	0/3	0/3
neptune	35268/35270	34633/35270	1454/35270	35265/35270
nmap	73/75	44/75	75/75	75/75
normal	32038/32041	27229/32041	23043/32041	32017/32041
loadmodule	0/1	0/1	0/1	1/1
perl	1/1	0/1	1/1	1/1
pod	81/84	50/84	84/84	81/84
warezclient	327/329	313/329	249/329	324/329
rootkit	1/1	0/1	0/1	0/1
satan	523/525	474/525	0/525	521/525
smurf	92868/92868	92690/92868	92787/92868	92866/92868
phf	0/1	0/1	0/1	0/1
portsweep	336/336	322/336	336/336	336/336
teardrop	325/328	166/328	115/328	326/328
buffer_overflow	7/7	0/7	7/7	7/7

Таблица 8.

Точность определения подтипа атаки (23 класса) – часть 2

Классы	Логическая регрессия	Наивный байесовский классификатор	Метод опорных векторов	Метод k-ближайших соседей
back	722/723	722/723	723/723	721/723
warezmaster	4/7	2/7	3/7	7/7
land	1/6	1/6	0/6	0/6
guess_passwd	20/20	20/20	19/20	19/20
imap	1/3	2/3	1/3	1/3
ipsweep	382/391	23/391	382/391	389/391
ftp_write	4/6	3/6	3/6	5/6
spy	0/1	1/1	0/1	0/1
multihop	0/3	0/3	0/3	1/3
neptune	3526/35270	3526/35270	1454/35270	35266/35270
nmap	70/75	75/75	70/75	72/75
normal	31988/32041	23043/32041	32020/32041	32013/32041
loadmodule	0/1	0/1	1/1	1/1
perl	0/1	1/1	0/1	1/1
pod	81/84	84/84	81/84	81/84
warezclient	325/329	249/329	324/329	326/329
rootkit	0/1	0/1	0/1	0/1
satan	510/525	488/525	519/525	519/525
smurf	92867/92868	92867/92868	92787/92868	92867/92868
phf	0/1	0/1	0/1	0/1
portsweep	335/336	336/336	334/336	334/336
teardrop	305/328	115/328	316/328	325/328
buffer_overflow	7/7	7/7	7/7	7/7

(benign = 32018/23, dos = 129277/10, probe = 1315/5, r2l = 359/10, u2r = 3/7), при определении подтипа атаки (back = 723/723, warezmaster = 3/7, land = 0/6, guess_passwd = 19/20, imap = 0/3, ipsweep = 390/391, ftp_write = 3/6, spy = 0/1, multihop = 0/3, neptune = 35265/35270, nmap = 75/75, normal = 32017/32041, loadmodule = 1/1, perl = 1/1, pod = 81/84, warezclient = 324/329, rootkit = 0/1, satan = 521/525, smurf = 92866/92868, phf = 0/1, portsweep = 336/336, teardrop = 326/328, buffer_overflow = 7/7).

В обоих случаях данный алгоритм является одним их наиболее точных и безошибочных (для 5 классов параметр accuracy составляет 0.999662, для 23 классов – 0.999576). Наиболее близко к методу деревьев решений подошел только алгоритм случайного леса (для 5 классов параметр accuracy составляет 0.999834, для 23 классов – 0.999748), однако, последний довольно сильно уступает в скорости. Модель плохо определяет только классы с очень маленьким количеством членов, что видно при определении типа атаки, где плохо идентифицировался класс u2r (3 из 7 верно определенных члена), и при определении подтипа атаки, где классы land, imap, spy, multihop, rootkit и phf не идентифицировались (содержат от 1 до 6 членов). Но все остальные классы идентифицируются моделью либо без ошибок, либо с их минимальным количеством, что подтверждается в табл. 6 и 7.

Время работы данной модели оказалось минимальным, поэтому можно предположить, что это оптимальная модель для обработки рассматриваемой выборки данных.

Литература

1. *Singh A., Gupta B. B. Distributed denial-of-service (DDoS) attacks and defense mechanisms in various web-enabled computing platforms: issues, challenges, and future research directions // International Journal on Semantic Web and Information Systems (IJSWIS). – 2022. – Т. 18. – №. 1. – С. 1–43. DOI: 10.4018/IJSWIS.297143*
2. *Eliyan L. F., Di Pietro R. DoS and DDoS attacks in Software Defined Networks: A survey of existing solutions and research challenges // Future Generation Computer Systems. – 2021. – Т. 122. – С. 149–171. DOI: 10.1016/j.future.2021.03.011*
3. *Hu Q. et al. A rotating machinery fault diagnosis method based on multi-scale dimensionless indicators and random forests // Mechanical systems and signal processing. – 2020. – Т. 139. – С. 106609. DOI: 10.1016/j.ymssp.2019.106609*
4. *Nhat-Duc H., Van-Duc T. Comparison of histogram-based gradient boosting classification machine, random Forest, and deep convolutional neural network for pavement raveling severity classification // Automation in Construction. – 2023. – Т. 148. – С. 104767. DOI: 10.1016/j.autcon.2023.104767*
5. *Hancock J. T., Khoshgoftaar T. M. CatBoost for big data: an interdisciplinary review //Journal of big data. – 2020. – Т. 7. – №. 1. – С. 94. DOI: 10.1186/s40537-020-00369-8*
6. *Schober P., Vetter T. R. Logistic regression in medical research //Anesthesia & Analgesia. – 2021. – Т. 132. – №. 2. – С. 365–366. DOI: 10.1213/ANE.0000000000005247*
7. *Wickramasinghe I., Kalutarage H. Naive Bayes: applications, variations and vulnerabilities: a review of literature with code snippets for implementation //Soft Computing. – 2021. – Т. 25. – №. 3. – С. 2277–2293. DOI: 10.1007/s00500-020-05297-6*
8. *Priyanka, Kumar D. Decision tree classifier: a detailed survey // International Journal of Information and Decision Sciences. – 2020. – Т. 12. – №. 3. – С. 246–269. DOI: 10.1504/IJIDS.2020.108141*
9. *Pisner D. A., Schnyer D. M. Support vector machine // Machine learning. – Academic Press, 2020. – С. 101–121. DOI: 10.1016/B978-0-12-815739-8.00006-7*
10. *Sinaga K. P., Yang M. S. Unsupervised K-means clustering algorithm // IEEE access. – 2020. – Т. 8. – С. 80716–80727. DOI: 10.1109/ACCESS.2020.2988796*
11. *Oyewole G. J., Thopil G. A. Data clustering: application and trends //Artificial Intelligence Review. – 2023. – Т. 56. – №. 7. – С. 6439-6475. DOI: 10.1007/s10462-022-10325-y*
12. *Ren Y. et al. Deep clustering: A comprehensive survey //IEEE Transactions on Neural Networks and Learning Systems. – 2024. DOI: 10.1109/TNNLS.2024.3403155*
13. *Antoniadis A., Lambert-Lacroix S., Poggi J. M. Random forests for global sensitivity analysis: A selective review // Reliability Engineering & System Safety. – 2021. – Т. 206. – С. 107312. DOI: 10.1016/j.ress.2020.107312*
14. *Aria M., Cuccurullo C., Gnasso A. A comparison among interpretative proposals for Random Forests // Machine Learning with Applications. – 2021. – Т. 6. – С. 100094. DOI: 10.1016/j.mlwa.2021.100094*
15. *Bo Y. et al. Real-time hard-rock tunnel prediction model for rock mass classification using CatBoost integrated with Sequential Model-Based Optimization // Tunnelling and underground space technology. – 2022. – Т. 124. – С. 104448. DOI: 10.1016/j.tust.2022.104448*

References

1. *Singh A., Gupta B. B. Distributed denial-of-service (DDoS) attacks and defense mechanisms in various web-enabled computing platforms: issues, challenges, and future research directions //International Journal on Semantic Web and Information Systems (IJSWIS). – 2022. – Т. 18. – №. 1. – С. 1–43. DOI: 10.4018/IJSWIS.297143*
2. *Eliyan L. F., Di Pietro R. DoS and DDoS attacks in Software Defined Networks: A survey of existing solutions and research challenges // Future Generation Computer Systems. – 2021. – Т. 122. – С. 149–171. DOI: 10.1016/j.future.2021.03.011*
3. *Hu Q. et al. A rotating machinery fault diagnosis method based on multi-scale dimensionless indicators and random forests // Mechanical systems and signal processing. – 2020. – Т. 139. – С. 106609. DOI: 10.1016/j.ymssp.2019.106609*

4. Nhat-Duc H., Van-Duc T. Comparison of histogram-based gradient boosting classification machine, random Forest, and deep convolutional neural network for pavement raveling severity classification //Automation in Construction. – 2023. – Т. 148. – С. 104767. DOI: 10.1016/j.autcon.2023.104767
5. Hancock J. T., Khoshgoftaar T. M. CatBoost for big data: an interdisciplinary review //Journal of big data. – 2020. – Т. 7. – №. 1. – С. 94. DOI: 10.1186/s40537-020-00369-8
6. Schober P., Vetter T. R. Logistic regression in medical research //Anesthesia & Analgesia. – 2021. – Т. 132. – №. 2. – С. 365-366. DOI: 10.1213/ANE.0000000000005247
7. Wickramasinghe I., Kalutarage H. Naive Bayes: applications, variations and vulnerabilities: a review of literature with code snippets for implementation //Soft Computing. – 2021. – Т. 25. – №. 3. – С. 2277–2293. DOI: 10.1007/s00500-020-05297-6
8. Priyanka, Kumar D. Decision tree classifier: a detailed survey //International Journal of Information and Decision Sciences. – 2020. – Т. 12. – №. 3. – С. 246–269. DOI: 10.1504/IJIDS.2020.108141
9. Pisner D. A., Schnyer D. M. Support vector machine //Machine learning. – Academic Press, 2020. – С. 101-121. DOI: 10.1016/B978-0-12-815739-8.00006-7
10. Sinaga K. P., Yang M. S. Unsupervised K-means clustering algorithm //IEEE access. – 2020. – Т. 8. – С. 80716-80727. DOI: 10.1109/ACCESS.2020.2988796
11. Oyewole G. J., Thopil G. A. Data clustering: application and trends //Artificial Intelligence Review. – 2023. – Т. 56. – №. 7. – С. 6439–6475. DOI: 10.1007/s10462-022-10325-y
12. Ren Y. et al. Deep clustering: A comprehensive survey //IEEE Transactions on Neural Networks and Learning Systems. – 2024. DOI: 10.1109/TNNLS.2024.3403155
13. Antoniadis A., Lambert-Lacroix S., Poggi J. M. Random forests for global sensitivity analysis: A selective review //Reliability Engineering & System Safety. – 2021. – Т. 206. – С. 107312. DOI: 10.1016/j.ress.2020.107312
14. Aria M., Cuccurullo C., Gnasso A. A comparison among interpretative proposals for Random Forests //Machine Learning with Applications. – 2021. – Т. 6. – С. 100094. DOI: 10.1016/j.mlwa.2021.100094
15. Bo Y. et al. Real-time hard-rock tunnel prediction model for rock mass classification using CatBoost integrated with Sequential Model-Based Optimization //Tunnelling and underground space technology. – 2022. – Т. 124. – С. 104448. DOI: 10.1016/j.tust.2022.104448

АЛГОРИТМ ИМИТАЦИИ ДИНАМИЧЕСКИХ ХАРАКТЕРИСТИК ТРАФИКА ВЕБ-СЕРВИСА

Горбачёв А. А.[1], Лысенко Д. Э.[2]

DOI: 10.21681/2311-3456-2024-4-104-115

Цель исследования: *разработка алгоритма, основанного на классе ARIMA (autoregressive integrated moving average) – интегрированной модели авторегрессии – скользящего среднего, а также оценка алгоритма для решения задачи имитации сетевого трафика веб-сервиса, позволяющего с одной стороны обеспечить заданный уровень степени сходства динамических свойств реальных узлов вычислительных сетей с ложными, а с другой стороны – приемлемый уровень вычислительной сложности алгоритма.*

Используемые методы: *критерий Акаике, метод максимального правдоподобия, расширенный тест Дики – Фуллера, тест Филипса – Перрона, градиентный спуск, тест Дарбина – Уотсона.*

Результат исследования: *разработан алгоритм, который позволяет синтезировать временной ряд моментов генерации ложного веб-трафика, имеющий относительно низкую ошибку аппроксимации динамических характеристик реального сетевого трафика в условиях приемлемой вычислительной сложности процесса структурно-параметрической идентификации модели и расчета временного ряда для имитации веб-трафика.*

Научная новизна: *заключается в применении интегрированной модели авторегрессии – скользящего среднего с учетом ее адаптивной структурной идентификации по критерию Акаике, параметрической идентификации методом максимального правдоподобия, гиперпараметрической оптимизации длины обучающей выборки и длительности структурно-параметрической идентификации модели для моделирования временного ряда задержек между пакетами ложного трафика веб-сервиса информационных систем.*

Ключевые слова: *временной ряд, моделирование, маскирование, веб-сервис, ложные сетевые информационные объекты, имитация трафика.*

ALGORITHM FOR SIMULATING DYNAMIC TRAFFIC CHARACTERISTICS WEB SERVICE

Gorbachev A. A.[3], Lysenko D. E.[4]

The purpose of the study: *The aim of the work is to develop a model and algorithm based on the class of the integrated autoregression model – the moving average (hereinafter referred to as the ARIMA model), as well as to assess their quality to solve the problem of generating false dynamic properties of real nodes of computer networks when generating false network traffic of a web service, allowing on the one hand to provide a given level of similarity dynamic properties of real nodes of computer networks with false ones, and on the other hand, an acceptable level of computational complexity of the mathematical apparatus.*

The methods used are: *Akaike criterion, maximum likelihood method, extended Dickey – Fuller test, Philips – Perron, gradient descent, Darbin – Watson test, Harke – Bera, Cochrane criterion, direct and iterative time series generation method.*

Result: *the presented model makes it possible to synthesize a time series of moments of generating false web traffic, which has a relatively low error in approximating the dynamic characteristics of real network traffic in conditions of acceptable computational complexity of the process of structural parametric identification of the model and calculation of a time series for generating false web traffic. The presented algorithm makes it possible to increase the effectiveness of protecting computer network nodes by reducing the ability of an attacker to uncover the fact of generating false network traffic in terms of its dynamic characteristics.*

1 Горбачёв Александр Александрович, кандидат технических наук, Краснодарское высшее военное орденов Жукова и Октябрьской Революции Краснознаменное училище имени генерала армии С. М. Штеменко, г. Краснодар, Россия. E-mail: infosec23.00@mail.ru

2 Лысенко Дмитрий Эдуардович, Краснодарское высшее военное орденов Жукова и Октябрьской Революции Краснознаменное училище имени генерала армии С. М. Штеменко, г. Краснодар, Россия. E-mail: dmitrii.Lysencko@yandex.ru

3 Alexander A. Gorbachev, Ph.D., Krasnodar Higher Military Orders of Zhukov and the October Revolution Red Banner School named after General of the Army S. M. Shtemenko, Krasnodar, Russia. E-mail: infosec23.00@mail.ru

4 Dmitry E. Lysenko, Krasnodar Higher Military Orders of Zhukov and the October Revolution Red Banner School named after General of the Army S. M. Shtemenko, Krasnodar, Russia. E-mail: Dmitrii.Lysencko@yandex.ru

Scientific novelty: *it consists in the application of an integrated autoregression model – a moving average, taking into account its adaptive structural identification according to the Akaike criterion, parametric identification by the maximum likelihood method, hyperparametric optimization of the length of the training sample and the duration of the structural-parametric identification of the model to simulate a time series of delays between packets of false traffic of a web service of military information systems.*

Keywords: *time series, modeling, masking, web service, false network information objects, traffic simulation.*

Введение

В связи с ростом объемов обработки данных и предоставления информационных сервисов через Интернет, становится критически важным обеспечение их информационной безопасности. Атаки на веб-приложения – один из наиболее популярных методов кибератак.

По данным исследования центра реагирования на инциденты информационной безопасности промышленных инфраструктур «Лаборатории Касперского» (Kaspersky ICS CERT), 17% от общего числа атак пришлось на эксплуатацию уязвимостей и недостатков защиты веб-приложений[5].

Злоумышленники могут использовать скомпрометированные сайты в различных целях: для распространения вредоносного программного обеспечения, кражи конфиденциальных данных, несанкционированного внедрения информации, для мошенничества или проникновения во внутреннюю инфраструктуру организации [1].

Наряду с наиболее распространенными мерами защиты, включающими в себя методы и средства предотвращения вторжений [2], обнаружения и реагирования на инциденты[6], средства криптографической защиты[7], резервного копирования и восстановления[8], целесообразными для применения в общей системе защиты информационных систем являются методы и средства маскирования информационных направлений (трафика) [3, 4]. Маскирование трафика потенциально позволяет обеспечить выполнение требований к мерам защиты информационных систем, включающих: скрытие архитектуры и конфигурации систем [5, 6]; создание фиктивных систем или компонентов для обнаружения и анализа действий атакующих[9]; имитацию или сокрытие настоящих информационных технологий и структурных особенностей системы [7, 8].

Маскирование трафика осуществляется посредством имитации реального трафика между узлами вычислительной сети. В настоящее время разработан ряд научно-технических предложений по имитации реального трафика в локальных вычислительных сетях[10]. Однако, задача по обеспечению заданного уровня степени сходства динамических свойств реальных узлов вычислительных сетей с ложными при имитации сетевого трафика веб-сервиса остается актуальной.

При использовании обманных систем (*deception systems*, ложных сетевых информационных объектов) для маскирования трафика, системы могут стать менее уязвимыми к атакам, направленным на их дестабилизацию или выведение из строя. Это особенно важно для критических инфраструктур, таких как финансовые учреждения, здравоохранение и государственные службы, где последствия кибератак могут иметь значительные масштабы.

Имитация трафика веб-сервиса ложными сетевыми информационными объектами потенциально позволяет снизить эффективность сетевой разведки по отношению к узлам вычислительной сети.

Основная идея состоит в создании ложного трафика, который затрудняет выделение и анализ важных данных за счет:

5 Второе полугодие 2023 года — краткий обзор основных инцидентов промышленной кибербезопасности // Официальный информационный ресурс АО «Лаборатория Касперского» [Электронный ресурс]. 2023. – URL: https://ics-cert.kaspersky.ru (дата обращения 17.04.2024).

6 Канев А. Н. Мониторинг событий и обнаружение инцидентов информационной безопасности с использованием SIEM-систем // Международный студенческий научный вестник. 2015. №. 3-1. С. 122–123.

7 Авдошин С. М., Савельева А. А. Криптографические методы защиты информационных систем // Известия АИН им. А. М. Прохорова. Бизнес-информатика. 2006. Т. 17. №. 2. С. 91–99.

8 Даниленко А. Ю. Защита данных в сложных информационных системах // Труды Института системного анализа Российской академии наук. 2007. Т. 29. С. 49–58.

9 Иванов И. И., Максимов Р. В. Спецификация функциональной модели для расширения пространства демаскирующих признаков в виртуальных частных сетях // Инновационная деятельность в Вооруженных Силах Российской Федерации: Труды всеармейской научно-практической конференции, Санкт-Петербург. ВАС, 2017. С. 138–147.

10 Татарникова Т. М. Статистические методы исследования сетевого трафика // Информационно-управляющие системы. – 2018. – №. 5 (96). – С. 35–43.

- имитации активности пользователей и системных процессов путём имитации трафика, не несущего реальной информационной нагрузки, что создаёт дополнительный объём данных, среди которого злоумышленнику сложнее выделить значимую информацию;
- изменения параметров сетевого трафика, включая интервалы времени между пакетами, размеры пакетов и порядок их следования, для создания случайного характера трафика;
- применения алгоритмов машинного обучения для адаптации ложного трафика под текущие условия сети и активность пользователя, обеспечивая высокий уровень реалистичности и эффективности маскирования.

В данной статье разработан алгоритм, который может значительно повысить результативность защиты информационных систем от внутренних и внешних угроз. Сформулирована и решена задача структурно-параметрической идентификации интегрированной модели авторегрессии – скользящего среднего (*ARIMA*) для синтеза временного ряда моментов имитации сетевого трафика веб-сервиса от узлов вычислительной сети.

Идентификация сетевого трафика является одной из задач в области безопасности, защиты и управления трафиком сетей передачи данных. Решение данной задачи осуществляется с использованием методов классификации и моделирования сетевого трафика.

В основе ряда моделей трафика лежат стационарные случайные процессы, с помощью которых воспроизводятся характеристики трафика (количество пакетов, полученных или отправленных в течение определенного промежутка времени; интервалы между пакетами и т.д.). Основными из них являются:

- модели на основе законов распределения[11];
- модели на основе теории фракталов [9];
- регрессионные и авторегрессионные модели[12];
- модели экспоненциального сглаживания[13];
- модели, основанные на алгоритмах машинного обучения[14];
- модели на базе цепей Маркова [10];
- классификационные модели и др. [11, 12].

Наиболее популярными и широко используемыми являются классы авторегрессионных и нейросетевых моделей[15]. В рамках рассматриваемой задачи имитации трафика, с целью выделения достаточного ресурса для хранения трафика в сетевом оборудовании в краткосрочном промежутке времени, авторегрессионная модель имеет ряд преимуществ перед моделями глубокого обучения. В условиях малого количества исходных данных, высокой изменчивости статистических и динамических свойств временных рядов, отсутствия значительных временных и вычислительных ресурсов на обучение алгоритмов глубокого обучения, данная модель способна генерировать с приемлемой ошибкой аппроксимации временной ряд задержек между пакетами сетевого трафика на относительно коротких промежутках времени. В данной статье будут рассматриваться модели на основе стохастических временных рядов.

Модель *ARIMA* широко используется для анализа и генерирования значений временных рядов благодаря возможности моделировать различные типы данных, включая нестационарные временные ряды. Для построения модели *ARIMA* достаточно использовать информацию, содержащуюся в самих анализируемых данных временного ряда. Если ряд после взятия d последовательных разностей сводится к стационарному, то для генерирования новых значений временного ряда можно применить комбинированную модель авторегрессии и скользящего среднего, обозначаемую как ARIMA (p, d, q). Сокращение I в данной аббревиатуре означает «интегрированный» [13, 14].

Модель ARIMA (p, d, q) *– (модель Бокса-Дженкинса или модель интегрированной авторегрессии – скользящего среднего)* позволяет работать с зависимостями, имеющими тренд (1), параметры модели приведены в таблице 1.

$$\Delta^d Y_t = c + \sum_{i=1}^{p} \alpha_i \Delta^d Y_{t-i} + \sum_{j=1}^{q} \beta_j \Delta^d \varepsilon_{t-j} + \varepsilon_t, \quad (1)$$

11 Тырсин А. Н. Метод подбора наилучшего закона распределения непрерывной случайной величины на основе обратного отображения //Вестник Южно-Уральского государственного университета. Серия: Математика. Механика. Физика. – 2017. – Т. 9. – №. 1. – С. 31–38.

12 Селиверстова А. В. Сравнительный анализ моделей и методов прогнозирования // Современные научные исследования и инновации. 2016. № 11(67). С. 241–248.

13 Калекар П. С. Прогнозирование временных рядов с использованием экспоненциального сглаживания Холта-Уинтерса // Школа информационных технологий имени Канвала Рекхи. 2004. №.13. С. 1–13.

14 Гладышев А. И., Жуков А. О. Достоинства и недостатки имитационного моделирования с использованием нейронных сетей // Вестник Российского нового университета. 2013. №. 4. С. 53.

15 Тихонов Э. Е. Методы прогнозирования в условиях рынка: учебное пособие. Невинномысск, 2006. – 221 с.

Таблица 1.

Параметры модели ARIMA

Параметры	Описание
Y_t	уровень временного ряда в момент времени t (зависимая переменная)
Y_{t-i}	уровни временного ряда в моменты времен, соответственно (независимые переменные)
α_i	оцениваемые коэффициенты авторегрессии
ε_t	случайное возмущение, описывающее влияние переменных, не учтенных в модели
ε_{t-j}	значения остатков j временных периодов назад (независимые переменные)
β_j	оцениваемые коэффициенты скользящего среднего
d	порядок модели *ARIMA*, характеризующий степень интегрирования
Δ^d	оператор взятия конечной разности порядка d
p	параметр обозначает количество лагов (задержек) временного ряда, используемых в качестве предикторов
q	параметр указывает на количество лагов ошибок сгенерированных новых значений, используемых в модели

В общем виде модель (2) представляет собой отображение входных характеристик в выходные. Входные характеристики представляют собой множество управляемых факторов-аргументов A (3-4) и множество неуправляемых параметров S (5). Выходные характеристики модели Z (6) представляют собой временной ряд пауз между пакетами генерируемого ложного сетевого трафика веб-сервиса, то есть модель позволяет реализовать имитацию трафика в смысле идентичности динамических характеристик реального и ложного трафика без имитации содержимого.

$$F : \{A,S\} \longrightarrow Z, \quad (2)$$

В качестве неуправляемых и управляемых факторов выступают:

$$A = \{p,q,\Theta,l\}, \quad (3)$$

$$\Theta = \{c,\alpha_i,\beta_j,\varepsilon_\tau\},\ i \in [1,...,p],\ j \in [1,...,q],\ d \in [0,1], \quad (4)$$

$$S = \{\tau_1,...,\tau_K\}, \quad (5)$$

$$Z = \{F(\tau_1,p,q,\Theta,n),...,F(\tau_K,p,q,\Theta,n)\}. \quad (6)$$

где: Θ – параметры модельного оператора, l – длина аппроксимируемого ряда, S – множество неуправляемых параметров (входной имитируемый временной ряд пауз между Опакетами реального сетевого трафика веб-сервиса), Z – выходные характеристики модели, представляющие собой временной ряд пауз между пакетами имитируемого (ложного сетевого трафика).

Область допустимого множества факторов модели формализована выражением 7:

$$Q = \begin{cases} \tau \in R;\ n \in [1,...,10^5]; \\ p \in [0,...,5];\ q \in [0,...,5];\ d \in [0,1]; \\ c \in R;\ \varepsilon_t \in [0,+\infty]; \\ \alpha_i \in [-1,1];\ \beta_j \in [-1,1]. \end{cases} \quad (7)$$

Модель применяется для генерации новых значений временного ряда Z.

Таблица 2.

Основные исходные данные

Параметры	Описание
l	длина считываемого временного ряда, задержек между пакетами сетевого трафика вычислительной сети, необходимых для идентификации математической модели *ARIMA* или устанавливается временной интервал, в течение которого будут собираться данные.
K^*_{st}	критическое значение критерия стационарности временного ряда для уровня значимости с целью определения стационарности временного ряда и структурной идентификации математической модели *ARIMA*.

Описание алгоритма имитации динамических характеристик трафика веб-сервиса

Основной задачей алгоритма является поиск оптимальных параметров интегрированной модели авторегрессии – скользящего среднего для генерации новых значений пауз между пакетами ложного трафика, основанного на динамических характеристиках реального трафика информационных систем, тем самым снижая эффективность сетевой разведки злоумышленников и последующей реализации компьютерных атак в вычислительной сети.

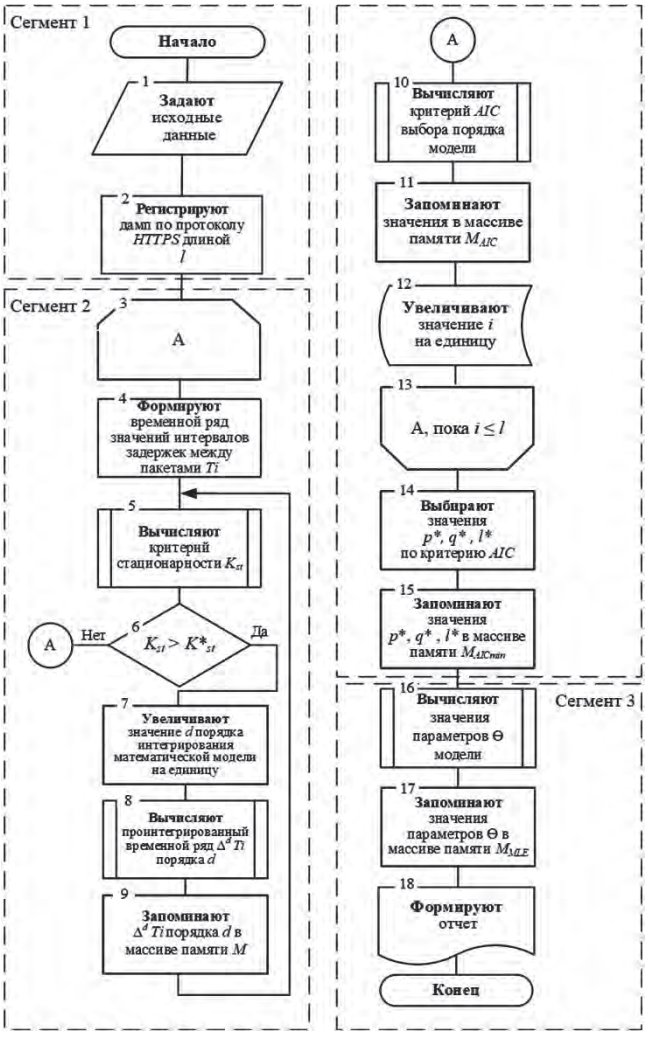


Рис. 1. Алгоритм структурной и параметрической идентификации модели

Создание модифицированных потоков данных обеспечивает среду, в которой атакующие сталкиваются с препятствиями при попытке идентифицировать реальные (отличить от ложных) информационные ресурсы, в связи с чем снижается качество анализа сетевого трафика злоумышленниками.

В таком случае особенно важно не только разработать адекватный алгоритм генерации, но и учесть природу трафика, протокол передачи, архитектуру сети, степень загруженности и характер нагрузки. В зависимости от перечисленных выше факторов динамические свойства трафика будут различаться.

Реализация предлагаемого алгоритма структурной и параметрической идентификации интегрированной модели авторегрессии – скользящего среднего для имитации трафика веб-сервиса поясняется блок-схемой последовательности действий, представленной на рис. 1 и включает следующие этапы:

1. *Задают исходные данные (блок 1), обозначение и описание которых приведены в таблице 2.*

Регистрируют дамп реального сетевого трафика по протоколу *HTTPS* (блок 2 на рис. 2).

Выполняют сбор сетевого трафика с помощью специализированного программного обеспечения и проводят фильтрацию данных, ограничиваясь пакетами, передаваемыми через порты, характерными для протокола *HTTPS* (*HyperText Transfer Protocol Secure*). Особое внимание уделяется пакетам с флагом *SYN*, которые инициируют *TCP*-соединения. К примеру, выборка из дампа сетевого трафика

вычислительной сети, снятого с сетевого устройства за 4 часа рабочего времени, содержит 7587 фактов регистрации поступления *TCP*-пакетов с флагом *SYN* на установление сетевого соединения по протоколу *HTTPS* (рис. 2). Для обеспечения точности и надежности результатов анализа была проведена предварительная обработка данных. В частности, была проведена очистка данных от поврежденных пакетов и пакетов, не относящихся к исследуемому потоку данных.

2. *Формируют временной ряд пауз между пакетами протокола HTTPS (рис. 3а) и проверяют*

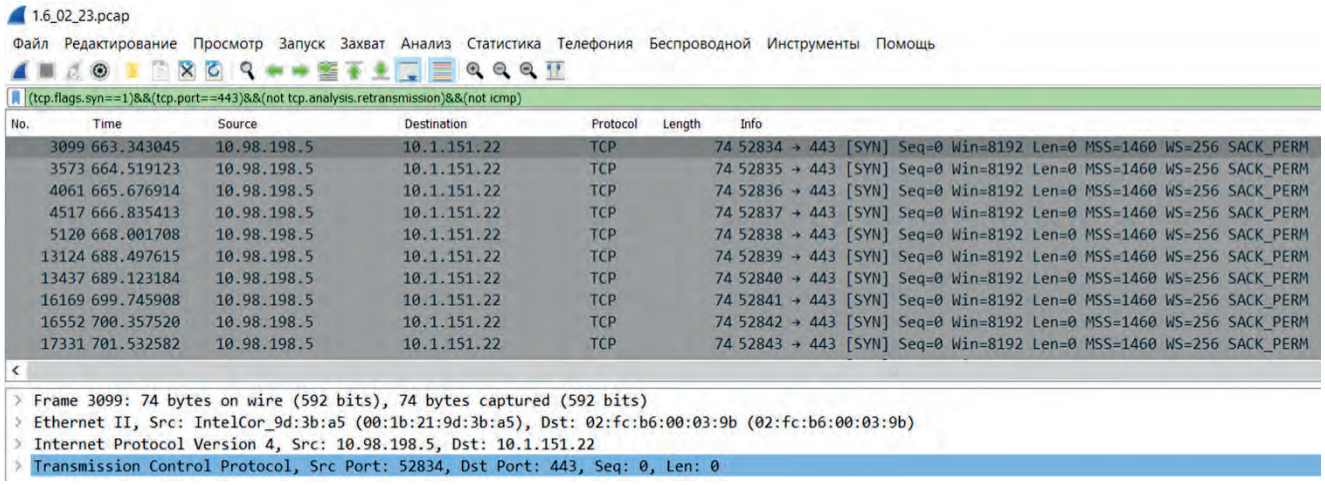


Рис. 2. Извлечение признаков из эмпирических данных о событиях, характеризующих временной ряд

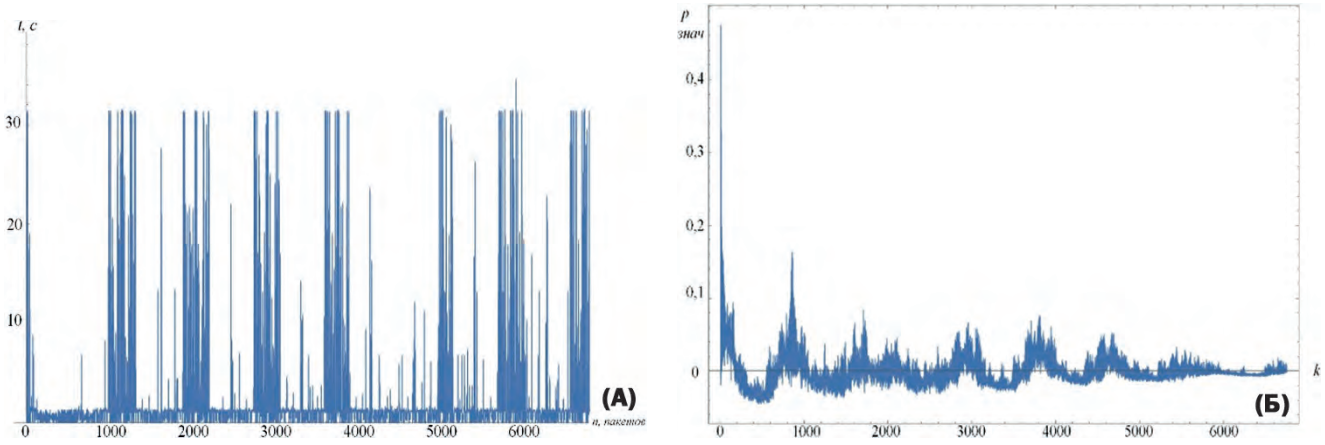


Рис.3. а) График временного ряда пауз между SYN–пакетами веб-трафика;
б) График автокорреляционной функции процесса регистрации TCP пакетов с флагом SYN на установление сетевого соединения

Таблица 3.

Результаты оценки стационарности исследуемого временного ряда с использованием тестов единичного корня

Наименования теста (критерия)	Значение статистики	p - value	Уровень значимости	Интерпретация результатов теста
Тест Дики – Фуллера	-87,840	1,6585×10-8	0,05	временной ряд стационарен
Расширенный Тест Дики – Фуллера	-6,892	6,0228×10-9	0,05	временной ряд стационарен
Тест Филипса – Перрона	-27,931	2,077×10-5	0,05	временной ряд стационарен

временной ряд на наличие явного тренда и гетероскедастичности (непостоянной дисперсии) (рис. 3б) для дальнейшего анализа и выбора модели (блок 4 на рис. 2).

Проверяют временной ряд на стационарность (блок 5, 6 на рис. 2). Оценка стационарности временного ряда может быть проведена с использованием специфических параметрических тестов или статистических «тестов единичного корня» (*Unit root test*), которые позволяют оценить стационарность временного ряда (табл. 3).

В случае, если условие $K_{st} > K^*_{st}$ не выполняется, что соответствует сетевому трафику, обладающему свойством стационарности, вычисляют значения критерия Акаике (*AIC*) для выбора порядка математической модели для всех комбинаций параметров p, q порядка модели (блок 10 на рис. 2).

В случае если условие $K_{st} > K^*_{st}$ выполняется, что соответствует сетевому трафику, не обладающему свойством стационарности, увеличивают значение порядка интегрирования Δ^d математической модели на единицу. Затем вычисляют проинтегрированный временной ряд $\Delta^d T_i$ порядка Δ^d задержек между пакетами сетевого трафика длиной l. После чего запоминают проинтегрированный временной ряд порядка Δ^d в массиве памяти M. Затем вычисляют значение критерия стационарности K_{st} проинтегрированного временного ряда порядка Δ^d (блок 7–9 на рис.2).

Выбирается модель с параметрами порядка, соответствующими минимальному значению статистики[16]:

$$AIC(A,S) = 2k(A,S) - 2ln(\bar{L}(A,S)) \longrightarrow \min_{A,S \in Q} \qquad (8)$$

где k – количество оцененных параметров (включая p, q, константу c, если она включена, и дисперсию ошибок σ^2; $\bar{L}$ – максимальное значение логарифмической функции правдоподобия.

Данная процедура повторяется для каждой модели *ARMA*, и выбирается модель с наименьшим критерием *AIC*. Использование *AIC* в качестве инструмента для выбора модели *ARMA* позволяет автоматизировать процесс поиска оптимальных параметров, особенно при использовании программного обеспечения для статистического анализа, которое может быстро перебирать множество комбинаций параметров и автоматически вычислять *AIC* для каждой модели. Результаты запоминаются в массиве памяти M_{AIC} (блок 11 на рис. 2).

Итерационный процесс продолжается до тех пор, пока не будет найдена оптимальная модель по информационному критерию Акаике и оптимальная длина временного ряда, начиная с минимальной длины $l = 2$ и увеличиваясь с шагом $i = 1$ (блок 12–15 на рис. 2).

3. *Оценка параметров модели по методу максимального правдоподобия (блок 16 на рис.2).*

После структурной идентификации, проведенной на предыдущем шаге, осуществляется параметрическая идентификация модели.

В статистике применяются три основных метода оценивания:

1) метод наименьших квадратов;
2) метод моментов;
3) метод максимального правдоподобия [15].

Как правило, применение метода максимального правдоподобия для этих целей в моделях *ARIMA* (p, d, q) дает асимптотически несмещенную, состоятельную и эффективную оценку параметров. Его используют для любых моделей, задающих вид распределения наблюдаемых переменных. Два других метода можно использовать лишь тогда, когда распределение переменных можно представить в определенном виде. Если есть гипотеза о точном виде распределения, то всегда понятно, как получать оценки параметров, распределений параметров и различных статистик, как проверять гипотезы, хотя сами расчеты могут быть относительно трудоемкими. Если правильно выбрать параметризацию, то распределение оценок в малых выборках может быть близко к асимптотическому, если неправильно, то асимптотическое распределение будет неудовлетворительной аппроксимацией.

Оценка параметров модели представляет собой ключевой этап в анализе временного ряда, который требует точного и систематического подхода. На первом этапе строится логарифмическая функция правдоподобия $ln\ L$, которая представляет собой логарифм вероятности наблюдаемых данных

16 Носко В. П. Эконометрика. Элементарные методы и введение в регрессионный анализ временных рядов / В. П. Носко. – Москва: Фонд «Институт экономической политики им. Е. Т. Гайдара», 2004. – 501 с.

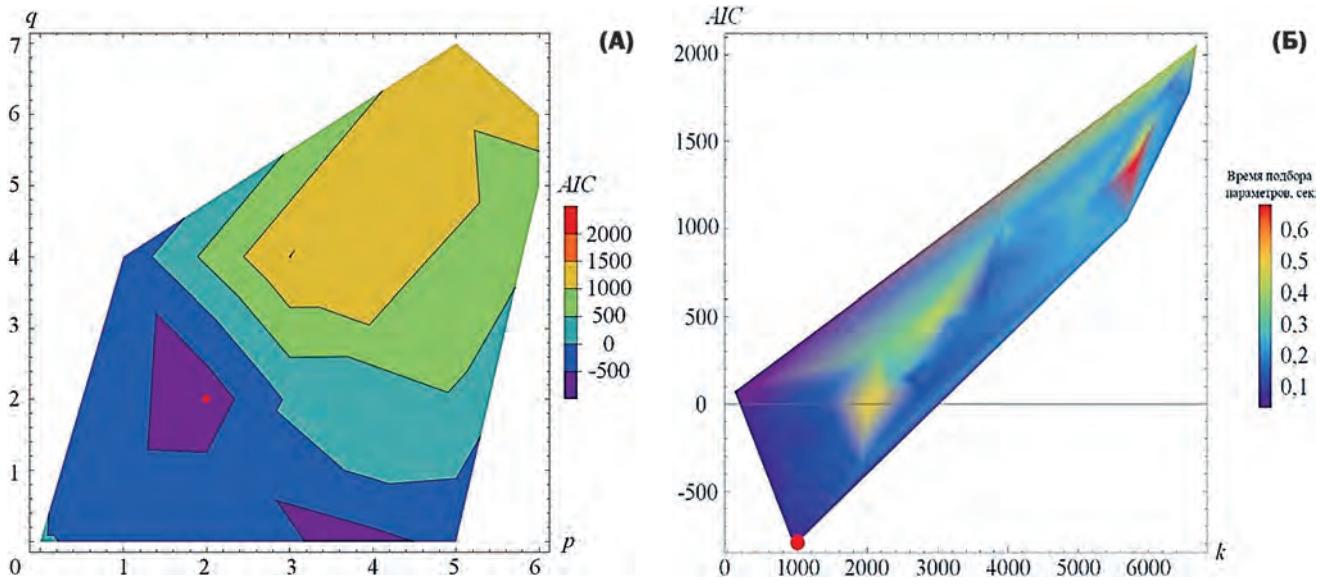


Рис. 4. Графическая интерпретация структурной идентификации модели:
структурная идентификация модели по критерию Акаике (а); оценка оптимальной длины обучающей выборки k^* (б)

Таблица 4.

Результаты значений параметров авторегрессии, скользящего среднего и дисперсии ошибок

Модель и ее порядок	**Длина обучающей выборки временного ряда k, знач.**	**Значение параметров**	**Значение *AIC***	**Время оценки параметров, сек**
ARMA (2,2)	1000	$c = 0{,}25986, \{\hat{a}_i = 0{,}17677; 0{,}47375\}, \{\hat{\beta}_j = -0{,}15073; -0{,}176258\}, \hat{\sigma}^2 = 0{,}446593$	–794	0,7757
ARMA (4,0)	800	$c = 0{,}34921, \{\hat{a}_i = 0{,}0174;0{,}2389;0{,}0808;0{,}1622\}, \hat{\sigma}^2 = 0{,}44329$	–638	0,0830
ARMA (2,1)	600	$c = 0{,}05116, \{\hat{a}_i = 0{,}95010; 0{,}00414\}, \{\hat{\beta}_j = -0{,}87796\}, \hat{\sigma}^2 = 1{,}2913$	–399	0,0720
ARMA (5,0)	1900	$c = 0{,}44921, \{\hat{a}_i = 0{,}0800; 0{,}1275; 0{,}1477; 0{,}1000; 0{,}054\}, \hat{\sigma}^2 = 0{,}8224$	–357	0,1724
ARMA (1,3)	1100	$c = 0{,}26701, \{\hat{a}_i = 0{,}76122\}, \{\hat{\beta}_j = -0{,}66714; 0{,}02674; 0{,}02489; 0{,}0531\}, \hat{\sigma}^2 = 1{,}31893$	–310	0,1190

Таблица 5.

Результаты работы алгоритма по поиску оптимальных значений

Размер обучающей выборки, шт.	1000
Модель	*ARMA* (2,2)
Значение AIC	–794
Параметры модели	$c = 0{,}25986, \{\hat{a}_i = 0{,}17677; 0{,}47375\}, \{\hat{\beta}_j = -0{,}15073; -0{,}176258\}, \hat{\sigma}^2 = 0{,}446593$
Время подбора параметров, с	0,0096975
Общее время работы алгоритма, с	67, 4401839

при заданных параметрах модели. Для модели *ARIMA* (p, d, q) эта функция может быть выражена как (9):

$$lnL\,(a_i,\beta_j,\sigma^2) = -\frac{n}{2}\ln(2\pi\sigma^2) - \frac{1}{2\sigma^2}\sum_{t=1}^{n}(Y_t - \tilde{Y}_t)^2, \quad (9)$$

где Y_t – значение временного ряда в момент времени t; $\tilde{Y}_t$ – предсказанные значения модели; a_i – коэффициент *AR* части модели; β_j – коэффициент *MA* части модели; σ^2 – оценка дисперсии ошибок; n – общее количество наблюдений.

Для максимизации функции правдоподобия необходимо вычислить её частные производные по каждому из параметров модели: a_i (для $i = 1, \ldots, p$), β_j (для $j = 1,\ldots,q$) и σ^2. Это позволит определить направление наискорейшего роста функции правдоподобия.

Поскольку аналитическое решение задачи максимизации логарифмической функции правдоподобия часто недостижимо, применяются численные методы оптимизации, такие как градиентный спуск, метод Ньютона – Рафсона или алгоритмы квази-Ньютона. Эти методы итеративно корректируют оценки параметров, двигаясь в направлении градиента логарифмической функции правдоподобия.

Итерационный процесс продолжается до тех пор, пока не будет достигнут критерий сходимости (пока изменения в логарифмической функции правдоподобия или в значениях параметров не станут незначительными, в нашем случае это значение равно 10^{-4}). Это указывает на то, что были найдены параметры, максимизирующие функцию правдоподобия, и процесс оптимизации может быть остановлен.

После завершения процесса параметрической оптимизации, полученные значения параметров $\hat{a}_i$, $\hat{\beta}_j$, $\hat{\sigma}^2$ используются как оценки исходных параметров модели *ARIMA*. Эти оценки предоставляют информацию о взаимосвязях внутри временного ряда и могут быть использованы для дальнейшего анализа и генерации новых значений. В контексте модели *ARIMA* это может быть записано как (10):

$$(\hat{a}_i,\hat{\beta}_j,\hat{\sigma}^2) = argmax_{a_i,\beta_i,\sigma^2 \in Q}\, lnL(a_i,\beta_j,\sigma^2) \quad (10)$$

где: $\hat{a}_i$, $\hat{\beta}_j$, $\hat{\sigma}^2$ – оцененные значения параметров авторегрессии, скользящего среднего и дисперсии ошибок соответственно; $lnL(a_i,\beta_j,\sigma^2)$ – логарифмическая функция правдоподобия модели.

В процессе исследования была выполнена оценка и выбор оптимальных моделей, расчет их параметров и времени выполнения по информационному критерию Акаике. Изначально для каждого временного ряда, начиная с минимальной длины $l = 2$ и увеличиваясь с шагом $i = 1$, была подобрана модель (рис. 4).

После чего была сформирована таблица, содержащая данные о типе модели, параметрах авторегрессии и скользящего среднего, константе, дисперсии шума, порядках модели (p и q), времени выполнения расчетов и значения *AIC*. Для удобства анализа и дальнейшего обсуждения результаты были упорядочены по возрастанию значения критерия *AIC*, что позволило выделить модели с наилучшими значениями информационного критерия. Из полной таблицы были отобраны 5 наилучших моделей, которые демонстрируют наименьшее значение *AIC*, указывающее на оптимальное соотношение между качеством аппроксимации и сложностью модели. Результаты полученных значений представлены в таблице 4.

Формируют отчет (блок 18 на рис. 2). Формируется таблица (таблица 5), включающая результаты структурной и параметрической идентификации модели ARMA.

Вывод

В ходе исследования был разработан алгоритм структурной и параметрической идентификации интегрированной модели авторегрессии – скользящего среднего, который позволяет синтезировать временной ряд моментов имитации веб-трафика, имеющий низкую ошибку аппроксимации динамических характеристик реального сетевого трафика в условиях приемлемой вычислительной сложности процесса структурно-параметрической идентификации модели и расчета временного ряда для имитации веб-трафика. Подход базировался на итеративной процедуре структурной идентификации и оценки параметров моделей.

Структурная идентификация модели *ARIMA* осуществлялась посредством автоматического выбора порядков модели. Определены диапазоны значений для параметров авторегрессии (p) и скользящего среднего (q), которые для модели *ARIMA*(p, d, q)

находятся в следующих интервалах: p от 0 до 5, q от 0 до 3, порядок интегрирования d был определен в интервале от 0 до 2. Оценка моделей по информационному критерию Акаике выявила, что оптимальные значения *AIC* находятся в диапазоне от –794 до 2000 для различных комбинаций p и q.

Размеры обучающих выборок k были определены в интервале от 200 до 2800 значений, что демонстрирует гибкость подхода в адаптации к разнообразным объемам данных.

Числовые результаты для выбранных моделей *ARMA*(p, q) и *ARIMA*(p, d, q) отражают следующее: модель *ARMA*(2,2) с длиной обучающей выборки в 1000 значений и параметрами $c = 0{,}25986$, $\{\hat{a}_i = 0{,}17677;\ 0{,}47375\}$, $\{\hat{\beta}_j = -0{,}15073;\ -0{,}176258\}$, $\hat{\sigma}^2 = 0{,}446593$, показала *AIC* равный –794, что является оптимальным результатом в данном исследовании.

Время, затраченное на подбор параметров, составило 0,0096975 секунды, демонстрируя относительно высокую вычислительную эффективность разработанного алгоритма. Общее время работы алгоритма составило 67,4401839 секунды, подтверждая возможность его использования в условиях реального времени.

Сформированная на основе этого подхода процедура оценки моделей позволяет достичь оптимального баланса между точностью моделирования и вычислительной сложностью модели и алгоритма. Сложные и многоэтапные процедуры, такие как перебор параметров модели и оценка стационарности рядов, требуют значительных вычислительных ресурсов. Поэтому оптимизация алгоритмов подобных процессов играет ключевую роль в повышении эффективности общей системы анализа сетевого трафика.

Полученные результаты могут быть использованы для разработки алгоритма имитации сетевого трафика с целью введения в заблуждение злоумышленников и повышения защищенности информационных систем.

Литература

1. *Шерстобитов Р. С. Модель маскирования информационного обмена в сети передачи данных ведомственного назначения // Системы управления, связи и безопасности. 2024. № 1. С. 1–25. DOI: 10.24412/2410-9916-2024-1-001-025.*
2. *Фатеев А. Г. Применение средств защиты информации для реализации мер защиты, установленных специальными нормативными документами Федеральной службы по техническому и экспертному контролю // Инжиниринг и технологии. 2020. Т. 5, № 1. С. 24–29. DOI 10.21685/2587-7704-2020-5-1-6.*
3. *Москвин А. А., Максимов Р. В., Горбачев А. А. Модель, оптимизация и оценка эффективности применения многоадресных сетевых соединений в условиях сетевой разведки // Вопросы кибербезопасности. 2023. № 3(55). С. 13–22. DOI 10.21681/2311-3456-2023-3-13-22.*
4. *Горбачев А. А., Максимов Р. В. Проблема маскирования и применения технологий машинного обучения в киберпространстве // Вопросы кибербезопасности. 2023. № 5(57). С. 37–49. DOI 10.21681/2311-3456-2023-5-37-49.*
5. *Maximov R. V., Sokolovsky S. P., Telenga A. P. Methodology for substantiating the characteristics of false network traffic to simulate information systems // CEUR Workshop Proceedings : BIT 2021 – Selected Papers of 11th International Scientific and Technical Conference on Secure Information Technologies, Moscow. 2021. pp. 115–124.*
6. *Maximov R. V., Sokolovsky S. P., Telenga A. P. Honeypots network traffic parameters modelling // CEUR Workshop Proceedings: BIT 2021 – Selected Papers of 11th International Scientific and Technical Conference on Secure Information Technologies, Moscow. 2021. pp. 229–239.*
7. *Способ (варианты) защиты вычислительных сетей. Патент № 2307392 C1 Российская Федерация, МПК G06F 21/00, H04L 9/32. Выговский Л. С., Заргаров И. А., Кожевников Д. А., Максимов Р. В., Павловский А. В.,Стародубцев Ю. И., Худайназаров Ю. К., Юров И. А.; заявитель и патентообладатель Военная академия связи (RU). – № 2006114974/09 : заявл. 02.05.2006: опубл. 27.09.2007.*
8. *Способ контроля информационных потоков в цифровых сетях связи. Патент № 2267154 C1 Российская Федерация, МПК G06F 12/14, G06F 11/00. Андриенко А. А., Куликов О. Е., Костырев А. Л., Максимов Р. В., Павловский А. В., Лебедев А. Ю., Колбасова Г. С.; заявитель и патентообладатель Военная университет связи (RU). № 2004121529/09. заявл. 13.07.2004; опубл. 27.12.2005.*

9. Мельникова Ю. В., Лажаунинкас Ю. В. Компьютерное моделирование экономических процессов с применением методов фрактального анализа // Наука Красноярья. – 2022. – Т. 11. – №. 4. – С. 7–23.
10. Егоров И. К. Проверка прогнозирования посещения веб-страниц на основе цепи Маркова для моделирования профиля поведения пользователей / И. К. Егоров, В. Ю. Радыгин // Инновационные механизмы управления цифровой и региональной экономикой: Материалы V Международной студенческой научной конференции, Москва, 15-16 июня 2023 года. – Москва: Национальный исследовательский ядерный университет «МИФИ», 2023. – С. 429–437.
11. Микульский А. А. Обзор моделей прогнозирования // Dunărea–Nistru: Anuar. 2019. Т. 6. С. 284–304.
12. Хайндман Р. и Атанасопулос Дж. Прогнозирование: принципы и практика / пер. с англ. А. В. Логунова. – М.: ДМК Пресс, 2023. – 458 с.: ил
13. Мирзакулова Ш. А. Исследование временного ряда на стационарность // Образовательная система: новации в сфере современного научного знания: сборник научных трудов. Казань: ООО «СитИвент», 2019. С. 318–333.
14. Фелькер М. Н., Чеснов В. В. Исследование влияния изменения параметров модели ARIMA на качество прогноза для коротких наборов данных // Вестник Южно-Уральского государственного университета. Серия: Компьютерные технологии, управление, радиоэлектроника. 2021. Т. 21. №. 3. С. 36–46.
15. Скоробогатых Е. Ю. К вопросу о методах нахождения оценок параметров регрессионных моделей / Е. Ю. Скоробогатых, С. Н. Мухина // Известия Балтийской государственной академии рыбопромыслового флота: психолого-педагогические науки. – 2023. – № 3(65). – С. 205-212. – DOI 10.46845/519.242071-5331-2023-3-65-205-212.

References

1. Sherstobitov R. S. Model maskirovaniya informatsionnogo obmena v seti peredachi dannikh vedomstvennogo naznacheniya [A model for organizing information exchange in a departmental data transmission network has been developed]. Management, communication and security systems. 2024. vol. 1. pp. 1–25. DOI: 10.24412/2410-9916-2024-1-001-025.
2. Fateev A. G. Primenenie sredstv zashchiti informatsii dlya realizatsii mer zashchiti, ustanovlennikh spetsialnimi normativnimi dokumentami Federalnoi sluzhbi po tekhnicheskomu i ekspertnomu kontrolyu [The use of information security tools for the implementation of protection measures established by special regulatory documents of the Federal Service for Technical and Expert Control]. // Inzhiniring i tekhnologii, 2020, vol. 1, pp. 24–29 (in Russia).
3. Moskvin A. A., Maksimov R. V., Gorbachev A. A. Model, optimizatsiya i otsenka effektivnosti primeneniya mnogoadresnikh setevikh soedinenii v usloviyakh setevoi razvedki [Model, optimization and evaluation of the effectiveness of multicast network connections in the context of network intelligence]. Cybersecurity issues. 2023. vol. 3(55). pp. 13-22. DOI 10.21681/2311-3456-2023-3-13-22 (in Russia).
4. Gorbachev A. A., Maksimov R. V. Problema maskirovaniya i primeneniya tekhnologii mashinnogo obucheniya v kiberprostranstve [The problem of masking and applying machine learning technologies in cyberspace]. Cybersecurity issues. 2023. vol. 5(57). pp. 37–49. DOI 10.21681/2311-3456-2023-5-37-49 (in Russia).
5. Maximov R. V., Sokolovsky S. P., Telenga A. P. Methodology for substantiating the characteristics of false network traffic to simulate information systems // CEUR Workshop Proceedings : BIT 2021 – Selected Papers of 11th International Scientific and Technical Conference on Secure Information Technologies, Moscow. 2021. pp. 115–124.
6. Maximov R. V., Sokolovsky S. P., Telenga A. P. Honeypots network traffic parameters modelling // CEUR Workshop Proceedings : BIT 2021 – Selected Papers of 11th International Scientific and Technical Conference on Secure Information Technologies, Moscow. 2021. pp. 229–239.
7. Sposob (varianti) zashchiti vichislitelnikh setei. Patent № 2307392 C1 Rossiiskaya Federatsiya, MPK G06F 21/00, H04L 9/32. Vigovskii L. S., Zargarov I. A., Kozhevnikov D. A., Maksimov R. V., Pavlovskii A. V.,Starodubtsev Yu. I., Khudainazarov Yu. K., Yurov I. A.; zayavitel i patentoobladatel Voennaya akademiya svyazi (RU). – № 2006114974/09 : zayavl. 02.05.2006: opubl. 27.09.2007 (in Russian).
8. Sposob kontrolya informatsionnikh potokov v tsifrovikh setyakh svyazi. Patent № 2267154 C1 Rossiiskaya Federatsiya, MPK G06F 12/14, G06F 11/00. Andrienko A. A., Kulikov O. E., Kostirev A. L., Maksimov R. V., Pavlovskii A. V., Lebedev A. Yu., Kolbasova G. S.; zayavitel i patentoobladatel Voennaya universitet svyazi (RU). № 2004121529/09. zayavl. 13.07.2004; opubl. 27.12.2005 (in Russian).
9. Melnikova Yu. V., Lazhauninkas Yu. V. Kompyuternoe modelirovanie ekonomicheskikh protsessov s primeneniem metodov fraktalnogo analiza [Computer modeling of economic processes using fractal analysis methods] // Science Krasnoyarsk. 2022. vol. 11. pp. 7–23.
10. Yegorov I. K. Proverka prognozirovaniya poseshcheniya veb-stranits na osnove tsepi Markova dlya modelirovaniya profilya povedeniya polzovatelei / I. K. Yegorov, V. Yu. Radigin // Innovatsionnie mekhanizmi upravleniya tsifrovoi i regionalnoi ekonomikoi : Materiali V Mezhdunarodnoi studencheskoi nauchnoi konferentsii, Moskva, 15–16 iyunya 2023 goda. – Moskva: Natsionalnii issledovatelskii yadernii universitet «MIFI», 2023. – S. 429–437. – EDN ATCIFV.
11. Mikulskii A. Obzor modelei prognozirovaniya [Overview of forecasting models]. Dunărea–Nistru: Anuar, 2019, vol. 6, pp. 284–304 (in Russia).

12. *Khaindman R. Dzh. i Atanasopulos Dzh. Prognozirovanie: printsipi i praktika. [Forecasting: principles and practice]: Melbourne, Australia. 2021 (in Russia).*

13. *Mirzakulova, Sh. A. Issledovanie vremennogo ryada na statsionarnost [Investigation of the time series for stationarity]. Obrazovatelnaya sistema: novatsii v sfere sovremennogo nauchnogo znaniya : sbornik nauchnikh trudov, Kazan, 2019, pp. 318–333 (in Russia).*

14. *Felker M. N., Chesnov V. V. Issledovanie vliyaniya izmeneniya parametrov modeli ARIMA na kachestvo prognoza dlya korotkikh naborov dannikh [Investigation of the effect of changing the parameters of the ARIMA model on the quality of the forecast for short data sets]. Vestnik Yuzhno-Uralskogo gosudarstvennogo universiteta. Seriya: Kompyuternie tekhnologii, upravlenie, radioelektronika, 2021, vol. 3, pp. 36–46 (in Russia).*

15. *Skorobogatikh Y. Y. K voprosu o metodakh nakhozhdeniya otsenok parametrov regressionnikh modelei [On the question of methods for finding estimates of the parameters of regression models] / Y. Y. Skorobogatikh, S. N. Mukhina // Izvestiya Baltiiskoi gosudarstvennoi akademii ribopromislovogo flota: psikhologo-pedagogicheskie nauki. – 2023. – vol. 3(65). pp. 205–212. – DOI 10.46845/519.242071-5331-2023-3-65-205-212.*

РАЗРАБОТКА ПРОГРАММНО-АППАРАТНОГО КОМПЛЕКСА МОДЕЛИРОВАНИЯ МНОГОЗНАЧНЫХ КОМПЬЮТЕРНЫХ АТАК

Шелухин О. И.[1], Раковский Д. И.[2]

DOI: 10.21681/2311-3456-2024-4-116-130

Цель исследования: *разработка и программная реализация экспериментального программно-аппаратный комплекса (ПАК) для сбора телеметрии компьютерных сетей (КС) в условиях проведения многозначных контролируемых компьютерных атак (КА), а также анализ результатов имитационного моделирования многозначных атак, полученных с помощью реализованного комплекса.*

Методы исследования: *имитационное моделирование; машинное обучение; методы многозначного анализа; программная реализация программно-аппаратного комплекса для исследования свойства многозначности классовых меток.*

Объектами исследования *являются теоретические и практические вопросы многозначности классовых меток в сфере информационной безопасности.*

Результаты исследования. *Создан ПАК для сбора телеметрии в ходе имитационного моделирования компьютерных атак в компьютерных системах, обладающих свойством многозначности в табличном представлении. ПАК имитирует реальные данные, соответствующие задачам информационной безопасности. Новизна разработанного ПАК заключается автоматизированной параллельной маркировке всех КА, осуществляемых на КС, что позволяет учесть многозначность уже на этапе сбора данных. С использованием разработанного ПАК, сформирован многозначный набор данных, представляющий собой диагностическую информацию о сети, подвергаемой 3 типам КА, совершаемым параллельно – «Отказ в обслуживании»; «Сетевая разведка»; «Фаззинг». Обнаружено, что многозначная КА (совокупность однозначных КА) является отдельной сущностью с собственным распределением информативной значимости атрибутного пространства. Поскольку многозначная КА является отдельной сущностью, эта сущность может быть выявлена алгоритмами МО с высокой обобщающей способностью, способными к кластеризации. Если алгоритм МО не подразумевает многозначный выход, то даже при правильно выделенном кластере «внутри», отсутствие многозначного выхода приводит к ошибке классификации.*

Научная и практическая значимость. *Описан функционал предлагаемого ПАК для моделирования многозначных КА; формат данных в табличном представлении, собираемых при помощи разработанного ПАК. Данные, порождаемые ПАК, могут быть использованы при разработке средств обнаружения вторжений, учитывающих многозначность классовых меток. Предлагаемый ПАК позволяет исследовать свойство многозначности классовых меток посредством точной настройки соотношения однозначных и многозначных классовых меток за счет конфигуратора КА.*

Ключевые слова: *информационная безопасность, сетевые атаки, многозначная классификация, машинное обучение, имитационное моделирование, набор данных, экспериментальные данные.*

DEVELOPMENT OF A HARDWARE AND SOFTWARE SYSTEM FOR MODELLING MULTI-LABELED COMPUTER ATTACKS

Sheluhin O. I.[3], Rakovskiy D. I.[4]

The aim of the study: *development and software implementation of an experimental hardware-software complex for collecting telemetry of computer networks under conditions of multi-labeled controlled computer attacks, as well as analysis of the results of simulation modelling of multi-labeled attacks obtained with the help of the implemented complex.*

1 Шелухин Олег Иванович, доктор технических наук, профессор Московского технического университет связи и информатики, Москва, Россия. E-mail: sheluhin@mail.ru, ORCID: https://orcid.org/0000-0001-7564-6744

2 Раковский Дмитрий Игоревич, аспирант Московского технического университета связи и информатики, Москва, Россия. E-mail: Prophet_alpha@mail.ru, ORCID: https://orcid.org/0000-0001-7689-4678

3 Oleg I. Sheluhin., Dr.Sc., Full Professor, Moscow Technical University of Communications and Informatics, Moscow, Russia. E-mail: sheluhin@mail.ru, ORCID: https://orcid.org/0000-0001-7564-6744

4 Dmitry I. Rakovskiy, Postgraduate student, Moscow Technical University of Communication and Informatics, Moscow, Russia. E-mail: Prophet_alpha@mail.ru, ORCID: https://orcid.org/0000-0001-7689-4678

Research methods: *simulation modelling; machine learning; methods of multi-value analysis; software implementation of the hardware-software complex for the study of the property of multi-value class labels.*

Research results. *Objects of research are theoretical and practical questions of multi-labeled class labels in the sphere of information security.*

Scientific significance. *A hardware-software complex for telemetry collection in the course of simulation modeling of computer attacks in computer systems with multi-label property in tabular representation is created. hardware-software complex simulates real data corresponding to the tasks of information security. The novelty of the developed hardware-software complex is the automated parallel labeling of all computer attacks carried out on the computer network, which allows to take into account multi-label already at the stage of data collection. Using the developed hardware-software complex, multi-label data set is formed, which is diagnostic information about the network, subjected to 3 types of computer attacks made in parallel – «Denial of Service»; «Network Intelligence»; «Fuzzing». It is found that multi-label computer attack is a separate entity with its own distribution of informative significance of attribute space. Since multi-label computer attack is a separate entity, this entity can be detected by machine learning algorithms with high generalization ability capable of clustering. If the machine learning algorithm does not involve multi-label output, then even with a correctly identified cluster «inside», the lack of multi-label output leads to a classification error.*

Scientific and practical significance. *The functionality of the proposed hardware-software complex for modeling multi-label computer attacks is described; the format of data in tabular representation, collected with the help of the developed hardware-software complex. The data generated by the hardware-software complex can be used in the development of intrusion detection tools that take into account multi-label class labels. The proposed hardware-software complex allows to investigate the multi-label property of class labels by fine-tuning the ratio of single-valued and multi-label class labels through the computer attack configurator.*

Keywords: *Information security, network attacks, multi-label classification, machine learning, simulation modeling, dataset, experimental data.*

Введение

Системы обнаружения вторжений (СОВ), в чьей основе находятся алгоритмы машинного обучения (МО), как правило, требуют объемной выборки «исторических данных», соответствующих защищаемой компьютерной сети (КС) [1–3]. Для корректной работы СОВ, «исторические данные» должны содержать актуальные типы компьютерных атак (КА); реализации каждой КА должны быть разнообразными по своим параметрам[4].

Одной из актуальных особенностей данных, влияющих на качество решения задач классификации и прогнозирования, является многозначность классовых меток[5] [5]. Исследованию свойства многозначности посвящен ряд работ, связанных с медициной, компьютерным зрением, работой с текстом [6,7]. Учет многозначности классовых меток позволяет снизить количество ложноотрицательных и ложноположительных ошибок классификации [8].

Как правило, существующие наборы данных, описывающие поведение КС в момент совершения КА, игнорируют многозначность данных, как, например, UNSW-NB15 [9]. Анализ существующих наборов данных, находящихся в открытом доступе, показал, что многозначные наборы данных, пригодные для решения задач многозначной классификации по ряду вопросов информационной безопасности, либо отсутствуют, либо доля многозначных записей ничтожна, что требует создания специализированного стенда для целенаправленного формирования многозначных данных в контролируемых условиях. Редким исключением является многозначная база данных SR-BH 2020 [10].

Редкость баз данных, содержащих многозначные КА, находящихся в открытом доступе, актуальной является разработка и реализация программно-аппаратного комплекса (ПАК) для сбора телеметрии и имитационного моделирования многозначных КА. Важным условием функционирования ПАК является проведение каждой КА в контролируемых условиях.

Анализ существующих решений в сфере ИБ [11] (а также см.[6]) выявил уникальность предлагаемого решения: не существует программных или программно-аппаратных решений, находящихся в открытом доступе, направленных на исследование свойства многозначности в данных.

Целью работы является разработка и программная реализация экспериментального ПАК для сбора телеметрии КС в условиях проведения многозначных контролируемых КА, а также анализ результатов имитационного моделирования многозначных атак, полученных с помощью реализованного комплекса.

Структурная схема функционирования ПАК

Формализуем механизм работы ПАК для сбора телеметрии и имитационного моделирования

5 Gibaja E., Ventura S. A Tutorial on Multilabel Learning // ACM Comput. Surv. 2015. Т. 47, № 3. С. 1–38с. DOI: 10.1145/2716262

6 Д. И. Котенко, И. В. Котенко, И. Б. Саенко, Методы и средства моделирования атак в больших компьютерных сетях: состояние проблемы, Тр. СПИИРАН, 2012, выпуск 22, 5–30

многозначных КА. Зададим топологию T исследуемой КС в виде двух множеств хостов:

$$T = \{VH_i;\ i = \overline{1,I}\} \cup \{AH_j;\ j = \overline{1,J}\} \cup DAS \cup Router, \quad (1)$$

где VH_i – i-й хост, имитирующий жертву (далее – атакуемый хост, от англ. *Victim host*); AH_j – j-й хост, имитирующий машину злоумышленника (далее – атакующий хост, от англ. *Attack host*), проводящую контролируемую КА на VH_i; DAS – сервер агрегации данных (англ. *data aggregation server*), аккумулирующий телеметрию с VH_i и AH_j, а также содержащий конфигуратор КА; $Router$ – маршрутизатор (группа маршрутизаторов, или фрагмент сети Интернет), соединяющий множество атакуемых и атакующих хостов.

В контексте разработки ПАК уместно говорить о проведении контролируемых компьютерных атак (ККА), чье проведение полностью прогнозируемо на этапе планирования и контролируется в течение хода эксперимента. Введем в рассмотрение перечень ККА AL, которые атакующие хосты AH_j способны реализовать на атакуемые хосты VH_i:

$$AL = \{attackk;\ k = \overline{1,K}\}. \quad (2)$$

Каждая КА описывается рядом статичных $attack_k$ и варьируемых $vattack_k$ параметров – AoI_k:$attack_k \cup vattack_k$. Статичные параметры $attack\_k$: $\langle params_{l_k}\rangle$; $pl_k = \overline{1,PL_k}$ являются общими для каждой реализации КА. Общее число параметров атаки PL_k и их содержательное наполнение варьируется в зависимости от специфики КА[7].

Введем варьируемые параметры АК, которые могут изменяться в рамках конкретной реализации – AoI_k (англ. *Attack on Interval*). Такие параметры задаются либо фиксированными числами, либо законами распределения, выбираемыми из библиотеки распределений $FL = \{F_{lf}(\alpha_p);\ p = \overline{1,P_{lf}},\ lf = \overline{1,LenF}\}$, где α_p – p-й параметр lf-го закона распределения:

$$AoI_k\langle IS,IE,attack_k,ah,tar,dur,int,etcp\rangle, \quad (3)$$

где IS – параметр, точное время начала интервала атаки; IE – параметр, точное время окончания интервала атаки; ah – атакующий хост, реализующий экземпляр атаки в пределах указанных интервалов; tar – множество целей атаки для dur – длительность атаки в пределах указанных интервалов; int – интенсивность атаки в пределах указанных интервалов; $etcp$ – множество иных варьирующихся параметров.

Конкретное множество параметров $etcp$ детализируется в зависимости от механизма реализации КА. Общее число параметров атаки – Lk – варьируется в зависимости от требуемой детализации. Значения параметров обусловлено механизмом реализации атаки, сложностью ее исполнения, используемыми протоколами, приложениями, устройствами.

При практической реализации сборщика, необходимо учесть условия функционирования анализируемой КС. Поскольку анализируемая КС является целью проведения КА, в ней допускается нарушение целостности, доступности и конфиденциальности информации, а также деструктивное воздействие на поддерживающую инфраструктуру T.

При превышении некоторого критического порога деструктивного воздействия на систему КС выходит из строя и сбор телеметрии с нее становится невозможным. Для предотвращения уничтожения КС в следствие фатального воздействия КА, предусмотрен механизм оценки максимально допустимого негативного воздействия на КС i-й атакуемый хост VH_i – $MaxDamage_{VH_i}$ – со стороны атакующих хостов. Под $MaxDamage_{VH_i}$ будем понимать максимально допустимое время ответа i-го атакуемого хоста VH_i на синхронизирующий сигнал, поступающий с сервера агрегации данных DAS.

Взаимодействие между элементами КС DAS, VH_i и AH_j (4) осуществляется через программные агенты 1-го и 2-го типов, распространяемые на соответствующие хосты: $PA = \{prograg_{1,i};\ i = \overline{1,I}\} \cup \{prograg_{2,j};\ j = \overline{1,J}\}$.

Программные агенты обоих типов связаны с сервером агрегации данных DAS. Программные агенты 1-го типа $prograg_{1,i}$ осуществляют сбор телеметрической информации с атакуемых хостов VH_i и их передачу на DAS. Программные агенты 2-го типа – $prograg_{2,j}$ – осуществляют сбор телеметрической информации с атакующих хостов AH_j и реализуют КА, связанные с AH_j, согласно управляющим командам, поступающим с DAS.

Так как технические показатели хостов топологии T (2) могут отличаться, то выбрать одинаковую частоту сбора телеметрической информации для все хостов не представляется возможным. Неверный выбор частоты сбора телеметрической информации может повлечь за собой излишнюю нагрузку на вычислительные мощности атакуемых хостов, что критично при проведении ККА из-за угрозы превышения максимально допустимого времени ответа i-того атакуемого хоста VH_i – $MaxDamage_{VH_i}$.

Одним из способов вычисления допустимой частоты сбора телеметрической информации является запуск нагрузочного тестирования на каждом VH_i и вычисление среднего времени, необходимого для обработки одной итерации сбора телеметрии.

На этапе проведения ККА, в момент реализации атаки, с помощью датчика псевдослучайных чисел

7 CAPEC – Common Attack Pattern Enumeration and Classification (CAPECTM) [Электронный ресурс]. URL: https://capec.mitre.org/index.html (дата обращения: 12.09.2023).

RND формируется закон распределения $F_{params_{lk}}$ с выбранными параметрами реализации атаки внутри каждого интервала $IS - IE$. В случае необходимости полного контроля за осуществлением ККА параметры распределения заменяются фиксированными числами.

Взаимодействие между атакующими хостами AH_j и хостами-жертвами VH_i, описывается вектором:

$$AoI_k: \vec{V}_k = (AoI_{kw}; w = \overline{1,W_k}), \quad (4)$$

где W_k – количество случаев, когда k-я КА $attack_k$ реализуется в течение эксперимента.

В рамках топологии (1) результате воздействия атакующими хостами AH_j на хосты-жертвы VH_i компьютерными атаками (2) с параметрами (3), объединенными в вектора (4), формируется нагрузка на атакуемые хосты, считываемая программными агентами 1-го типа и отравляемая на сервер агрегации данных.

Конфигурация воздействия по каждой КА (расписание КА) может быть представлена в виде итогового множества CoA (англ. *Chronology of Attacks*):

$$CoA = (\vec{V}_k; k = \overline{1,K}). \quad (5)$$

Визуализация формализованного выше приведенными соотношениями механизма работы стенда, представлена на рис. 1.

Топология T для исследуемой КС отражена путем визуализации в виде двух контролируемых зон – зоны атакуемых VH_i и атакующих AH_j хостов. Зоны VH_i и AH_j, в свою очередь, разделены неконтролируемой зоной, имитирующей сеть Интернет и содержащей маршрутизатор *Router*.

На каждом из VH_i установлен программный агент первого типа $prograg_{1,i}$. На каждом из хостов AH_j установлен программный агент второго типа $prograg_{2,j}$. На сервере агрегации данных DAS расположена база данных для агрегируемый телеметрических данных с AH_j и VH_i. DAS предназначен для контроля взаимодействия между программными агентами. Маршрутизатор сети является связующим звеном между всеми хостами VH_i и AH_j.

Программные агенты второго типа – $prograg_{2,j}$ – распространяются на атакующие хосты AH_j; их задачами является:

- Взаимодействие с DAS с целью получения расписания ККА;
- Проведение ККА согласно полученному расписанию;
- Отправка на DAS информации об успешном старте и остановке проведения ККА согласно полученному расписанию;
- Обмен диагностической информацией с DAS.

Для реализации КА сервер агрегации данных DAS посылает управляющие сигналы на атакующие хосты. Реализация каждой КА на атакующем хосте выполняется в виде вызываемого docker-контейнера, содержащего предустановленное программное

$$T = \left\{VH_i; i = \overline{1,I}\right\} \cup \left\{AH_j; j = \overline{1,J}\right\} \cup DAS \cup Router$$

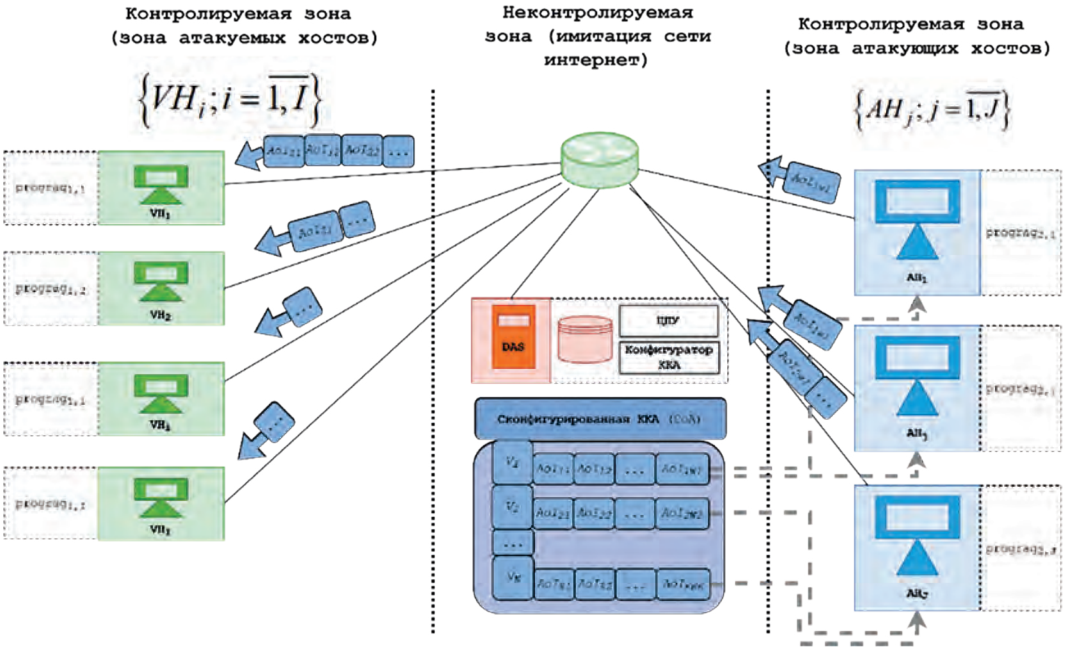


Рис. 1. Структурная и схема функционирования ПАК

обеспечение и скрипты для выполнения КА. Управление ходом КА (ее прекращение или повторение заданное количество раз) осуществляется программным агентом $prograg_{2,j}$.

В качестве иллюстрации на рис. 1, приведены несколько элементов CoA, направленных на различные атакуемые хосты (детализация дана для хостов VH_1, VH_2). На хост VH_1 направлены атаки двух типов: две реализации атаки AoI_{11}, AoI_{12}, и реализация атаки AoI_{22}. На хост VH_2 направлена реализация атаки AoI_{22}. Полная информация о сконфигурированных компьютерных атаках – CoA – доступна на DAS, в конфигураторе ККА. Детализация данного узла раскрывается в соответствующем разделе.

Данные телеметрии собираются программными агентами на DAS. Здесь же производится маркировка и последующая аккумуляция данных, поступающих с программных агентов. При необходимости из сформированной базы данных осуществляется выгрузка дампов в пригодном для последующего анализа выбранными алгоритмами МО.

Сценарий использования разработанного ПАК, при известном перечне КА $AL = \{attack_k;\ k = \overline{1,K}\}$ и их статичных параметрах $\langle params_{l_k}\rangle$, включает:

1) настройку взаимодействия атакуемых хостов VH_i между собой в рамках эксперимента (определение роли каждого хоста в рамках моделируемого бизнес-процесса; актуализация программного обеспечения; сетевой топологии на хостах и на $Router$);
2) развертывание подсети атакующих хостов AH_j;
3) создание «расписания КА»: задание векторов AoI_k по каждой из K КА при помощи разработанного конфигуратора КА;
4) инициализацию эксперимента: запуск программных агентов 1-го и 2-го типов для сбора данных; проверка корректности их взаимодействия с DAS; запуск стороннего программного обеспечения для сбора дополнительной телеметрии (при необходимости) на VH_i;
5) проведение эксперимента: КА реализуются атакующими хостами AH_j согласно управляющим командам, посылаемым с DAS на программные агенты 2-го типа;
6) завершение эксперимента и формирование выходных данных.

После завершения эксперимента, ПАК формирует многозначный набор данных, содержащий диагностическую информацию о сети, подвергаемой КА из перечня $AL = \{attack_k;\ k = \overline{1,K}\}$ согласно п. 3 сценария. ПАК включает в себя ряд скриптов, написанных на языке python, позволяющих объединить диагностическую информацию, собранную с программных агентов и сторонних сборщиков телеметрии: *Wireshark, MSI Afterburner, Windows Perfmon*.

Особенности имитационного моделирования многозначных КА в ПАК

Для тонкой настройки проведения серии ККА с различными параметрами на атакуемые хосты VH_i, в ПАК реализован конфигуратор ККА, содержащий библиотеку статичных параметров $params_{l_k}$; библиотеку распределений случайных величин $F_l(\alpha_p)$, используемых при формировании варьируемых параметров AoI_k во время проведения эксперимента; функционал планировщика ККА и связанного с ним расписания проведения ККА.

Конфигуратор ККА необходим для планирования и автоматизации объемных во времени экспериментов. Он позволяет задать точное время начала и конца каждой ККА из перечня доступных для реализации. Визуализация конфигуратора ККА приведена на рис. 2.

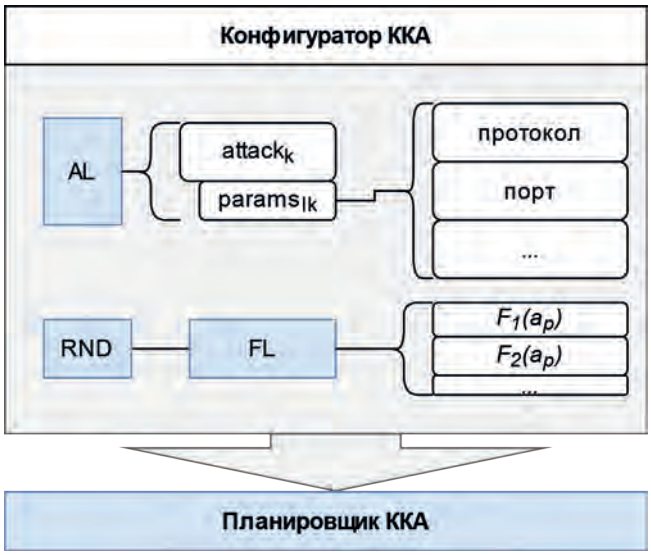


Рис. 2. Визуализация конфигуратора ККА

Согласно (2) .... (4), КА каждого типа характеризуется ее параметрами $params_{l_k}$, общими для каждой отдельной реализации такой атаки, и рядом варьируемых параметров AoI_k:$\langle IS,IE,attack_k,ah,tar,dur,int,etcp\rangle$, уникальных для каждой реализации КА.

Набор параметров $params_{l_k}$ задается перед началом эксперимента и в дальнейшем не меняется. Содержимое $params_{l_k}$, как правило, уникален для каждого типа КА и прописывается в bash-скриптах, находящихся в вызываемых контейнерах *Docker*, реализующих механизм указанной атаки.

Содержимое AoI_k задается либо константами, либо законами распределения – $F_l(\alpha_p)$. Формирование случайных величин в соответствии с $F_l(\alpha_p)$ происходит с помощью генератора псевдослучайных чисел по законам распределения из библиотеки распределений FL.

Планировщик ККА является важным элементом конфигуратора ККА. Временная диаграмма, иллюстрирующая работу планировщика ККА, приведенная на рис. 3, позволяет наглядно визуализировать многозначные классовые метки [12]. Каждая реализация атаки задается параметрами – AoI_k (5). Для задания итогового множества CoA (5), необходимо воспользоваться планировщиком ККА. На рисунке 3, по оси абсцисс отложено время эксперимента, в рамках которого осуществляются ККА. В качестве иллюстрации перечня возможных КА, отложенных на оси ординат, выбраны атаки из базы данных *CAPEC* [13]:

- две атаки типа «отказ в обслуживании», направленные на один хост исследуемой сетевой топологии (*CAPEC-125: Flooding*) – DoS_{p1} и DoS_{p2};
- атака типа «сканирование портов» (*CAPEC-300: Port Scanning*);
- атака типа Scanning for Vulnerable Software (*CAPEC-310: Scanning for Vulnerable Software*).

Поскольку реализуется несколько КА типа «отказ в обслуживании», направленных на хост исследуемой системы, в моменты одновременной реализации данных атак справедливо говорить об атаке типа «массовый отказ в обслуживании».

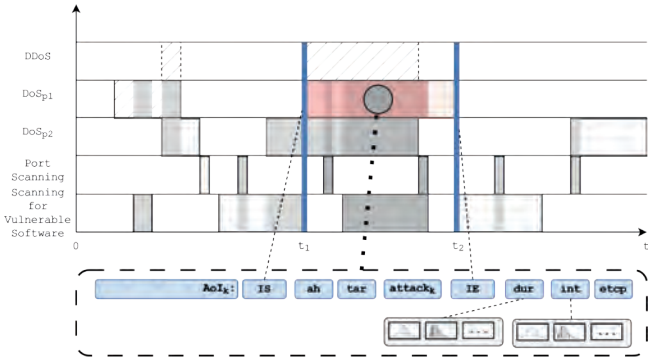


Рис.3. Временная диаграмма визуализации работы механизма планирования ККА

Диаграмма содержит прямоугольные области, отмечающие точное время начала и окончания интервала каждой компьютерной атаки. В рамках каждого интервала задаются параметры КА. В качестве иллюстрации, приведена детализация параметров КА типа «отказ в обслуживании». В пределах каждого интервала определены варьируемые параметры AoI_k:⟨IS,IE,$attack_k$,ah,tar,dur,int,$etcp$⟩. Ряд метрических параметров (таких, как dur и int) может быть задан как константой, так и законом распределения из библиотеки *FL*.

Многозначность собираемых данных проиллюстрируем на конкретном примере. Для этого рассмотрим визуализацию расписания ККА. *Визуализация расписания ККА* необходима для облегчения планирования ККА человеком и контроля за долей многозначных КА в формируемом наборе данных. Пример визуализации расписания ККА для одного атакуемого хоста приведен в табл. 1. Каждые сутки в таблице представлены 24 ячейками, маркированными от «00:00» – полуночи до «23:00» – одиннадцати часов вечера. Интервал времени – час. В каждый из интервалов времени может быть реализована одна или несколько КА (в визуализации – 6 типов). Параметры каждой КА (в том числе и атакующий хост, IP-адрес атакуемого хоста, интенсивность КА и т.д.) задаются в конфигураторе КА; на представленной визуализации данная информация опускается для большей наглядности.

В таблице присутствует цветовое разделение, выполненное в виде градаций серого цвета:

- Белым цветом отмечены интервалы, когда КА определенного типа не реализуется.
- Светло-серым цветом отмечены интервалы, когда КА реализуется и при этом кроме данной КА

Таблица 1.

Пример расписания КА для одного атакуемого хоста

Дата	Время, ч	Атака №1	Атака №2	Атака №3	Атака №4	Атака №5	Атака №6
22.04.2024	0:00						
	1:00						
	2:00						
	3:00						
	4:00						
	5:00						
	6:00						
	7:00						
	8:00						
	9:00						
	10:00						
	11:00						

в данном интервале ни одна другая КА не реализуется (однозначные КА);

- Темно-серым цветом отмечены интервалы, когда КА реализуется и при этом реализуется иная КА – наблюдается многозначная КА.

Примерами интервалов времени, когда наблюдаются многозначные КА, являются:

- 22.04.2024; 0:00 – 2:00 (КА №1 и №4);
- 22.04.2024; 2:00 – 5:00 (КА №1, №2 и №4);
- 22.04.2024; 7:00 – 8:00 (КА №1, №2, №3);
- и иные.

Поскольку в моменты производится воздействие сразу нескольких КА с разными параметрами на один атакуемый хост VH_i, их совокупное *синергетическое* воздействие может приводить к фатальным последствиям для последнего [14]. В результате такого воздействия, происходит одновременное «наложение» реализаций атак (как это также отмечено на рис. 3; интенсивность цвета отражает количество одновременно воздействующих КА). Представленная многозначность данных наблюдается в реальных компьютерных системах [8,15].

Результатом работы ПАК является сформированная многозначная база данных КА, предназначенная для исследования специфического явления – многозначности классовых меток компьютерных атак.

Конфигуратор ККА допускает настройку стенда на однозначный–бинарный или многоклассовый режимы работы. Для реализации бинарного режима работы стенда вида «нормальное состояние КС – реализация конкретной атаки» в конфигураторе необходимо выбрать один тип атаки, после чего настроить интервалы ее реализации.

Для реализации многоклассового режима работы ПАК в конфигураторе предусмотрено разграничение интервалов начала и окончания атак каждого типа строго без показанных выше пересечений по времени.

Отметим, что при планировании эксперимента с помощью ПАК, рекомендуется ориентироваться на эксплуатационные характеристики телекоммуникационного оборудования, используемого для имитации сети Интернет (узел *Router* в топологии T). При выходе из строя узла, связывающего подсеть атакующих хостов и атакуемых хостов, ряд запланированных в расписании ККА производится не будет до устранения неисправности на маршрутизаторе. Во избежание потери данных, в ПАК предусмотрено резервирование данных на каждом хосте, на котором располагаются программные агенты. В случае выхода из строя узла (ряда узлов) сети ПАК, возможно восстановление данных из резервных копий.

Анализ многозначных данных, формируемых ПАК

Для решения задач классификации, прогнозирования и исследования многозначных данных в ПАК программно реализован новый исследовательский фреймворк (ИФ). Фреймворк представляет собой шаблон, облегчающий сравнение алгоритмов МО между собой в задачах прогнозирования и классификации. Архитектура разработанного исследовательского фреймворка (ИФ), реализованна на Python версии 3.10, с применением следующих открытых библиотек: *pandas, seaborn, matplotlib, time, numpy, sklearn, keras, tensorflow*. Предусмотрено сравнение алгоритмов МО в задачах бинарной, однозначной и многозначной классификаций.

Процесс проведения исследования можно разделить на **два этапа**:

Этап 1 *– исследование и предобработка исходных экспериментальных данных;*

Этап 2 *– проведение эксперимента классификации.*

Этап 1. Процесс исследования свойств экспериментальных данных начинается с задания исходных параметров предобработки ЭД табличного типа. В качестве входных данных на ИФ подается:

- Переменная, отвечающая за тип классификации: бинарная, многоклассовая, многозначная.
- Логическая переменная, отвечающая за необходимость предварительного перемешивания данных.
- Логическая переменная, отвечающая за необходимость трансформации атрибутов ЭД.
- Логическая переменная, отвечающая за необходимость формирования ROC-кривых.
- Логическая переменная, отвечающая за метод построения ROC-кривой: «Один против одного» (One-vs-one, OVO) или «один против всех» (One-vs-everyone, OVE или One-vs-rest – OVR).
- Наименование эксперимента. В наименование эксперимента обязательно включается информация обо всех логических переменных, содержащихся в исходных данных.
- Количество блоков разделения ЭД в режиме перекрестной проверки (кросс-валидации) по нотации *K-Fold*. По умолчанию используется «классическая» кросс-валидация с разделением исходных ЭД на два блока: блок обучающих данных и блок тестовой выборки.
- Массив, содержащий в себе наименование всех вторичных атрибутов, исследуемых ЭД.
- Переменная, отвечающая за тип эксперимента, проводимого на этапе 2.
- Набор переменных для оптимизации вычислений: логическая переменная, отвечающая за необходимость пропуска этапа 1 в случае наличия

заранее обработанной информации; переменная, ограничивающая количество циклов, выполняемых на этапе 2 и так далее.

Визуализация этого этапа приведена на рис. 4.

Этап 1 состоит из пяти *шагов*, на каждом из которых происходит обработка данных и формирование сопутствующих выкладок: таблиц, графиков, диаграмм, текстовой информации и прочего. Рассмотрим данные шаги более подробно.

Шаг 1. Получение первичных данных и разведочный анализ. Первичные данные выгружаются в ИФ из таблицы формата .csv (*пункт (1) на схеме рис. 4*), после чего выполняется их разведочный анализ.

Разведочный анализ данных представляет собой анализ ЭД по каждому атрибуту $A_m = \{a_{mn};\ m = \overline{1,M},\ n = \overline{1,N}\}$ по следующим показателям: количество записей (count): $count_{A_m} = |A_m| = N$; Среднее (mean): $mean_{A_m} = \bar{A}_m$; Среднее квадратическое отклонение (*corrected sample standard deviation* (в нотации библиотеки pandas – *sample standard deviation*, STD) – $STD_{A_m} = \sqrt{\frac{1}{N-1}\sum_{n=1}^{N}(a_{mn} - \bar{A}_m)^2}$; минимальное значение атрибута (min): $min_{A_m} = minA_m$; максимальное значение атрибута (max) $max_{A_m} = maxA_m$; нижний, 50%-й и верхний процентили (percentile, P). Результаты разведочного анализа маркированы *пунктом (2) на схеме рис. 4*.

Дополнительно оценивается количество уникальных значений у атрибута: $\mu_m{:}A_m \longrightarrow N \cup \{0\}$, где – множество натуральных чисел с включением нуля. Также оценивается количество некорректных (NaN, пропусков) значений атрибута. Результат разведочного анализа сводится в таблицу и сохраняется. Этому пункту соответствует таблица с обозначенными результатами анализа (*пункт (3) на схеме рис. 4*). Дополнительно выполняется частотный анализ целевого столбца, данные выводятся в отдельную таблицу и сохраняются для последующей визуализации.

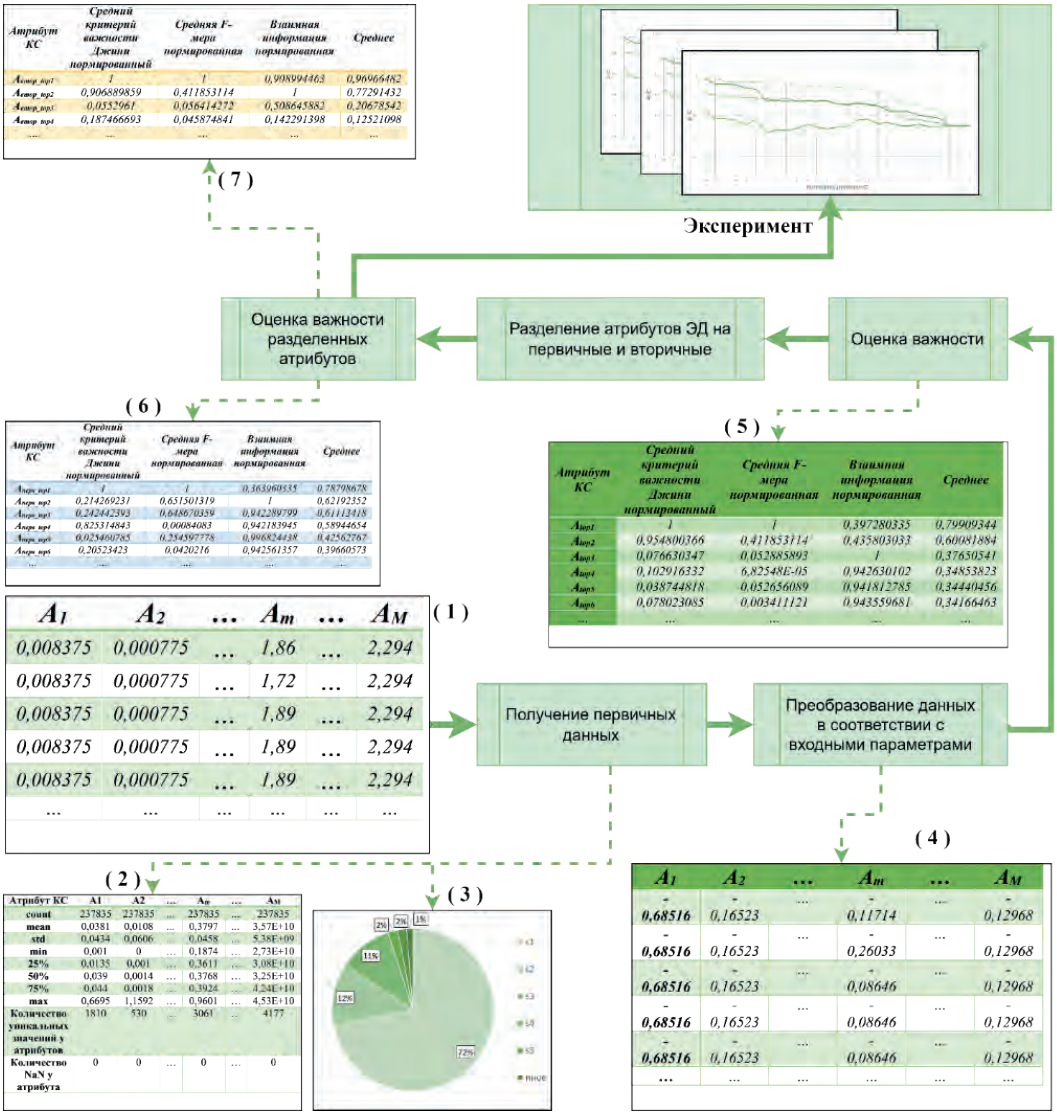


Рис.4. Архитектура ИФ. Этап предобработки данных

Шаг 2. Преобразование данных в соответствии с входными параметрами. На данном шаге ЭД анализируются по критерию «количество уникальных значений атрибута». Если «количество уникальных значений атрибута» равно единице – атрибут исключается из дальнейшего анализа.

Если логическая переменная, отвечающая за необходимость предварительного перемешивания данных равна истине – то данные перемешиваются в режиме «группировка по одной записи». Для сохранения возможности повторного проведения эксперимента начальное значение генератора случайных чисел всегда ставится равной определенной константе.

Если логическая переменная, отвечающая за необходимость трансформации атрибутов ЭД, равна «истине» – то проводится нормализация и стандартизация атрибутов посредством удаления среднего значения и масштабирования всех атрибутов до единичной дисперсии [16]. Кроме изложенного на данном шаге, выполняется кодирование категориальных меток классов под стандарты классификаторов scikit-learn. Категориальные атрибуты кодируются своими порядковыми номерами, например, «а» соответствует «1»; «б» соответствует «2» и так далее. Порядковый номер присваивается в порядке первого вхождения метки класса в ЭД. Отметим, что перекодирование никак не влияет на итоговые результаты классификации. Результатом выполнения данного шага является таблица трансформированных данных (*пункт (4) на схеме рис. 4*).

Шаг 3. Оценка важности атрибутов ЭД. На данном шаге выполняется оценка важности атрибутов ЭД по разным критериям. В реализованном ИФ реализованы три упомянутых метрики на базе библиотеки scikit-learn. Статистический критерий важности атрибутов вычисляется на основании p-value, взаимной информации. В критерии важности, вычисленные на основании *p-value*, включена *F-мера*, вычисленная между метками класса и значениями атрибутов посредством дисперсионного анализа (*ANalysis Of VAriance, ANOVA*). Реализован также способ вычисления F-меры, вычисленной между метками класса и значениями атрибутов методами регрессионных тестов.

Каждая из вышеприведенных оценок может быть вычислена различными мета-методами. Отметим, что для задач вывода важности всех атрибутов и их последующего отбора, не обязательно использовать все перечисленные мета-методы, поскольку сами по себе они не влияют на результаты оценки, а влияют лишь на способ отбора по существующим оценкам. Выбор мета-методов должен быть определен исследователем в контексте решаемой им задачи.

SelectKBest – метод формирования оценки и отбора k лучших атрибутов по определенной метрике: $Kfold_{sort(A,PARAM)} = \{A_{top1}, At_{op2}, ..., A_{topK} \mid K \le M\}$, где $sort(\boldsymbol{A}, PARAM)$ – функция сортировки по убыванию набора атрибутов $\boldsymbol{A}$ по некоторому критерию (оценке, параметру) – $PARAM$ – возвращающая набор атрибутов, K – параметр метода; A_{top1} – атрибут, имеющий наивысшую оценку среди всех атрибутов; At_{op2} – атрибут, ранжированный на второе место – и так далее. Метод SelectKBest, как следует из его названия, отбирает K атрибутов КС, имеющих наибольшую важность.

SelectPercentile – метод формирования оценки и отбора атрибутов по наивысшему перцентилю по определенной метрике

$$Kpercentile_{sort(A,PARAM)} = \\ = \{A\_topk \mid k = \overline{1,\lceil M \times 0.01 \times K \rceil}; K \le 100\}.$$

SelectFpr – метод формирования оценки и отбора атрибутов по наименьшему количеству ошибок (выражается через p-значение, α) первого рода по определенной метрике:

$$SelectFPR_{sort(A,PARAM),\alpha} = \{\forall A_k \mid pvalue\ A_k \le \alpha\}.$$

SelectFdr – метод формирования оценки и отбора атрибутов по наименьшему количеству ошибок второго рода, вычисляемая из p-value по определенной метрике:

$$SelectFDR_{sort(A,PARAM)} = \{\forall A_k \mid pvalue\ A_k \in BHP\},$$

где BHP – процедура Бенджамина-Хохберг (*Benjamini-Hochberg procedure*)[8].

SelectFwe – метод формирования оценки и отбора атрибутов по частоте ошибок по семействам (*Family-wise error rate*, FWE) по определенной метрике:

$$SelectFWER_{sort(A,PARAM),\alpha} = \{\forall A_k \mid 1 - FP_{TP=0} \le \alpha\}.$$

В случае необходимости выбора нескольких мета-алгоритмов оценки атрибутов по важности, в разработанном ИФ предусмотрена функция усреднения по группе. В каждой группе (Джини, p-value, взаимная информация) метрики, полученные при помощи перечисленных выше мета-методов, усреднялись и нормировались по трем группам. Результаты оценки значимости атрибутов визуализированы в виде таблицы, *пункт (5) на схеме рис. 4*.

Шаг 5. Разделение атрибутов ЭД на первичные и вторичные. На данном этапе в соответствии с входными параметрами происходит разделение атрибутов ЭД на первичные и вторичные. Первичные

8 Benjamini Y., Hochberg Y. Controlling the False Discovery Rate: A Practical and Powerful Approach to Multiple Testing // Journal of the Royal Statistical Society Series B: Statistical Methodology. 1995. Т. 57, № 1. С. 289–300. DOI: 10.1111/j.2517-6161.1995.tb02031.x

и вторичные атрибуты КС сохраняются в отдельные таблицы.

Шаг 6. Оценка важности разделенных атрибутов. Полученные наборы данных еще раз оцениваются по важности по указанным на шаге 3 критериям, внутри своих групп (*пункты (6) и (7) на схеме рис. 4*).

После предобработки ЭД, оценки важности их атрибутов, первичные атрибуты ЭД, повторно оцененные по важности внутри своей группы и подаются на вход Этапа 2.

Этап 2. На этапе 2 оцениваются результаты решения задачи классификации или прогнозирования. Предусмотрена «классическая» перекрестная проверка с разделением сходных ЭД на два блока: блок обучающих данных и блок тестовой выборки. Каждый шаг перекрёстной проверки разбивает исходные ЭД на несколько блоков равного объема; при этом один блок является тестовой выборкой ЭД, а остальные – обучающей.

Визуализация этого этапа приведена на рис. 5. Для корректной работы алгоритма атрибуты исходных экспериментальных данных оцениваются по информативности (*пункт (1) на схеме рис. 5*).

В ИФ реализована перекрестная проверка только по нотации *K-Fold* с разделением только на обучающую и тестовую выборки (без валидационной выборки). Метрики включают в себя как метрики оценки качества среднего по множеству классов (так называемые макро-метрики), так и метрики оценки качества на основе множества записей (микро-метрики). В дополнение к вычислению известных бинарных оценочных метрик на основе количества истинно положительных результатов (*TP*) истинно отрицательных результатов (*TN*), ложноположительных результатов (*FP*) и ложноотрицательных результатов (*FN*) вычисляется *accuracy*, *precision*, *recall f-мера*, *ROC* и связанная с ней *AUC*.

По окончанию цикла перекрестной проверки, из ЭД удаляется первичный атрибут в соответствии с некоторым условием. Условие может быть «максимальная важность» и «минимальная важность». После удаления одного из атрибутов циклы повторяются заново. Как только все атрибуты окажутся удаленными – ИФ завершит свою работу, породив таблицы итоговых результатов: детализированная таблица экспериментов по каждому блоку перекрестной проверки (*пункт (2) на схеме рис. 5*) и обобщенная (усредненная) таблица итогов проведенного эксперимента (*пункты (3) и (4) на схеме рис. 5*).

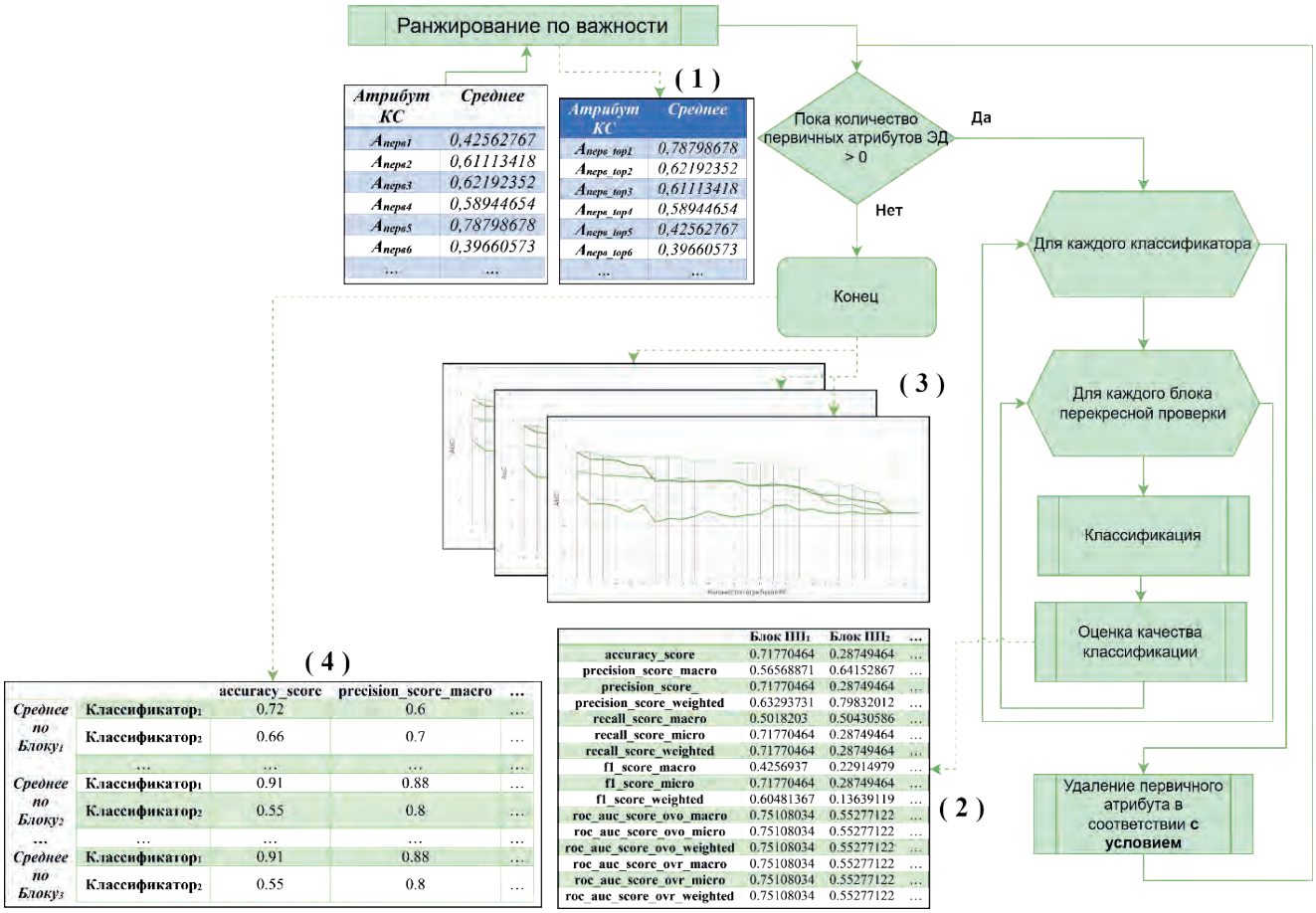


Рис. 5. Архитектура фреймворка. Этап проведения эксперимента

Исследование влияния сокращения атрибутной размерности на эффективность классификации по нескольким метрикам способствует решению следующих задач, сопряженных с анализируемым набором ЭД:

1. Сравнение разных методов классификации ЭД: бинарный, многоклассовый, многозначный.
2. Оценка степени влияния проблемы классового дисбаланса в частотной и временной областях на результаты классификации при различных подходах к предобработке исходных ЭД.
3. Оценка степени влияния проблемы атрибутной размерности («проклятие размерности»
4. Экспериментальная проверка влияния важных (незначительных) атрибутов ЭД на результаты классификации.
5. Сравнить результаты классификации на различных наборах ЭД.
6. Сравнение классификаторов, основанных на различных подходах, принципах и математических аппаратах, при различной атрибутной размерности.
7. Проверка эмпирической гипотезы о монотонности функции зависимости убывания эффективности классификации целевого столбца по какой-либо метрике.

Основными недостатками разработанного ИФ являются:

1) Зависимость времени исследования ЭД от реализаций алгоритмов в открытых библиотеках *pandas*, *seaborn*, *matplotlib*, *time*, *numpy*, *sklearn*.
2) Отсутствие графического интерфейса ИФ (работа с ИФ предполагает работу с программным кодом).

Результаты проведенного эксперимента с использованием предложенного ПАК

Количество записей экспериментальных данных в итоговом наборе составлял 263.388 шт. Набор данных содержал 125 атрибутов метрического типа и был разделен на 3 категории: аппаратные атрибуты атакуемого хоста; атрибуты, связанные с сетевым взаимодействием; атрибуты, извлеченные из системных журналов операционной системы Windows. Информация, собранная с сетевой карты и системных журналов, преобразовывалась в метрические атрибуты посредством вычисления количественных характеристик (средняя длина пакета; количество уникальных событий; количество уникальных сессий и т.д.) в рамках окна размером 1 секунда.

Проведённый анализ атрибутного пространства выявил, что атрибутами с наибольшим количеством уникальных значений являются атрибуты, извлеченные из журналов ОС *Windows*, а также атрибуты, связанные мониторингом функционирования видеокарты. Расписание проведения ККА сконфигурировано таким образом, чтобы часть атак различных категорий происходила одновременною. Реализация нескольких ККА одновременно в соответствии с расписанием позволил собрать многозначные данные.

Распределение атак с каждого атакующего хоста приведено на рис. 6.а. Распределение атак каждого типа приведено на рис 6.б. Подсчет классовых меток для построения частотной статистики в рамках указанных распределений выполнялся независимо. В случае формирования статистики по каждому атакующему хосту, классовые метки подсчитывались по каждому хосту (AH_1 … AH_5). В случае формирования статистики по каждому типу КА – подсчитывались по каждому типу КА («Отказ в обслуживании»; «Сетевая разведка»; «Фаззинг»).

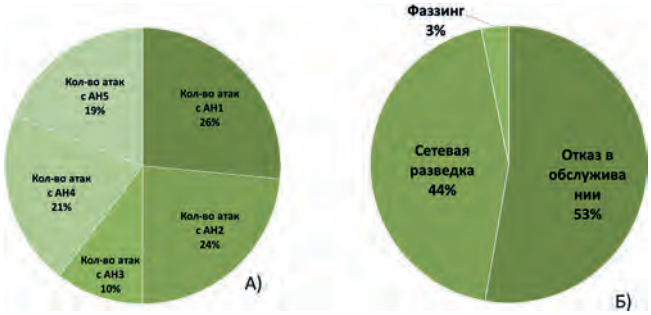


Рис.6. Распределение КА:
а) – с каждого атакующего хоста; б) –каждого типа.

Всего совокупно с каждого хоста было собрано 488 120 ед. записей о проведении КА. Отметим, что суммарное количество классовых меток превышает объем собранных данных вследствие наличия многозначности в данных. Дополнительно отметим также, что из-за независимого подсчета частотной статистики для распределения атак с **каждого атакующего хоста** и распределение атак каждого **типа**, вследствие различной размерности пространства классовых меток и **наличия многозначных записей**, суммарный объем классовых меток различается. Различия связаны с одновременно реализуемыми КА одного типа по разным хостам.

На рис. 7.а приведено распределение классовых меток **по количеству хостов**, одновременно участвующих в КА, а на рис. 7.б распределение классовых меток по каждому **типу** КА, одновременно участвующих в атаке на VH_1. В отличии от рис. 6, классовые метки подсчитывались по каждому хосту (AH_1 … AH_5).

Количество классовых меток, связанных с отсутствием КА, составляет. 20% от общего количества классовых меток (51605 ед).

Анализ гистограмм, характеризующих информационную значимость атрибутов КС, показал, что для некоторых атрибутов многозначной КА их значимость

Рис. 7. Распределение классовых меток:
а) По одновременно задействованным хостам при реализации КА;
б) По одновременно совершаемым типам КА.

превышает информационную значимость однозначных КА, входящих в ее состав. Обнаружено, что многозначная КА (совокупность однозначных КА) является отдельной сущностью, обладающей собственным распределением информативной значимости атрибутного пространства.

Оценим и сравненим информативность атрибутов, собранных в результате эксперимента с использованием ПАК. Оценка значимости атрибутного пространства производилась с использованием библиотеки scikit-learn; модуля SelectKBest. Анализ доступных функций определил наиболее подходящую для решения поставленной задачи – chi2. Дополнительно для оценки информативности атрибутов использовался индекс Джини, вычисляемый с использованием реализации алгоритма Random Forest (RF) библиотекой scikit-learn

На рис. 8 приведена информационная значимость каждого из 115 атрибутов для 23 комбинаций КА. Рис. 8.а соответствует анализу информативности каждого атрибута по критерию chi2; рис. 8.б – анализу информативности каждого атрибута по индексу Джини (RF).

Анализ распределения гистограмм позволяет сделать два вывода. Каждый алгоритм оценки информативности формирует уникальную «картину» распределений значимости атрибутов. Например, алгоритм оценки информативности посредством по критерию chi2, выделил группу атрибутов, связанную с частотой центрального процессора, как значимую для многозначных атак, вызывающих «отказ в обслуживании». При этом индекс Джини для этих атрибутов незначителен. Аналогичная ситуация для распределения

Рис.8. Информационная значимость каждого из 115 атрибутов для 23 комбинаций КА:
а) анализ информативности каждого атрибута по критерию chi2;
б) анализ информативности каждого атрибута по индексу Джини (RF).

значимости атрибутов по критерию «индекс Джини» (RF). Вторым выводом является то, что разные КА имеют разное распределение значимых атрибутов. Анализ «спектра» полученных распределений выявил разделимость КА по информативности атрибутов, что позволяет решать задачу классификации наблюдаемых атак на имеющихся данных. Анализ гистограмм показывает, что многозначная КА, хоть и сочетает в себе признаки однозначных КА, являющихся ее составляющими, но является отдельной сущностью, чье распределение невозможно получить посредством сложения распределений однозначных КА.

В результате, как показано в [17], работа с многозначной КА как с отдельной сущностью может повысить точность классификации и прогнозирования, что обусловлено как особенностями алгоритмов МО, работающих в режиме обучения «с учителем», так и синергетическим эффектом многозначных данных.

Как известно, под синергией понимается усиливающий эффект взаимодействия двух или более факторов, характеризующийся тем, что совместное действие этих факторов существенно превосходит простую сумму действий каждого из указанных факторов. Так, например, в [17] алгоритмы МО на базе искусственной нейронной сети, работающие в режиме обучения «с учителем», чья архитектура предполагает наличие «скрытых» слоев и состояний, способны к выделению записей с многозначной классовой меткой (КА) в отдельный кластер. Выделение записей производится за счет формирования отдельных решающих правил для таких записей посредством выделения посредством корректировки ряда весовых коэффициентов (в случае искусственной нейронной сети; отдельных решающих деревьев в случае древовидных алгоритмов).

Поскольку многозначная КА является отдельной сущностью, эта сущность может быть выявлена алгоритмами МО с высокой обобщающей способностью, способными к кластеризации (например, искусственная нейронная сеть с включением самоорганизующихся карт Кохонена [18,19] в свою структуру). Если алгоритм МО не подразумевает многозначный выход, то даже при правильно выделенном кластере «внутри», отсутствие многозначного выхода приводит к ошибке классификации по двум причинам. Первой причиной является несовпадение результирующей однозначной классовой метки и многозначной эталонной метки (если данные размечены как многозначные) [20,21]. Второй причиной является «наложения» решающих правил, связанных с отнесением неразмеченной записи либо к многозначной КА, либо к однозначной КА, входящей в состав многозначной [22]. В случае некорректной разметки исходных данных (данные маркируются как однозначные при наличии многозначных записей), ошибка классификации (прогнозирования) происходит из-за несовпадения результирующей многозначной классовой метки и однозначной эталонной метки.

Выводы

Описывается создание ПАК для сбора телеметрии в ходе имитационного моделирования КА в КС, обладающих свойством *многозначности* в табличном представлении. Данные, порождаемые ПАК, могут быть использованы для противодействия КА при разработке СОВ, учитывающих многозначность «исторических» записей и интерпретироваться как средство обнаружения КА в КС.

ПАК имитирует реальные данные, соответствующие задачам информационной безопасности. За счет большого количества настраиваемых параметров моделирования КА, возможна «тонкая» настройка распределения классовых меток и соотношения доли однозначных и многозначных записей в данных, формируемых ПАК.

Новизна разработанного ПАК заключается автоматизированной параллельной маркировке всех КА, осуществляемых на КС, что позволяет учесть многозначность уже на этапе сбора данных.

С использованием разработанного ПАК, сформирован многозначный набор данных, представляющий собой диагностическую информацию о сети, подвергаемой 3 типам КА, совершаемым параллельно – «Отказ в обслуживании»; «Сетевая разведка»; «Фаззинг». В рамках реализации ККА типа «отказ в обслуживании» проведены атаки по по протоколам *ICMP*, *UDP* и *TCP*; в рамках реализации ККА типа «Сетевая разведка» проводились КА «сканирование портов» и «сканирование операционной системы».

Реализован новый фреймворк для решения задач классификации, прогнозирования и исследования гиперпараметров ИНС с множественным выходом для многозначных данных.

Обнаружено, что многозначная КА (совокупность однозначных КА) является отдельной сущностью с собственным распределением информативной значимости атрибутного пространства. Поскольку многозначная КА является отдельной сущностью, эта сущность может быть выявлена алгоритмами МО с высокой обобщающей способностью, способными к кластеризации. Если алгоритм МО не подразумевает многозначный выход, то даже при правильно выделенном кластере «внутри», отсутствие многозначного выхода приводит к ошибке классификации. Работа с многозначной КА как с отдельной сущностью, повышает точность классификации и прогнозирования.

Литература

1. *Котенко И. В., Дун Х. Обнаружение атак в интернете вещей на основе многозадачного обучения и гибридных методов сэмплирования // Вопросы кибербезопасности. 2024. Т. 60, № 2. С. 10–21. DOI: 10.21681/2311-3456-2024-2-10-21.*
2. *Рзаев Б. Т., Лебедев И. С. Применение бэггинга при поиске аномалий сетевого трафика // Научно-технический вестник информационных технологий, механики и оптики. 2021. Т. 21, № 2. С. 234–240. DOI: 10.17586/2226-1494-2021-21-2-234-240.*
3. *Solomin A. A., Ivanova Yu. A. Modern approaches to multiclass intent classification based on pre-trained transformers // Naučno-teh. vestn. inf. tehnol. meh. opt. 2020. Т. 20, № 4. С. 532–538. DOI: 10.17586/2226-1494-2020-20-4-532-538.*
4. *Лебедев И. В., Симонян А. Г. Анализ Трафика Для Исследования Сетевой Активности И Обнаружения Атак // Сборник трудов XIV Международной отраслевой научно-технической конференции. 2020. Москва: ООО «Издательский дом Медиа паблишер», 2020. С. 215–216.*
5. *Du Z., He K., Lui W., He W. Automated Neural Machine Translation for Icd Coding // Industry and agriculture. Т. 66, № 1. С. 41–58.*
6. *Бергер А. И., Гуда С. А. Свойства алгоритмов поиска оптимальных порогов для задач многозначной классификации // Компьютерные исследования и моделирование. 2022. Т. 14, № 6. С. 1221–1238.*
7. *Karpovich S. N. Multi-Label Classification of Text Documents using Probabilistic Topic Modeling // SPIIRAS Proceedings. 2016. Т. 4, № 47. С. 92–104. DOI: 10.15622/sp.47.5.*
8. *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.*
9. *Talukder Md. A., Hasan K. F., Islam Md. M., Uddin Md. A., Akhter A., Yousuf M. A., Alharbi F., Moni M. A. A dependable hybrid machine learning model for network intrusion detection // Journal of Information Security and Applications. 2023. Т. 72. С. 103405. DOI: 10.1016/j.jisa.2022.103405.*
10. *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. 102788. DOI: 10.1016/j.cose.2022.102788.*
11. *Кондаков С. Е., Рудь И. С. Модель процесса проведения компьютерных атак с использованием специальных информационных воздействий // Вопросы Кибербезопасности. 2021. Т. 45, № 5. С. 12–20. DOI: 10.21681/2311-3456-2021-5-12-20.*
12. *Шелухин О. И., Раковский Д. И. Визуализация Аномальных Событий При Прогнозировании Состояний Компьютерных Систем На Основе «Исторических Данных» // Reds: Телекоммуникационные Устройства И Системы. 2022. Т. 12, № 2. С. 53–58.*
13. *Vasilyev V., Kirillova A., Vulfin A., Nikonov A. Cybersecurity Risk Assessment Based on Cognitive Attack Vector Modeling with CVSS Score // 2021 International Conference on Information Technology and Nanotechnology (ITNT). Samara, Russian Federation: IEEE, 2021. С. 1–6. DOI: 10.1109/ITNT52450.2021.9649191.*
14. *Раковский Д. И. Обнаружение компьютерных атак и предупреждение нарушений функционирования компьютерных сетей на основе многозначных закономерностей // Сборник трудов III Всероссийской научной школы-семинара «Современные тенденции развития методов и технологий защиты информации». 2023. С. 307–311.*
15. *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. 102788. DOI: 10.1016/j.cose.2022.102788.*
16. *Кажемский М. А., Шелухин О. И. Многоклассовая Классификация Сетевых Атак На Информационные Ресурсы Методами Машинного Обучения // Труды Учебных Заведений Связи. 2019. Т. 5, № 1. С. 107–115. DOI: 10.31854/1813-324X-2019-5-1-107-115.*
17. *Шелухин О. И., Раковский Д. И. Многозначная классификация компьютерных атак с использованием искусственных нейронных сетей с множественным выходом // Труды учебных заведений связи. 2023 Т. 9, № 4. С. 95–111. DOI:10.31854/1813-324X-2023-9-4-97-113*
18. *Kukartsev V., Nelyub V., Kozlova A., Borodulin A., Rukosueva A. Intelligent Data Analysis as a Method of Determining the Influence of Various Factors on the Level of Customer Satisfaction of the Company // Data Analytics in System Engineering / под ред. Silhavy R., Silhavy P. Cham: Springer Nature Switzerland, 2024. Т. 935. С. 109–128. DOI: 10.1007/978-3-031-54820-8_11.*
19. *Karnaukh S. G., Markov O. E., Kukhar V. V., Shapoval A. A. Classification of steels according to their sensitivity to fracture using a synergetic model // Int J Adv Manuf Technol. 2022. Т. 119, № 7–8. С. 5277–5287. DOI: 10.1007/s00170-022-08653-y.*
20. *Zhang X., Zhuang Y., Zhang T., Li C., Chen H. Masked Image Modeling Auxiliary Pseudo-Label Propagation with a Clustering Central Rectification Strategy for Cross-Scene Classification // Remote Sensing. 2024. Т. 16, № 11. С. 1983. DOI: 10.3390/rs16111983.*
21. *Zhao T., Zhang Y., Miao D., Zhang H. Multi-granular labels with three-way decisions for multi-label classification // Int. J. Mach. Learn. & Cyber. 2023. Т. 14, № 11. С. 3737–3752. DOI: 10.1007/s13042-023-01861-2.*
22. *Priyadharshini M., Banu A. F., Sharma B., Chowdhury S., Rabie K., Shongwe T. Hybrid Multi-Label Classification Model for Medical Applications Based on Adaptive Synthetic Data and Ensemble Learning // Sensors. 2023. Т. 23, № 15. С. 6836. DOI: 10.3390/s23156836.*

References

1. *Kotenko I. V., Dun H. Obnaruzhenie atak v internete veshhej na osnove mnogozadachnogo obuchenija i gibridnyh metodov sjemplirovanija // Voprosy kiberbezopasnosti. 2024. Т. 60, № 2. S. 10–21. DOI: 10.21681/2311-3456-2024-2-10-21.*
2. *Rzaev B. T., Lebedev I. S. Primenenie bjegginga pri poiske anomalij setevogo trafika // Nauchno-tehnicheskij vestnik informacionnyh tehnologij, mehaniki i optiki. 2021. Т. 21, № 2. S. 234–240. DOI: 10.17586/2226-1494-2021-21-2-234-240.*
3. *Solomin A. A., Ivanova Yu. A. Modern approaches to multiclass intent classification based on pre-trained transformers // Naučno-teh. vestn. inf. tehnol. meh. opt. 2020. Т. 20, № 4. S. 532–538. DOI: 10.17586/2226-1494-2020-20-4-532-538.*
4. *Lebedev I. V., Simonjan A. G. Analiz Trafika Dlja Issledovanija Setevoj Aktivnosti I Obnaruzhenija Atak // Sbornik trudov XIV Mezhdunarodnoj otraslevoj nauchno-tehnicheskoj konferencii. 2020. Moskva: OOO «Izdatel'skij dom Media pablisher», 2020. S. 215–216.*
5. *Du Z., He K., Lui W., He W. Automated Neural Machine Translation for Icd Coding // Industry and agriculture. Т. 66, № 1. S. 41–58.*
6. *Berger A. I., Guda S. A. Svojstva algoritmov poiska optimal'nyh porogov dlja zadach mnogoznachnoj klassifikacii // Komp'juternye issledovanija i modelirovanie. 2022. Т. 14, № 6. S. 1221–1238.*

7. *Karpovich S. N. Multi-Label Classification of Text Documents using Probabilistic Topic Modeling // SPIIRAS Proceedings. 2016. T. 4, № 47. S. 92–104. DOI: 10.15622/sp.47.5.*
8. *Rakovskij D. I. Vlijanie problemy mnogoznachnosti metok klassov sistemnyh zhurnalov na zashhishhennost' komp'juternyh setej // Naukoemkie Tehnologii V Kosmicheskih Issledovanijah Zemli. 2023. T. 15, № 1. S. 48–56s. DOI: 10.36724/2409-5419-2023-15-1-48-56.*
9. *Talukder Md. A., Hasan K. F., Islam Md. M., Uddin Md. A., Akhter A., Yousuf M. A., Alharbi F., Moni M. A. A dependable hybrid machine learning model for network intrusion detection // Journal of Information Security and Applications. 2023. T. 72. S. 103405. DOI: 10.1016/j.jisa.2022.103405.*
10. *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. T. 120. S. 102788. DOI: 10.1016/j.cose.2022.102788.*
11. *Kondakov S. E., Rud' I. S. Model' processa provedenija komp'juternyh atak s ispol'zovaniem special'nyh informacionnyh vozdejstvij // Voprosy Kiberbezopasnosti. 2021. T. 45, № 5. S. 12–20. DOI: 10.21681/2311-3456-2021-5-12-20.*
12. *Sheluhin O. I., Rakovskij D. I. Vizualizacija Anomal'nyh Sobytij Pri Prognozirovanii Sostojanij Komp'juternyh Sistem Na Osnove «Istoricheskih Dannyh» // Reds: Telekommunikacionnye Ustrojstva I Sistemy. 2022. T. 12, № 2. S. 53–58.*
13. *Vasilyev V., Kirillova A., Vulfin A., Nikonov A. Cybersecurity Risk Assessment Based on Cognitive Attack Vector Modeling with CVSS Score // 2021 International Conference on Information Technology and Nanotechnology (ITNT). Samara, Russian Federation: IEEE, 2021. S. 1–6. DOI: 10.1109/ITNT52450.2021.9649191.*
14. *Rakovskij D. I. Obnaruzhenie komp'juternyh atak i preduprezhdenie narushenij funkcionirovanija komp'juternyh setej na osnove mnogoznachnyh zakonomernostej // Sbornik trudov III Vserossijskoj nauchnoj shkoly-seminara «Sovremennye tendencii razvitija metodov i tehnologij zashhity informacii». 2023. S. 307–311.*
15. *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. T. 120. S. 102788. DOI: 10.1016/j.cose.2022.102788.*
16. *Kazhemskij M. A., Sheluhin O. I. Mnogoklassovaja Klassifikacija Setevyh Atak Na Informacionnye Resursy Metodami Mashinnogo Obuchenija // Trudy Uchebnyh Zavedenij Svjazi. 2019. T. 5, № 1. S. 107–115. DOI: 10.31854/1813-324X-2019-5-1-107-115.*
17. *Sheluhin O. I., Rakovskij D. I. Mnogoznachnaja klassifikacija komp'juternyh atak s ispol'zovaniem iskusstvennyh nejronnyh setej s mnozhestvennym vyhodom // Trudy uchebnyh zavedenij svjazi. 2023 T. 9, № 4. S. 95–111. DOI:10.31854/1813-324X-2023-9-4-97-113*
18. *Kukartsev V., Nelyub V., Kozlova A., Borodulin A., Rukosueva A. Intelligent Data Analysis as a Method of Determining the Influence of Various Factors on the Level of Customer Satisfaction of the Company // Data Analytics in System Engineering / pod red. Silhavy R., Silhavy P. Cham: Springer Nature Switzerland, 2024. T. 935. S. 109–128. DOI: 10.1007/978-3-031-54820-8_11.*
19. *Karnaukh S. G., Markov O. E., Kukhar V. V., Shapoval A. A. Classification of steels according to their sensitivity to fracture using a synergetic model // Int J Adv Manuf Technol. 2022. T. 119, № 7–8. S. 5277–5287. DOI: 10.1007/s00170-022-08653-y.*
20. *Zhang X., Zhuang Y., Zhang T., Li C., Chen H. Masked Image Modeling Auxiliary Pseudo-Label Propagation with a Clustering Central Rectification Strategy for Cross-Scene Classification // Remote Sensing. 2024. T. 16, № 11. S. 1983. DOI: 10.3390/rs16111983.*
21. *Zhao T., Zhang Y., Miao D., Zhang H. Multi-granular labels with three-way decisions for multi-label classification // Int. J. Mach. Learn. & Cyber. 2023. T. 14, № 11. S. 3737–3752. DOI: 10.1007/s13042-023-01861-2.*
22. *Priyadharshini M., Banu A.F., Sharma B., Chowdhury S., Rabie K., Shongwe T. Hybrid Multi-Label Classification Model for Medical Applications Based on Adaptive Synthetic Data and Ensemble Learning // Sensors. 2023. T. 23, № 15. S. 6836. DOI: 10.3390/s23156836.*

АЛГОРИТМ ОЦЕНКИ УРОВНЯ ЦИФРОВОЙ АВТОНОМИИ КОМПОНЕНТОВ ИНФРАСТРУКТУРЫ ЦИФРОВОГО ПРОСТРАНСТВА

Рыженко А. А.[1], Селезнёв В. М.[2]

DOI: 10.21681/2311-3456-2024-4-131-139

Целью работы *является разработка и формализация алгоритма оценки уровня цифровой автономии компонентов инфраструктуры цифрового пространства, позволяющие рассматривать цифровые данные как бикубическую систему хранения атрибутивной информации.*

Метод исследования: *методы мультимножества, концептуальное моделирование, алгоритмизация процессов, ресурсов и объектов.*

Результат исследования: *разработана модель и алгоритм оценки автономии цифровых ресурсов, позволяющих рассматривать данные цифровой среды не только как источник информации для обладателей, но и как микросистему, позволяющую хранить служебную и атрибутивную информацию, а также нежелательные инъекции. В качестве формального описания используется числовое представление алгебры мультимножеств, как одного из наиболее эффективного инструмента представления процессов бинарной системы данных. Полученная постановка решает актуальную проблему формализации данных – моделирование процессов изменения атрибутивной модели цифрового объекта, а также оценки возможных изменений.*

Научная новизна *заключается в разработке нового элемента концептуального моделирования деструкторов моделей – бикубическая система оценки уровня автономии цифровых объектов.*

Ключевые слова: *деструктор, моделирование, интеллектуальный агент, фасет, иерархия, правила перехода, автоном, цифровое пространство, система.*

ALGORITHM FOR ASSESSING THE LEVEL OF DIGITAL AUTONOMY OF DIGITAL SPACE INFRASTRUCTURE COMPONENTS

Ryzhenko A. A.[3], Seleznev V. M.[4]

The aim of the work *is to develop and formalize an algorithm for assessing the level of digital autonomy of digital space infrastructure components, allowing us to consider digital data as a bicubic system for storing attribute information.*

Research method: *multiset methods, conceptual modeling, algorithmization of processes, resources and objects.*

Research result: *a model and algorithm for assessing the autonomy of digital resources has been developed, allowing us to consider digital environment data not only as a source of information for owners, but also as a microsystem that allows storing service and attribute information, as well as unwanted injections. As a formal description, the numerical representation of multiset algebra is used, as one of the most effective tools for representing the processes of a binary data system. The resulting formulation solves the current problem of data formalization – modeling the processes of changing the attribute model of a digital object, as well as assessing possible changes.*

The scientific novelty *lies in the development of a new element of conceptual modeling of model destructors – a bicubic system for assessing the level of autonomy of digital objects.*

Keywords: *destructor, modeling, intelligent agent, facet, hierarchy, transition rules, autonomy, digital space, system.*

1 Рыженко Алексей Алексеевич, кандидат технических наук, доцент, доцент кафедры информационной безопасности, Финансовый университет при Правительстве РФ, г. Москва, Россия. E-mail: AARyzhenko@fa.ru

2 Селезнёв Владимир Михайлович, кандидат технических наук, заведующий кафедрой информационной безопасности, Финансовый университет при Правительстве РФ, г. Москва, Россия. E-mail: VMSeleznyov@fa.ru

3 Aleksey A. Ryzhenko, Ph.D., Associate Professor, Financial University under the Government of the Russian Federation, Moscow. E-mail: AARyzhenko@fa.ru

4 Vladimir M. Seleznev, Ph.D., Head of department of information security, Financial University under the Government of the Russian Federation, Moscow. E-mail: VMSeleznyov@fa.ru

Введение

Существует типичное заблуждение, что в цифровой среде передается информация, которую можно отправить, получить и т.д. На уровне рядового пользователя вполне можно этим и ограничиться. Обладатели информации не обязаны знать, что происходит с данными при кодировании и декодировании, а также какую дополнительную служебную информацию хранит в себе каждый файл любой операционной системы [1]. В качестве подтверждения можно проанализировать терминологию, прописанную в ключевых федеральных законах – 149-ФЗ и 152-ФЗ. Таких понятий как *информация*, *владелец*, *хозяин* и даже *пользователь* просто не существует. Единственный статус у каждого субъекта цифровой среды – *обладатель информации*. Данный уровень достаточно подробно рассмотрен в юридической литературе, особый акцент делается на разнице между обладателем и правообладателем информации [2]. С другой стороны, термин *данные* не несет в себе никакой семантической нагрузки, представлен как набор *сигналов*, передаваемых через каналы связи. Достаточно корректное определение. В результате, под данными можно понимать не только то, что отображается обладателю, но и то, что видит операционная система на прикладном уровне, и то, что может быть незаконно добавлено (инъекция) в тело файла. Именно это обстоятельство и мешает юридической системе дать точное определение – что такое цифровая информация. В качестве выхода из данной ситуации было предложено делать оценку уровня автономии каждого цифрового ресурса, что даст возможность рассматривать каждый файл не только как объект, содержащий какую-либо информацию, но и принадлежность, что является одним из ключевых критериев цифрового суверенитета [3, 4].

Ранее была рассмотрена технология обучения интеллектуального агента умной бот-сети [5], а также этапы формирования единой модели данных, основанной на единой базе правил и распределенной архитектуре баз ассоциаций [6]. Аналогичные исследования проводятся и по другим современным направлениям, где необходимо проводить оценку для формирования критериев обратной связи [7].

2. Новый подход формализации данных, основанный на алгебре процессов

Рассмотрим простую задачу оценки уровня автономии цифрового объекта на этапах жизненного цикла. Условие: для цифрового изображения, передаваемого по каналам связи, на основе атрибутивной схемы необходимо предугадать возможное заражение инъекцией вредоносом. Исходные наборы атрибутов представлены в табл. 1.

Таблица 1.

Атрибуты цифрового изображения

Внутренние атрибуты	Внешние атрибуты
1 – размер × разрешение 2 – глубина цвета 3 – тип кодирования / сжатие 4 – устройство захвата 5 – дата создания	1 – имя 2 – атрибуты 3 – размер файла 4 – источник 5 – дата изменения

Представим цифровое изображение не как графический файл, а как битовая последовательность блоков кодирования изображения. Большиинство свободно распространяемых графических форматов состоят из двух больших блоков: первый – кодовая матрица изображения, второй – атрибутивная составляющая и блок служебной информации. Как правило, второй блок заполняется изначально нулями и не содержит необходимую для самого файла информацию. Именно этим фактором и пользуются инъектологи, прописывая во второй блок другие файлы (инъекции). Как выявить вложенный файл – до сих пор не существует универсальных алгоритмов и многие антивирусные программы пропускают файлы с инъекцией. Аналогичные исследования отражены в ряде актуальных работ, например [8, 9]. Рассмотрим сначала пример использования атрибутивной модели на дереве решений, затем отображение в виде бикубической модели и перейдем к формальному описанию и примерам использования на практике.

Первый этап: на мобильном устройстве выполнен захват и формирование нового цифрового изображения. При конвертировании в доступный формат автоматически добавился первый список атрибутов из двух частей (табл. 1).

Второй этап: пользователь решил отправить фото изображение через мессенджер. Прикрепляет цифровое фото как контейнер и отправляет получателям. При передачи запускается служба аудита, встроенная в мессенджер, которая автоматически добавляет в служебный блок корректировку – другой метод сжатия (фото изображение становится меньше в байтовом эквиваленте), дата создания нового изображения и т.д. (рис. 1).

Примечание: на рисунках 1–3 модули I–V – этапы процесса анализа атрибутов, 1–5 – атрибуты таблицы 1. В кружках обозначены статусы процессов от 1 до 5, о чем будет подробнее представлено в третьей части формализации.

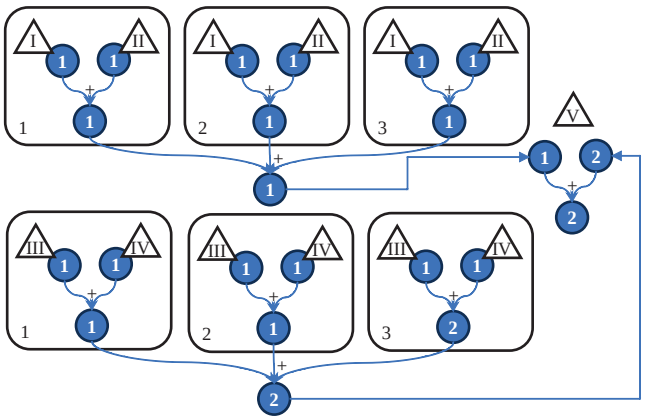


Рис. 1. Выявление вредоноса по правилу «тип кодирование – размер»

В результате пользователь получает изображение с измененным набором атрибут. Если пользователю надо только само изображение, т.е. первый блок, то операционной системе больше нужен второй описательный блок для получения служебной информации. При этом сразу необходимо учесть важный фактор: если сам отправитель умышленно сделал инъекцию в цифровое изображение, то у него могут возникнуть проблемы с отправлением с сохранением целостности файловой архитектуры. Другими словами, если отправитель отправит зараженный файл просто в ветку чата, то второй блок будет изменен встроенной службой, но если отправит как вложение файла без распознования мессенджером файла как изображения, то инъекция будет передана получателю. На рисунке 1 отображена исходная ветка дерева анализа и принятия решений решений. Встроенный агент обнаружил, что полученный файл имеет другой метод сжатия и другой размер. При этом возможно два вариант: изменения мессенджером и изменение отправителем. Происходит дальнейший анализ атрибутов.

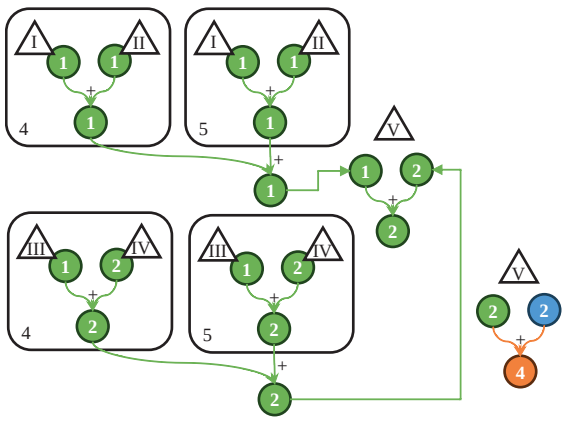


Рис. 2. Выявление вредоноса по правилу «источник – дата»

Производится проверка атрибутов источника информации и даты изменения. Если сжатие изменил мессенджер, то это отразится в атрибуте источника, если отправитель – изменений не будет. Далее происходит проверка даты и времени изменения файла. Атрибут не изменится и будет меньше даты и времени отправления отправителем, если инъекция была сделана самим отправителем. Если изменения внес мессенджер, то дата изменится на более позднюю и отразится в атрибутах (рис. 2). В результе четыре атрибута дают вариант решения (рис. 3).

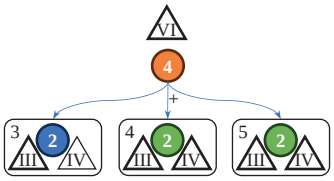


Рис. 3. Итоговый узел дерева решений для выявление вредоноса по правилам

Необходимо учесть, что функция XOR дает возможность исключения альтернативных веток с исключающим решением. В результате для исполнителя данного дерева (агента) строится простое правило:

$$((1+1)\oplus(1+1)\oplus(1+1)) + ((1+1)\oplus(1+1)\oplus(1+2)) + + ((1+1)\oplus(1+1)) + ((1+2)\oplus(1+2)) = 4 \xrightarrow[5]{} 2 + 2 + 2.$$

Аналогичные результаты можно обнаружить в ряде научных работ, например [10, 11].

Для формального описания двухкритериальной системы атрибутов можно использовать бикубические модели фасетных данных. Тогда графически описанный пример можно представить как куб с шестью фасетными гранями: три грани атрибутов отправители и три – получателя (рис. 4) [5]. На четырех гранях строятся фасеты атрибутов, на двух – деревья преобразования, представленные выше.

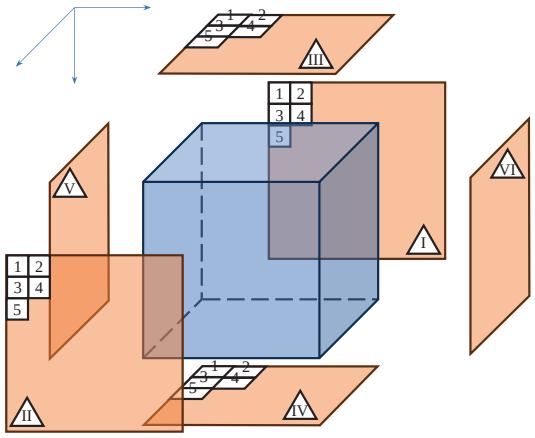


Рис. 4. Бикубическая модель атрибутов цифрового автонома

DOI: 10.21681/2311-3456-2024-4-131-139

Представленный пример отображает схематическое описание процессов построения правила дерева решения. Интересные аналогичные результаты можно наблюдать в работах по использованию алгебры мультимножеств для решения практических задач, например [12, 13]. Далее рассмотрим алгебраическую составляющую модели.

2.1. Формализация и моделирование процессов перехода состояний агентов

Разберем простейшую задачу сложения процессов при выборе альтернативного решения в узловой точке произвольного дерева решений. Алгебра синтаксической формы представления знаний предполагает следующую последовательность действий при классическом сложении: берем один закрытый процесс (т.е. процесс в пассивном режиме), открываем один активный процесс (т.е. запускаем в действие) – это «один». Открываем второй процесс – это «два» и т.д. Если предполагается, что активные и пассивные процессы разные, то решение будет в синтаксической постановке путем сложения процессов (частный случай). Тем не менее, существует и другой сценарий, когда процессы возвращаются обратно в закрытое состояние.

Например, сканер одной социальной сети был запущен по расписанию на поиск личности. Процесс закончен. Два варианта вывода результата: информация получена, и информация не получена. В первом случае проверяется количество решений. Для каждого строится отдельная ветка дерева решений. При этом параллельно второй процесс запускает поиск информации по личности в другой социальной сети, но ориентируется на варианты результатов первого поиска. Далее, для отключения возможности неразрешимых коллизий при несоответствии информации одновременных поисков решений используется семантическая алгебра процессов.

Алгоритм данной постановки, следующий: запускаем (открываем) один процесс – это один. Закрываем обратно и открываем снова – «+1», т.е. процесс произошел или добавился дважды, а результат при этом не изменился. Получаем, что «1+1=1». Данный сценарий используется в прикладной математике как логическая аддитивная Булева функция ИЛИ. Развивая процесс (не забывая о критерии целостности, т.е. всегда есть предполагаемая максимальная граница достаточности запущенных процессов) получаем, что, открыв два процесса, а потом, открыв и закрыв один из них имеем: «2+1=2». Расширяя до предела целого (допустим, узел дерева предполагает пять одновременно запущенных альтернативных процесса, т.е. равно «5»), имеем: «3+1=3», «4+1=4», «5+1=5». Здесь нет «и так далее» так как процессы в пределах целого «5» заканчиваются. Но, внутри целого можно также использовать и стандартный аддитивный сценарий сложения: «4+1=5» или «2+2=4», так как в пределах показателя целого можем использовать любые аддитивные процессы. Также поддерживается функция с нулем: «0+0=0», «0+1=1», ..., «0+5=5» (все процессы закрыты – все процессы открыты). Для того чтобы далее не путать результат классического сложения и сложения от целого обозначим первый (классический) вариант знаком «=», а результат по основанию от целого знаком «$\underset{5}{\rightarrow}$» (в данном случае, основание равно «5»). Независимо от величины целого в диапазоне от 0 до бесконечности или $[0,\infty)$, *верхняя граница* будет *не более максимального значения – значения* самого *целого*. Например, если целое (максимально допустимое количество одновременно обрабатываемых альтернатив) равно десяти, то целое равно десяти, но обозначение следствия к множеству решений будет зависеть от условия задачи, о чём будет сказано ниже.

Нижняя граница имеет при описанных условиях значение равное нулю (все процессы закрыты). Однако в задачах с отрицательной величиной (процессы не открываются – закрываются, а закрываются и открываются, т.е. обратная задача) допускается взаимообратное целому число, т.е. для данного примера нижняя граница будет равна «–5», а верхняя – «5» (целое, все процессы закрыты). В результате сценарий с одним прячущимся процессом и граничные сценарии в пределах целого *имеют одно основание*. Данная процедура возможна при уже запущенных интеллектуальных агентах обратным целевым деревом. При этом допускается, что прямое дерево будет использовать агентов обратного дерева решений. Можно предположить, что:

для любого целого верхней границей всегда будет значение (показатель) целого, нижней – ноль или взаимно-противоположное целому значение верхней границы. (П.3)

Как и ранее, далее для примера рассматриваем целое – максимум пять активных процессов, но изменим начальное условие. Если одновременно действующих открыл / закрыл процессов будет не один, а два (т.е. одновременно происходит поиск выбора решений для нескольких узловых точек прямого дерева решений), то результатом *аддитивного сложения* (например, на два) может быть, как два, так и три, и граничный – четыре (расширенный вариант функции XOR):

– «$2 + 2 \underset{5}{\rightarrow} 2$» – два процесса открыли, их же закрыли и открыли вновь – *обновляемый сценарий*. Подтверждение: $2 + 2 = (1_1 + 1_1) + (1_1 + 1_1) \underset{5}{\rightarrow} 1 + 1 = 2$. Так как $1_1 + 1_1 \underset{5}{\rightarrow} 1_1$;

– «$2 + 2 \underset{5}{\rightarrow} 3$» – два процесса открыли, один из них закрыли и открыли его же, но с другим (не равном первому) процессом – увеличивающий сценарий. Подтверждение: $2 + 2 = (1 + 1) + (1_1 + 1_1) \underset{5}{\rightarrow} 2 + 1_1 = 3$. Так как $1_1 + 1_1 \underset{5}{\rightarrow} 1_1$;
– «$2 + 2 \underset{5}{\rightarrow} 4$» – два процесса открыли, и, не закрывая предыдущие, открыли еще два – *классический сценарий*. Подтверждение: $2 + 2 = (1 + 1) + (1 + 1) = 4$.

Если действующих процессов не равное количество, т.е. в закрытии и открытии участвуют, допустим, два и три, то правило (П.1) сохраняется. Но, необходимо выполнять дополнительное условие: *максимальное количество закрытых и открытых процессов в пределах целого должно быть однозначно одинаковым*.

Особенностью предыдущего сценария является учет только предположения о целостности (П.1). Существует еще *субтрактивное сложение*, когда сумма может быть меньше любого слагаемого. Например, «$2 + 2 \underset{5}{\rightarrow} 1$» (два открытых процесса закрыли и открыли только один из них – отнимающий сценарий. Подтверждение: $2 + 2 = (1_1 + 1_1) + (1_1 + 1_1) \underset{5}{\rightarrow} 1_1 + 1_1 \underset{5}{\rightarrow} 1$. Так как $1_1 + 1_1 \underset{1}{\rightarrow} 1_1$. Рассмотрим данный сценарий (с теми же начальными условиями) на примере паевой геометрической фигуры (рис. 5).

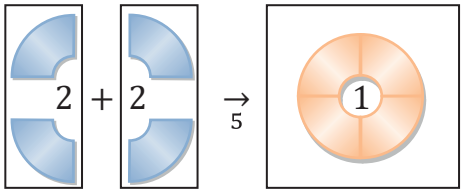


Рис. 5. Пример использования субтрактивной функции сложения внутри целого (пяти)

Раскрывая сущность целого, далее покажем, что результат любой суммы элементов целого может быть равен верхней границе, т.е. значению самого целого (рис. 6). Для рассматриваемого примера «$2 + 2 \underset{5}{\rightarrow} 5$» добавочный сценарий. Подтверждение: $2 + 2 = (1 + 1) + (1 + 1_1) \underset{5}{\rightarrow} (1 + 1) + (1 + 1_1 + 1_1) \underset{5}{\rightarrow} 5$, так как $1_1 \underset{1}{\rightarrow} 1_1 + 1_1$.

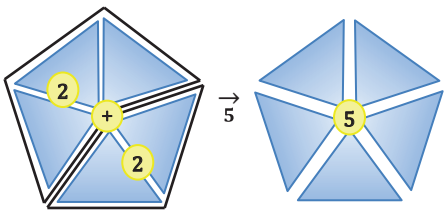


Рис. 6. Пример использования добавочного сценарий аддитивной функции сложения внутри целого пяти

Функция аддитивности и субтрактивности сохраняется и далее. Например, для целого десяти можно открывать и закрывать как все пять процессов, так и любое количество в пределах целого – пяти. Можно предположить, что:

показатель суммы определяет количество вариантов сложения, но не более целого. Ноль является нижним значением – исключение. (П.2)

Графически аддитивный алгоритм можно представить аналогично субтрактивному алгоритму сложения в пределах целого (рис. 7).

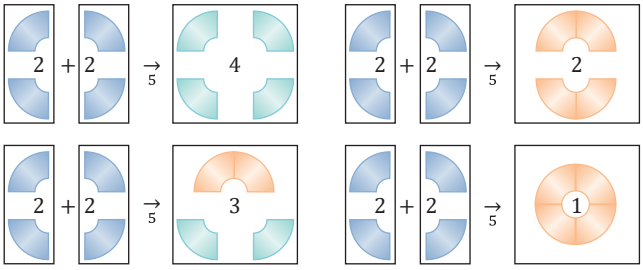


Рис. 7. Пример использования аддитивной и субтрактивной функций сложения внутри целого пяти

При изменении значения целого будет меняться количество возможных вариантов результатов сложения, и верхняя граница значений. Следовательно, можно предположить, что:

в пределах целого аддитивные и субтрактивные произвольные суммы элементов множества могут принимать значения равные одному из элементов этого множества. (П.3)

Другими словами, значение суммы может быть равно любому своему слагаемому.

аддитивной суммой любых элементов целого является множество последовательных чисел от наименьшего равного элементу до максимального равному результату суммы классического сложения в пределах целого или значению целого. (П.4)

Для правил П.3 и П.4 сумма нулей является исключением:

субтрактивной суммой любых элементов целого является множество последовательных чисел от наименьшего равного единице до максимального равному наименьшему элементу. (П.5)

Формальное описание для данного сценария может выглядеть следующим образом:

$$\sum_{i=0}^{n} a_i \underset{m}{\longrightarrow} [1,m], \text{ где } n \in [1,\infty),\ m \in [0,n] \qquad (1.1)$$

a_i – элемент множества, m – целое, n – произвольный элемент.

4. От формальной теории к практике использования

Рассмотрим несколько сценариев использования описанной модели на практических примерах в цифровой среде.

Сценарий 1: используем метод формирования дерева сценария достижения итоговой цели одного потока данных. Предполагается, что на всех промежуточных узлах дерева решений используются независимые решения, и лишь некоторые должны быть частью итогового сценария. Например, в рассмотренной ранее задаче кражи личности каждый последующий этап дерева решений будет зависеть от результатов предыдущего. При этом необходимо рассмотреть все возможные варианты сбора информации, но фактически образ личности будет составляться только из тех узловых точек, которые соответствуют целевому поиску. Иными словами, если на первых этапах вариантов решений будет множество (например, ассоциативный поиск по фотографии может представить множество решений), то каждый последующий поиск будет уже ограничен предыдущим выбором соответствия (включая ID, номера привязки к документам, средствам коммуникации и т.д.).

Задача 1 (частный случай): сбор данных состоит из двух решений на узловой точке, заложено в решение *пять* этапов поиска. Пусть на *первом этапе* найдено *шесть* альтернативных решений как результат основного поиска. Ограничением заложена допустимость – *три* решения (*два* промежуточных и *третий* итоговый). Следовательно, используются все *шесть* решений, но *три* из них будут подводящие, не выпадающие из общего поиска. В другом поиске получено *пять* решений, а разрешено только *два*, но оба должны подвергнуться дальнейшему использованию (такое вполне возможно если у пользователя несколько аккаунтов в одной социальной сети). Следовательно, *три решения* из них будут подводящие к итоговому. Необходимо также учесть, что общая

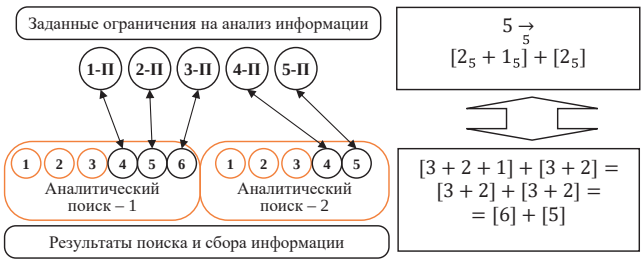


Рис. 8. Схематическое представление решения первой задачи

сумма всех процессов не может выйти за заданный верхний предел (рис. 8). *Необходимо построить и решить логическое выражение, описывающее процесс построения итогового решения*.

Обобщенное правило перехода состояний процесса поиска и выбора будет представлено следующим образом:

$$[3 + 2_5 + 1_5] + [3 + 2_5] \underset{5}{\longrightarrow} 5.$$

Согласно данному правилу, полученным промежуточным результатам поиска необходимо следовать следующим ограничениям:

- нельзя передать все результаты одного поиску;
- минимальное количество полученных решений одного поиска, используемых для проекта, не должно превышать максимальное количество допустимых решений самого проекта.

Сценарий 2: предположим, что некий «тролль» поселился в открытой ветке форума социальной сети ведомственной организации и начал вести свою пропаганду, используя слова и словосочетания негативного контента. Агенту необходимо провести анализ ленты используя контент сообщений за двое суток. Найти точки соприкосновения с официальной лентой Министерства, поставить соответствующие гиперссылки.

Новости 18.00

В 16.30 оперативный дежурный места массового скопления людей X г. Y_1 обнаружил чужеродный предмет возле кафе-столовая$_2$. Дежурный вызвал по телефону оперативную служба$_3$. В 16.40 произошел взрыв$_4$ мусорного бачка. Оперативная служба$_3$ прибыла с опозданием только в 16.45. Оставили машину за территорией организации$_2$ и чего-то ждали. Начальник оперативного штаба прибыл только в 17.00, когда уже было поздно. Спасатели$_3$ медленно стали разбирать образовавшийся завал$_4$. Пожар$_4$ продолжается, жертвы не известны. Уже уничтожен один этаж$_2$. Верхний этаж$_2$ пока горит, задымление, но спасатели что-то тушат и выносят.

Новости 8.00 следующего дня

Только к 19.00 удалось потушить пожар$_4$ на этаже$_2$ организации X_1. Уничтожен один комплекс$_2$ организации. Значительные повреждения основного сооружения. Сотрудники спасательной службы$_3$ действовали как сонные мухи. Если бы все было иначе, возможно последствия были бы намного меньше.

Проект в виде официальной новостной ленты

Вызов диспетчерской организации X_1 города Y_1 поступил в 16.35. Дежурный X_1 оставил заявку о пожаре$_4$ в районе второго этажа$_2$. В 16.38 на вызов выехала дежурная бригада спасателей$_3$. Теоретическое время прибытия – 10 мин., фактическое

составило 8 мин. На момент прибытия (16.45) произошел взрыв$_4$ мусорного бака$_2$. Пламя и осколки$_4$ раскинулись по территории объекта. Из-за отсутствия искусственных заграждений возможно дальнейшее распространение за территорию объекта. В связи с увеличением сложности чрезвычайной ситуации, собран специализированный оперативный штаб. До решения штаба о ликвидации оперативная бригада производила локализацию источника в пределах объекта. В 17.00 получены рекомендации центрального аппарата – алгоритм локализации и ликвидации. Очаги возгорания устранены к 19.00. Производится устранение последствий средствами спасательной службы$_3$.

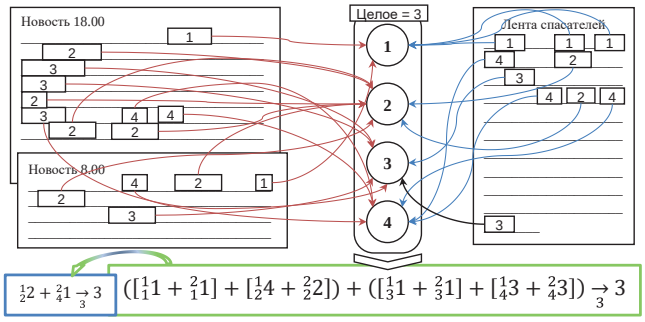


Рис. 9. Графическое представление условия задачи

Задача 2: для сообщений в пределах 100±20 слов допускается не более 3 ссылок [целое равно 3]. Второе сообщение в два раза меньше, чем первое [ссылок в два раза меньше]. Количество для каждой очередной ссылки в два раза меньше предыдущей. Остается первая попавшаяся ссылка из выбранных. *Задание:* вставить в ключевые позиции сообщения гиперссылки (рис. 9).

Разбираем сообщения (условия):

- слова из базы искусственного алфавита потенциальных источников попадаются в сообщениях 8 раз (индексы 1 и 2) $[{}^{1}_{1}1 + {}^{2}_{1}1]$ и $[{}^{1}_{2}4 + {}^{2}_{2}2]$ соответственно;
- слова из базы искусственного алфавита АСФ и типов аварий попадаются в сообщениях 8 раз (индексы 3 и 4) – $[{}^{1}_{3}1 + {}^{1}_{3}1]$ и $[{}^{1}_{4}3 + {}^{2}_{4}3]$ соответственно;
- первый алфавит используется в начале текста или в первых сообщениях (завязка), второй в конце или последних (развязка).

Общая функция перехода состояний выглядит следующим образом:

$$([{}^{1}_{1}1 + {}^{2}_{1}1] + [{}^{1}_{2}4 + {}^{2}_{2}2]) + ([{}^{1}_{3}1 + {}^{2}_{3}1\ ] + [{}^{1}_{4}3 + {}^{2}_{4}3]) \to_3 3.$$

Дальше необходимо сократить количество ссылок до трех возможных:

- первая и третья скобки попадают под правило $1_3 + 1_3 \to_3 1_3$ если не хотим добавить чего-то нового (в условии этого нет). Результат:

$$([{}^{1}_{1}1] + [{}^{1}_{2}4 + {}^{2}_{2}2]) + ([{}^{2}_{3}1] + [{}^{1}_{4}3 + {}^{2}_{4}3]) \to_3 3;$$

- четвертая скобка имеет равные элементы, но, $3_3 + 3_3 \to_3 3_3$, поглощаем первое (третье условие). Результат:

$$([{}^{1}_{1}1] + [{}^{1}_{2}4 + {}^{2}_{2}2]) + ([{}^{2}_{3}1] + [{}^{2}_{4}3\ ]) \to_3 3;$$

- раскрываем скобки с одним слагаемым и внешние:

$${}^{1}_{1}1 + [{}^{1}_{2}4 + {}^{2}_{2}2] + {}^{2}_{3}1 + {}^{2}_{4}3 \to_3 3;$$

убираем единичные ссылки, т.к. попадают под правило $1_3 + 1_3 \to_3 1_3$:

$$[{}^{1}_{2}4 + {}^{2}_{2}2] + {}^{2}_{4}3 \to_3 3;$$

- в первой скобке «4» выпадает за целое, разделяем и выносим за соответствие с проектом:

$$[{}^{1}_{2}2 + {}^{1}_{2}2 + {}^{2}_{2}2] + {}^{2}_{4}3 \to_3 3;$$

- раскрываем внутренние скобки:

$${}^{1}_{2}2 + {}^{2}_{4}3 \to_3 3;$$

- второе сообщение в два раза меньше первого, значит:

$${}^{1}_{2}2 + ({}^{2}_{4}2 + {}^{2}_{4}1) \to_3 3;$$

- раскрываем внутренние скобки:

$${}^{1}_{2}2 + {}^{2}_{4}2 + {}^{2}_{4}1 \to_3 3;$$

- во втором сообщении должно быть в два раза меньше ссылок. Выполняем третье условие, тогда:

$${}^{1}_{2}2 + {}^{2}_{4}1 \to_3 3.$$

Получаем две ссылки в первом сообщении с индексом «2» и одну ссылку во втором сообщении с индексом «4». В примере индексы дописываются для удобства анализа, хотя в задачах указывать не обязательно.

Заключение

Обзор современной литературы дает недвусмысленно понять, что несмотря на многочисленные попытки хоть как-то приблизить теорию к практике, многие научные деятели до сих пор не хотят отображать в своих публикациях практику использования научных достижений. Бывает и наоборот, исследователи приводят готовые фрагменты кода без соответствующих комментариев [14]. Данный фактор

не дает возможность полностью оценить как научные, так и практические результаты научных исследований. В данной работе сделана попытка приблизить достаточно мощный математический аппарат теории мультимножеств к практическим задачам цифрового пространства. Полученные результаты уже достаточно хорошо проявили себя на практике при построении контуров защиты корпоративных систем, предоставляющих доступ из внешней среды. Также развитие получило еще одно современное направление – построение дискретных пространств бинарных данных при создании кода быстрого отклика (*Quick Response Code*) корпоративного уровня, что дает дополнительную защиту к передаваемым данным. Некоторые практические результаты по неоднозначности кодирования информации, а также сокрытия искусственных алгоритмов отражено в ряде статей, например [15–17].

Литература

1. *Рыженко А. А. Организация системы подготовки сотрудников организаций в сфере противоборства механизмам социальной инженерии // Проблемы управления безопасностью сложных систем. Материалы XXX международной конференции. Под общей редакцией А. О. Калашникова, В. В. Кульбы. Москва, 2022. С. 337–342*
2. *Правообладатель данных или обладатель информации – кого имеет в виду закон? – режим доступа: https://zakon.ru/blog/2020/11/14/pravoobladatel_dannyh_ili_obladatel_informacii__kogo_ imeet_v_vidu_zakon (дата посещения 06.06.2024 г.)*
3. *Рыженко А. А., Рыженко Н. Ю. Интеллектуальные деструкторы и мобильные банковские клиенты // Актуальные проблемы и перспективы развития экономики: Труды XXI Международной научно-практической конференции. Симферополь-Гурзуф, 20–22 октября 2022 год. / Под ред. д.э.н., д.пед.н., профессора Н. В. Апатовой. – Симферополь: Издательский дом КФУ имени В. И. Вернадского, 2022. – с. 241-242.*
4. *Рыженко А. А., Рыженко Н. Ю. Утечки данных и рейтинги банков // Теория и практика экономики и предпринимательства. Труды XX Международной научно-практической конференции. Под редакцией Н. В. Апатовой. Симферополь, 2023. С. 215-216*
5. *Рыженко А. А. Умная бот-сеть или модель интеллектуального деструктора // Вопросы кибербезопасности. 2023. № 5(57). С. 60–68. DOI: 10.21681/2311-3456-2023-5-60-68*
6. *Рыженко А. А., Селезнёв В. М. Модель систематизации классификаторов деструктивных и конструктивных событий цифрового пространства // Вопросы кибербезопасности. 2024. № 3(61). С. 113-119. DOI: 10.21681/2311-3456-2024-3-113-119*
7. *Kaushik, B., Sharma, R., Dhama, K. et al. Performance evaluation of learning models for intrusion detection system using feature selection. J Comput Virol Hack Tech 19, 529–548 (2023). https://doi.org/10.1007/s11416-022-00460-z*
8. *Hashemi, H., Samie, M. E. & Hamzeh, A. IFMD: image fusion for malware detection. J Comput Virol Hack Tech 19, 271-286 (2023). https://doi.org/10.1007/s11416-022-00445-y*
9. *Alaeiyan, M., Parsa, S. A hierarchical layer of atomic behavior for malicious behaviors prediction. J Comput Virol Hack Tech 18, 367–382 (2022). https://doi.org/10.1007/s11416-022-00422-5*
10. *Dalla Preda, M., Ianni, M. Exploiting number theory for dynamic software watermarking. J Comput Virol Hack Tech 20, 41–51 (2024). https://doi.org/10.1007/s11416-023-00489-8*
11. *Babash, A. V. XOR ciphers model and the attack to it. J Comput Virol Hack Tech 18, 275–283 (2022). https://doi.org/10.1007/s11416-022-00419-0*
12. *Karamitas, C., Kehagias, A. Improving binary diffing speed and accuracy using community detection and locality-sensitive hashing: an empirical study. J Comput Virol Hack Tech 19, 319–337 (2023). https://doi.org/10.1007/s11416-022-00452-z*
13. *Nikolopoulos, S. D., Polenakis, I. Behavior-based detection and classification of malicious software utilizing structural characteristics of group sequence graphs. J Comput Virol Hack Tech 18, 383–406 (2022). https://doi.org/10.1007/s11416-022-00423-4*
14. *Casolare, R., Fagnano, S., Iadarola, G. et al. Picker Blinder: a framework for automatic injection of malicious inter-app communication. J Comput Virol Hack Tech 20, 331–346 (2024). https://doi.org/10.1007/s11416-023-00510-0*
15. *Секреты USA в Micro QR Code M4 (часть 1). – режим доступа: https://habr.com/ru/articles/781858/ (дата посещения 06.06.2024 г.)*
16. *Секреты USA в Micro QR Code M2 (часть 2). – режим доступа: https://habr.com/ru/articles/782488/ (дата посещения 06.06.2024 г.)*
17. *Секреты USA в Micro QR Code M3 (часть 3). – режим доступа: https://habr.com/ru/articles/782772/ (дата посещения 06.06.2024 г.)*

References

1. *Ryzhenko A. A. Organizacija sistemy podgotovki sotrudnikov organizacij v sfere protivoborstva mehanizmam social'noj inzhenerii // Problemy upravlenija bezopasnost'ju slozhnyh sistem. Materialy XXX mezhdunarodnoj konferencii. Pod obshhej redakciej A. O. Kalashnikova, V. V. Kul'by. Moskva, 2022. S. 337–342*
2. *Pravoobladatel' dannyh ili obladatel' informacii – kogo imeet v vidu zakon? – rezhim dostupa: https://zakon.ru/blog/2020/11/14/pravoobladatel_dannyh_ili_obladatel_informacii__kogo_ imeet_v_vidu_zakon (data poseshhenija 06.06.2024 g.)*
3. *Ryzhenko A. A., Ryzhenko N. Ju. Intellektual'nye destruktory i mobil'nye bankovskie klienty // Aktual'nye problemy i perspektivy razvitija jekonomiki: Trudy XXI Mezhdunarodnoj nauchno-prakticheskoj konferencii. Simferopol'-Gurzuf, 20-22 oktjabrja 2022 god. / Pod red. d.je.n., d.ped.n., professora N. V. Apatovoj. – Simferopol': Izdatel'skij dom KFU im. V.I. Vernadskogo, 2022. – s. 241-242.*
4. *Ryzhenko A. A., Ryzhenko N. Ju. Utechki dannyh i rejtingi bankov // Teorija i praktika jekonomiki i predprinimatel'stva. Trudy XX Mezhdunarodnoj nauchno-prakticheskoj konferencii. Pod redakciej N. V. Apatovoj. Simferopol', 2023. S. 215-216*
5. *Ryzhenko A. A. Umnaja bot-set' ili model' intellektual'nogo destruktora // Voprosy kiberbezopasnosti. 2023. № 5(57). S. 60–68. DOI: 10.21681/2311-3456-2023-5-60-68*
6. *Ryzhenko A. A., Seleznjov V. M. Model' sistematizacii klassifikatorov destruktivnyh i konstruktivnyh sobytij cifrovogo prostranstva // Voprosy kiberbezopasnosti. 2024. № 3(61). S. 113–119. DOI: 10.21681/2311-3456-2024-3-113-119*
7. *Kaushik, B., Sharma, R., Dhama, K. et al. Performance evaluation of learning models for intrusion detection system using feature selection. J Comput Virol Hack Tech 19, 529–548 (2023). https://doi.org/10.1007/s11416-022-00460-z*

8. *Hashemi, H., Samie, M. E. & Hamzeh, A. IFMD: image fusion for malware detection. J Comput Virol Hack Tech 19, 271–286 (2023). https://doi.org/10.1007/s11416-022-00445-y*
9. *Alaeiyan, M., Parsa, S. A hierarchical layer of atomic behavior for malicious behaviors prediction. J Comput Virol Hack Tech 18, 367–382 (2022). https://doi.org/10.1007/s11416-022-00422-5*
10. *Dalla Preda, M., Ianni, M. Exploiting number theory for dynamic software watermarking. J Comput Virol Hack Tech 20, 41–51 (2024). https://doi.org/10.1007/s11416-023-00489-8*
11. *Babash, A. V. XOR ciphers model and the attack to it. J Comput Virol Hack Tech 18, 275–283 (2022). https://doi.org/10.1007/s11416-022-00419-0*
12. *Karamitas, C., Kehagias, A. Improving binary diffing speed and accuracy using community detection and locality-sensitive hashing: an empirical study. J Comput Virol Hack Tech 19, 319–337 (2023). https://doi.org/10.1007/s11416-022-00452-z*
13. *Nikolopoulos, S. D., Polenakis, I. Behavior-based detection and classification of malicious software utilizing structural characteristics of group sequence graphs. J Comput Virol Hack Tech 18, 383–406 (2022). https://doi.org/10.1007/s11416-022-00423-4*
14. *Casolare, R., Fagnano, S., Iadarola, G. et al. Picker Blinder: a framework for automatic injection of malicious inter-app communication. J Comput Virol Hack Tech 20, 331–346 (2024). https://doi.org/10.1007/s11416-023-00510-0*
15. *Sekrety USA v Micro QR Code M4 (chast' 1). – rezhim dostupa: https://habr.com/ru/articles/781858/ (data poseshhenija 06.06.2024 g.)*
16. *Sekrety USA v Micro QR Code M2 (chast' 2). – rezhim dostupa: https://habr.com/ru/articles/782488/ (data poseshhenija 06.06.2024 g.)*
17. *Sekrety USA v Micro QR Code M3 (chast' 3). – rezhim dostupa: https://habr.com/ru/articles/782772/ (data poseshhenija 06.06.2024 g.)*

ИСПОЛЬЗОВАНИЕ ЦИФРОВЫХ ДВОЙНИКОВ С ЦЕЛЬЮ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КИБЕРФИЗИЧЕСКИХ СИСТЕМ

Водопьянов А. С.[1]

DOI: 10.21681/2311-3456-2024-4-140-144

Цель исследования *– работа посвящена исследованию методов использования цифровых двойников с целью обеспечения информационной безопасности киберфизических систем.*

Методология проведения работы*. При проведении исследований использовался системный анализ для анализа области применения цифровых двойников, их классификаций и моделей взаимодействия. При разработке прототипа цифрового двойника использовались математические модели, основанные на теории автоматов.*

Результат: *в результате исследования были рассмотрены понятия киберфизической системы и цифрового двойника, приведены существующие методы обеспечения информационной безопасности киберфизических систем, получены методы, повышающие информационную безопасность при синхронизации цифрового двойника и киберфизической системы, рассмотрены этапы обеспечения информационной безопасности с использованием цифрового двойника, причины преимущества цифрового двойника для промышленности, а также существующие протоколы по которым киберфизические системы взаимодействуют с киберпространством.*

Область применения результатов*. Полученные результаты не противоречат существующим нормативным документам по защите КИИ и могут быть использованы для повышения эффективности систем защиты информации в КИИ на этапах их проектирования и мониторинга работы.*

Научная новизна*. Предложена концептуальная модель цифровых двойников и классификация решаемых ими задач. Разработана модель цифрового двойника для проектирования систем управления информационной безопасностью.*

Ключевые слова: *синхронизация, концептуальная модель, конечные автоматы, критическая информационная инфраструктура.*

USING DIGITAL TWINS TO ENSURING INFORMATION SECURITY OF CYBERPHYSICAL SYSTEMS

Vodopyanov A. S.[2]

Purpose of the study *– the work is devoted to the study of methods for using digital twins to ensure information security of cyber-physical systems.*

Methodology of work*. When conducting research, system analysis was used to analyze the scope of digital twins, their classifications and interaction models. When developing a digital twin prototype, mathematical models based on automata theory.*

Result: *as a result of the study, the concepts of a cyber-physical system and a digital twin were considered, existing methods for ensuring information security of cyber-physical systems were given, methods were obtained that increase information security when synchronizing a digital twin and a cyber-physical system, the stages of ensuring information security using a digital twin were considered, the reasons for the advantages of a digital a double for industry, as well as existing protocols by which cyber-physical systems interact with cyberspace.*

Scope of application of the results*. The results obtained do not contradict existing regulatory documents on the protection of computer information systems and can be used to improve the efficiency of information security systems in computer information systems at the stages of their design and monitoring of operation.*

Scientific novelty*. A conceptual model of digital twins and a classification of the problems they solve are proposed. A digital twin model has been developed for the design of information security management systems.*

Keywords: *synchronization, conceptual model, finite state machines, critical information infrastructure.*

1 Водопьянов Александр Сергеевич, консультант Управления Федеральной службы по техническому и экспортному контролю Российской Федерации по Центральному федеральному округу. Москва, Россия. E-mail: AlexandrALex2024@yandex.ru

2 Alexander S. Vodopyanov, Consultant of the Office of the Federal Service for Technical and Export Control of the Russian Federation in the Central Federal District. Moscow, Russia. E-mail: AlexandrALex2024@yandex.ru.

Введение

Прогресс в сфере информационных и телекоммуникационных технологий дал старт новой (информационной) эпохе и появлению нового (информационного) общества, в котором информация и связь приобретают доминирующую ценность. В ходе развертывания информационной эпохи происходит формирование новой парадигмы влияния информационно-телекоммуникационных технологий на развитие самых разных отраслей промышленности, экономики и общества в целом.

Но вместе с прогрессом появляются и новые угрозы безопасности информации, они представляются в виде использовании различных новых методов хищения информации, использования новых типов вредоносного программного обеспечения, хакерских атаках, подмены результатов работы систем и их компонентов и многого другого. В том числе эти риски выражаются в киберфизических системах, имеющих в себе не только повседневные технологии, но и уникальные (особенные) методы и принципы работы, не задействованные нигде более, кроме как в данных решениях.

Работа киберфизических систем спасает жизни и обеспечивает устойчивое развитие экономики государства уже сегодня, но без должного уровня обеспечения их информационной безопасности, они могут представлять большую угрозу.

Существующие методы защиты киберфизических систем

Понятие киберфизических систем часто рассматривают совместно с понятием систем интернета вещей. Оба типа систем имеют схожие элементы, однако киберфизические системы являются более широким понятием и имеют более сложную архитектуру [4]. Киберфизическая система – это система, которая может эффективно интегрировать кибер- и физические компоненты, используя современные сенсорные, вычислительные и сетевые технологии [7].

Главная схожесть архитектур заключается в том, что на нижнем уровне киберфизических систем и систем интернета вещей лежит сенсорная сеть. Сенсорная сеть представляет собой динамическую, самоорганизующуюся и распределенную сеть датчиков и исполнительных устройств. Она предназначена для решения задач автоматизации, диагностики, телеметрии и межмашинного взаимодействия. Значительное внимание уделяется также прикладным возможностям киберфизических систем, позволяющим эффективно связывать объекты физического мира – производственные системы, транспортные средства, объекты энергетики, – с киберфизическим миром через вычислительные, информационно-коммуникационные сети, формируя единую информационно-управляющею среду [8].

Защита киберфизических систем строится в основном на защите стека технологий, лежащих в её основе, это мониторинг и анализ трафика элементов киберфизической системы, применение на её элементах механизмов идентификации, аутентификации и управления доступом, а также использование более стойких алгоритмов криптографической защиты информации, эти решения имеют высокую надёжность как метод защиты, но при этом могут оказывать в том числе и негативное влияние на целостность и доступность элементов киберфизических систем.

Традиционные средства защиты, такие как межсетевые экраны, средства антивирусной защиты, средства обнаружения и предотвращения вторжений и др., часто эффективны не в полной мере для защиты IoT-инфраструктуры из-за того, что трафик, генерируемый системой специфичен и сложен в анализе, а устройства взаимодействуют напрямую друг с другом.

Киберфизические системы могут получать доступ к киберпространству по различным сетевым протоколам, таким как Wi-Fi, WiMAX, GPRS и технологиям 3G/4G/LTE. Другие облегченные протоколы, такие как MQTT, CoAP, AMQP, Websocket, Node используются для передачи данных с периферийных устройств в облако для дальнейшего хранения и обработки. Каждый протокол имеет свои преимущества перед другими в зависимости от скорости, задержки, пропускной способности, надежности, безопасности и масштабируемости [9].

В общем виде система обнаружения вторжений для киберфизических систем осуществляет сбор трафика или его статистики и сравнивает собранные данные с эталоном, и любое отклонение от эталона может свидетельствовать об атаке [2]:

- изменение количества узлов в сети – это напрямую указывает на наличие нелегитимного узла;
- изменение уровня мощности сигнала узла – резкое изменение уровня принимаемого сигнала может свидетельствовать о подмене передающего узла;
- изменение маршрутов доставки данных – большинство киберфизических систем имеют ячеистую топологию, а одним из критериев выбора маршрута доставки является качество сигнала. Поэтому изменение маршрута может быть вызвано добавлением нового узла или подменой существующего, а соответственно, и влиянием на качество передачи;
- увеличение или уменьшение числа кадров, изменение типа трафика – в киберфизических системах узлы генерируют, как правило, однотипный трафик, поэтому изменение количества трафика

и его типа, например рост числа служебных пакетов, может указывать на присутствие злоумышленника;
- ухудшение характеристик производительности сети – снижение пропускной способности, увеличение задержек также может указывать на присутствие злоумышленника в системе;
- уменьшение или увеличение времени реакции на запросы – данный факт может указывать на подмену легитимного узла, например, более производительным устройством, в случае более быстрой реакции на запросы;
- изменение временных периодов отправки данных – узлы.

Каждый параметр отклонения в отдельности может давать ложный результат, поэтому их следует использовать в совокупности, но это усложняет задачу защиты киберфизических систем.

Использование цифрового двойника для обеспечения информационной безопасности киберфизических систем

Термин «цифровой двойник» появился более десяти лет назад и до сих пор не имеет четкого определения. Тем не менее интерес к этому направлению постоянно возрастает и особенно в тех областях, где много неформализуемых задач, нечетких значений параметров, случайных и непредвиденных ситуаций в автоматизированных системах управления, критических информационных инфраструктурах и социально значимых информационных системах. DT во многом могут решать часть этих задач на этапах проектирования, внедрения и мониторинга этих систем [5].

Использование цифровых двойников, является также одним из новых подходов в обеспечении информационной безопасности киберфизических систем.

Среди основных преимуществ цифровых двойников для промышленности [6] отметим, что они:

- позволяют реализовать дистанционный мониторинг и управление физическим объектом в реальном времени (РВ) там, где это невозможно другими средствами;
- обеспечивают большую автономию персонала в случае необходимости, таким образом повышая эффективность и безопасность производства, что особенно ценно с учетом опыта пандемии 2020 г.;
- создают условия для предиктивного обслуживания и планирования ремонтов оборудования за счет обработки и интеллектуального анализа в РВ больших объемов данных о работе промышленных активов;
- делают возможным анализ производственных сценариев и оценку риска путем проигрывания нештатных ситуаций без ущерба для реального производства;
- поддерживают и ускоряют принятие решений за счет расширенной аналитики данных в РВ;
- упрощают документирование и коммуникации, используя легкодоступную on-line информацию, и в сочетании с автоматизированной отчетностью повышают прозрачность бизнес-процессов.

Следовательно, при рассмотрении взаимодействия между технологическими процессами предприятия и процессами управления информационной безопасности, специалист по защите информации нуждается в исследовании обратной связи.

Технология цифровых двойников может позволить собирать цифровые следы с учётом уровня информационного риска при эмпирически определённых ситуациях.

Это может быть реализовано в форме имитационных моделей, обучающихся на основе сценариев реального использования с учетом особенностей технологического процесса и накопленных оперативных данных, а также виртуальных или аппаратных лабораторных стендах.

Цифровой двойник может быть как подключен к системе напрямую, обмениваясь с ней данными, так и использоваться в асимметричной схеме, когда обмен данными происходит в оговоренном заранее дискретном временном режиме.

Обеспечение безопасности с использованием технологии цифрового двойника гибкое и может проводиться на всех этапах жизненного цикла, позволяя моделировать различные события безопасности.

На этапе создания, это возможность изучения безопасного дизайна, обнаружения неправильной конфигурации программного обеспечения и тестирования механизмов безопасности [3].

На этапе эксплуатации, цифровой двойник может позволить обнаруживать вторжения, внедрять механизмы аутентификации, идентификации и использовать криптостойкие алгоритмы шифрования, без дополнительной нагрузки на физическую систему.

На этапе вывода из эксплуатации, цифровой двойник может помочь сохранять конфиденциальность информации в киберфизической системе.

В отличии от тех же «песочниц», использование цифрового двойника может усилить контроль за безопасностью киберфизических систем по следующим причинам:

1. Цифровой двойник может быть спроектирован таким образом, чтобы оставаться активным, не изолируя реальную среду на определённое время t, с встроенными функциями изоляции тупиковых областей тестирования.

2. Обладать свойствами размножения (ветвления) потоков команд и данных для параллельного изучения поведения (анализа) в сегментах двойника.
3. Быть не единственным и иметь «клонов» для реализации при защите информационной инфраструктуры метода «медовых ловушек».
4. Заставлять работать систему в условиях со смещённым временем, для анализа угроз, связанным со срабатыванием по времени.

Основными данными при обеспечении безопасности киберфизической системы может быть [10]:

- ❖ первичное измерительное оборудование (датчики и приборы);
- ❖ преобразование измеряемых параметров в цифровой формат;
- ❖ достаточная вычислительная мощность и хранилище данных;
- ❖ совершенная сетевая инфраструктура;
- ❖ внедрение предиктивной аналитики, позволяющей отслеживать и диагностировать состояния системы, а также прогнозировать возможные сбои.

При этом на всех этапах необходимо и контролировать выполнение требований о защите информации, а именно:

- ❖ к процессу хранения, передачи и обработки защищаемой в киберфизической системе информации;
- ❖ к киберфизической системе;
- ❖ к взаимодействию киберфизической системы с цифровым двойником;
- ❖ к условиям функционирования киберфизической системы;
- ❖ к содержанию работ по созданию (модернизации) киберфизической системы на различных стадиях и этапах ее создания (модернизации);
- ❖ к организациям (должностным лицам), участвующим в создании (модернизации) и эксплуатации киберфизической системы;
- ❖ к документации на киберфизическую систему.

Усилить безопасность взаимодействия цифрового двойника и киберфизической системы может, к примеру синхронизация в определённый период времени, что может снизить возможности злоумышленника при проведении целевых компьютерных атак на инфраструктуру [1].

Если описать данный метод с использованием конечных автоматов, то взаимодействие киберфизической системы и цифрового двойника представляется отношением элементов системы к их проекции в домене ($C \in X$).

Следовательно, значимые состояния элементов системы и их проекций в домене можно представить как множество этих состояний $S_c = \{S_{c0}, S_{c1}, S_{c2}, \ldots, S_{cn-1}\}$, $S_x = \{S_{x0}, S_{x1}, S_{x2}, \ldots, S_{xm-1}\}$, при этом значимых состояний двойника будет меньше, чем состояний физической системы ($n>m$), по причине того, что физическая часть системы остаётся главным контроллером домена цифрового двойника.

Множествами представляются и входные данные для физической системы и её цифрового двойника $I_c = \{I_{c0}, I_{c1}, \ldots, I_{cp-1}\}$, $I_x = \{I_{x0}, I_{x1}, \ldots, I_{xp-1}\}$.

При проведении синхронизации данных и контроля в период времени t, ключевое состояние киберфизической системы примет следующий вид: $S_{c,t} \in S_c$, следовательно такое же состояние примет и цифровой двойник $S_{x,t} \in S_x$. Входные данные также изменят своё состояние и будут представлены в следующем виде: $I_{c,t} \in I_c$ и цифровой двойник $I_{x,t} \in I_x$. Следовательно, можно вывести что начальные состояния киберфизической системы и цифрового двойника это $S_{c,0}$ и $S_{x,0}$.

Исходя из всего вышесказанного функции переходов выглядят как прямое произведение групп ключевых состояний и входных данных системы: $\delta_c: S_c \times I_c \longrightarrow S_c$ и $\delta_x: S_x \times I_x \longrightarrow S_x$.

Для обеспечения необходимого уровня их защиты при синхронизации, в предложенной схеме необходимо использовать шифрование по времени $t\ e_c \longrightarrow e_x$ или $e_x \longrightarrow e_c$.

Таким образом, полученный автомат можно увидеть на рисунке 1.

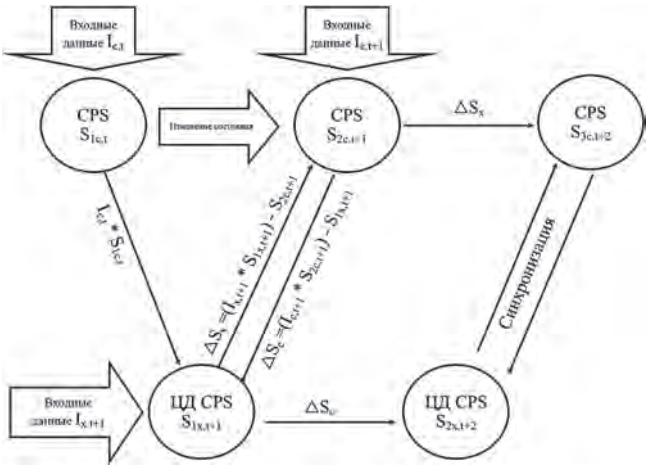


Рис. 1. Структура конечного автомата, двунаправленного порядка

Перед первой синхронизацией оператор отправляет ввод данных I_c в физический двойник

и система принимает первое ключевое состояние S_{1c}, следовательно в цифровом двойнике нет пока такого же состояния, после синхронизации, цифровой двойник получает на вход данные физической системы I_c и на основе её состояния S_{1c} принимает своё первое ключевое состояние S_{1x}.

В следующем временном интервале t+1, первое ключевое состояние цифрового двойника S_{1x} должно быть равно первому ключевому состоянию физической системы S_{1c} и когда физическая система получает на вход новую партию данных I_c она вычисляет разницу ΔS_c и отправляет её в цифровой двойник, который на её основе переходит уже в своё следующее ключевое состояние.

При двунаправленном обмене данными, оператор может подать набор данных I_x в цифровой двойник, тогда уже цифровой двойник будет использовать их для получения первого ключевого состояния S_{1x} и вычисления разницы необходимой для перехода физической системы в её новое состояние ΔS_x.

Следовательно, в момент времени t+2, если входных данных нет, ключевые состояния физической системы и цифрового двойника могут остаться прежними.

Если представить, что взаимодействие киберфизической системы и цифрового двойника однонаправленное (Рисунок 2), то мы получим другую структуру автомата. В этом случае синхронизация не потребуется, следовательно физическая система будет только передавать данные цифровому двойнику, что не позволит получить доступ из сети к физической системе злоумышленником.

Следовательно функция перехода будет выглядеть следующим образом: δ_c: $S_c \times I_c \longrightarrow S_c$ и δ_x: $S_c \times I_c \longrightarrow S_c$, $n = m$ так как домен для синхронизации не используется и оператор может только снимать показания телеметрии.

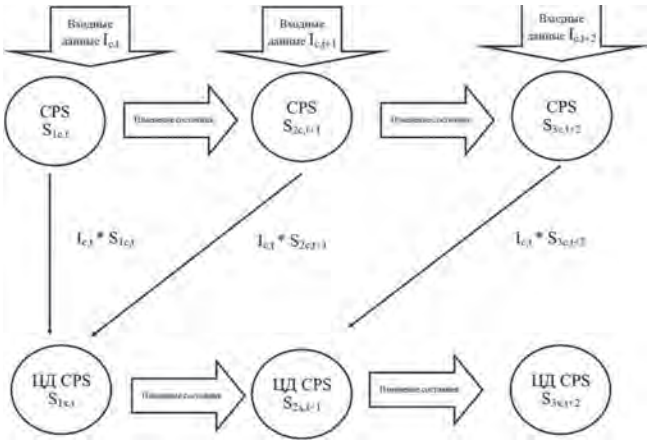


Рис. 2. Структура конечного автомата однонаправленного порядка

Вывод

Концепция цифровых двойников представляется новым направлением исследований в области информационной безопасности. На данный момент опубликовано лишь несколько статей, которые поверхностно касаются того, что может казаться возможным с использованием технологии цифровых двойников. Данный способ обеспечения безопасности киберфизических систем, с использованием технологий цифрового двойника лишь один из многих и позволяет немного повысить уровень защищённости при эксплуатации киберфизических систем, проблема данного решения заключается в сложности интеграции дополнительных модулей в поставляемое оборудование и их обслуживании.

Литература

1. *G. Lampropoulos, Kerstin V. Siakas – Enhancing and securing cyber-physical systems and Industry 4.0 through digital twins // A critical review July 2022Journal of Software: Evolution and Process 35(2011), DOI:10.1002/smr.2494.*
2. *M. Eckhart, A. Ekelhart – Digital Twins for Cyber-Physical Systems Security: State of the Art and Outlook // Security and Quality in Cyber-Physical Systems Engineering (pp.383–412), 2019. DOI:10.1007/978-3-030-25312-7_14.*
3. *Richard J. Somers, James A. Douthwaite, David J. Wagg, Neil D. Walkinshaw – Digital-twin-based testing for cyber–physical systems: A systematic literature review // Information and Software Technology Volume 156, 2022. DOI: 10.1016/j.insof.2022.107145.*
4. *Кушко Е. А., Грачёв Д. А., Паротькин Н. Ю., Золотарёв В. В. О вопросах безопасности киберфизических систем // Доклады Томского государственного университета систем управления и радиоэлектроники. 2022. № 4, том 2, С. 101–109 DOI: 10.21293/1818-0442-2022-25-4-101-109.*
5. *Минзов А. С., Невский А. Ю., Баронов О. Р., Немчанинова С.В. Цифровые двойники в системах управления // Вопросы кибербезопасности 2024 № 2(60). С.29–35. DOI: 10.21681/2311-3456-2024-2-29-35.*
6. *Дозорцев В. М. – Цифровые двойники в промышленности: генезис, состав, терминология, технологии, платформы, перспективы. Часть 1. Возникновение и становление цифровых двойников. Как существующие определения отражают содержание и функции цифровых двойников? // Автоматизация в промышленности DOI: 10.25728/avtprom.2020.09.01.*
7. *Расим Алгулиев, Ядигар Имамердиев, Людмила Сухостат – Обеспечение Информационной Безопасности Киберфизических Систем // Proqram mühəndisliyinin aktual elmipraktikiproblemləri. I respublika konfransı Bakı, 17 may 2017-ci il DOI: 10.25045/NCSoftEng.2017.07*
8. *Шкодырев В. П. Киберфизические системы как технологическая платформа синергетической интеграции перспективных прорывных технологий // Системный анализ в проектировании и управлении. 2020. DOI:10.18720/SPBPU/2/id20-109.*
9. *Смышляева А. А., Резникова К. М., Савченко Д. В. Современные технологии в Индустрии 4.0 – киберфизические системы // Интернет-журнал «Отходы и ресурсы», 2020. №3, DOI: 10.15862/02INOR320.*
10. *Мехтиев Ш. А. Анализ некоторых проблем надежности киберфизических систем // Информационные технологии в науке, образовании и производстве. 2022. №18(1). С. 42–47. DOI: 10.25045/NCInfoSec.2017.06.*

ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ ДЛЯ ГЛОБАЛЬНОГО МИРА

Стрельцов А. А.[1]

DOI: 10.21681/2311-3456-2024-4-145-147

Книга «**Информационно-коммуникационные технологии для глобального мира**»[2] подготовлена коллективом высококвалифицированных авторов на актуальную тему, связанную с воздействием достижений науки и технологий на систему международных отношений, мировую экономику, глобальную и национальную безопасность[3]. Информационно-коммуникационные технологии представляют собой инновацию эпохального значения, которая формирует новый этап научно-технологического прогресса, в основе которого лежит информационная трансформация техносферы. Данная проблематика является приоритетной в повестке дня международной политики и двусторонних отношений Российской Федерации.

Выпуск данной коллективной монографии приурочен к 80-летию образования МГИМО и 75-й годовщине установления дипломатических отношений с КНР. Книга продолжает серию публикаций в контексте объявленного президентом России Десятилетия науки и технологий. В течение последних лет МГИМО и Дипакадемией изданы учебники «Международная информационная безопасность: теория и практика», «Научно-технологический прогресс и современные международные отношения», «Международная безопасность в эпоху искусственного интеллекта».

Обращает на себя внимание сложность темы монографии «Информационно-коммуникационные технологии для глобального мира», потребовавшей синтеза знаний гуманитарных и технических наук, что обусловило привлечение к совместной работе профессоров и специалистов МГИМО и его подразделения Центра международной информационной безопасности и научно-технологической политики, Санкт-Петербургского государственного экономического университета и Института международного управления искусственным интеллектом Университета Цинхуа, а также ученых академических институтов и работников дипломатической службы России. Участие в подготовке материалов монографии экспертов России и Китая позволило представить проблематику воздействия ИКТ на международную жизнь максимально детально и глубоко

Структура книги представляется достаточно логичной и охватывающей все наиболее актуальные аспекты темы, связанные с цифровизацией мирового развития и международных отношений.

Первый раздел «Современный научно-технологический прогресс» состоит из четырех глав. В первой главе рассмотрены этапы, модели и тенденции НТП и отмечается, что современный научно-технологический прогресс характеризуют глобализация, информатизация, цифровая трансформация, доминирование высоких технологий и социально ответственных инноваций, а также масштабные научные исследования с опорой на мощный технический инструментарий. Также весьма актуальным является вклад авторов в понимание феномена технологического суверенитета.

Во второй и третьей главах рассмотрены все основные технологии, основанные на или содержащие компоненты ИКТ. Из анализа представленных материалов вытекает, что новые поколения информационно-коммуникационных технологий присутствуют практически во всех аспектах техносферы и жизнедеятельности человека.

При этом сильной стороной монографии на наш взгляд является развернутое рассмотрение прикладных аспектов информационной революции типа роста социальных сетей, цифровой трансформации государственного и муниципального управления, обработки больших данных, а также организации коммуникации и связи, транспорта, банковского дела, образования и других сфер активности человека с использованием технологических и социальных инноваций.

Особенное внимание уделено технологической квинтэссенции – технологии искусственного интеллекта как разновидности ИКТ. Учитывая быстрое расширение сферы применения этой технологии и связанные с ней возможности, вызовы и риски эти вопросы рассмотрены весьма подробно. В частности, раскрыт потенциал технологии искусственного интеллекта, сферы и направления её применения, а также возрастающая роль в развитии общества,

1 Стрельцов Анатолий Александрович, доктор технических наук, доктор юридических наук, профессор, Вице-президент Национальной ассоциации международной информационной безопасности, ведущий научный сотрудник Центра проблем информационной безопасности факультета «Вычислительная математика и кибернетика» МГУ имени М. В. Ломоносова, Москва, Россия. E-mail: aa.streltsov@yandex.ru

2 Информационно-коммуникационные технологии для глобального мира / Под общ. ред. О. А. Мельниковой, рук. проекта А. В. Крутских. М.: Издательство «Аспект Пресс». 2024. — 542 с.

3 На 2-й обложке нашего журнала редакция поместила изображение рецензируемой книги

бизнеса и управления в государственных делах. Растет число стран (свыше 60), взявших на вооружение национальные стратегии искусственного интеллекта. Всё большее внимание уделяется использованию этой технологии в военных целях.

Самостоятельная глава посвящена проблематике биотехнологий в контексте информатизации и цифровой трансформации. Широкий спектр решаемых задач социально-экономического, политического и экологического развития вывел биотехнологию за рамки научно-технологического направления и превратил в фактор глобального социально-экономического и политического влияния

Важно отметить, что в монографии присутствует также рассмотрение социально-гуманитарных технологий, причем акцентируется мысль, что человек, участвующий в развитии НТП и международных научно-технологических отношений, должен быть не просто образованным и законопослушным, но и приверженным научным принципам и соблюдать требования цифровой эпохи, а также быть адаптированным к ситуации постоянного техногенного воздействия.

Во втором разделе «Международные отношения в цифровую эпоху» отмечаются рост международной напряженности, связанный с переходом от гегемонии США вместе с сателлитами в направлении многополярного мира, становлению политического полицентризма и кризиса навязываемых Западом ценностей ценностей и идеологии государств, бывших в свое время колониальными державами, которые пытаются сохранить в новых формах хищнические подходы к странам «мирового большинства».

Особое внимание авторы раздела уделили гибридной войне нового поколения, развязанной «коллективным Западом» против России, Китая и ряда других членов ШОС и БРИКС с использованием высоких гуманитарных, когнитивных и социально-психологических технологий, разработанных с учетом достижений ИКТ. В результате усилий западных стран во главе с США современный мир погрузился в атмосферу лжи и обмана, которые камуфлируются «благими» намерениями и целями. В действительности объектами тотальной гибридной войны со стороны Запада являются воля, ментальность и сознание элит и других социальных групп, а также конкретных людей и народов Глобального Востока и Глобального Юга.

С учетом реалий гибридной войны расширяется фронт обеспечения международной информационной безопасности. Эта тема рассматривается в отдельной главе в контексте организованного Россией дискурса в ООН и международных организаций системы ООН, а также на площадках региональных организаций. Представляются важными критические оценки конкретных шагов западных государств, направленные на подрыв позитивных процессов диалога и сотрудничества, реализуемых единомышленниками России в рамках Группы правительственных экспертов и Рабочей группы открытого состава ООН.

Цифровая эпоха принесла также угрозы, обусловленные техно-гуманитарным дисбалансом, при котором переоценивается оптимальность технологических решений и уделяется недостаточное внимание человеку и его интересам, грамотной социализации, образованию и воспитанию. Например, создание электронных мегаструктур в условиях олигопольного монополизма и отсутствия честной конкуренции создает предпосылки техногенных катастроф. В течение последних лет современный мир испытал несколько подобных аварий. Последняя из них случилась совсем недавно и связана с деятельностью американской компании CrowdStrike в отношении монопольного провайдера информационных услуг Windows цифрового гиганта Microsoft.

К числу традиционных угроз современности относятся кибертерроризм и киберпреступность. Это сложные феномены требуют особого контроля и противодействия в силу гигантского экономического и политического урона человечеству, который они несут. Заслуживают внимания рассмотренные в соответствующей главе методы борьбы Интерпола и национальных правоохранительных органов с указанными вредоносными практиками.

Третий раздел «Вклад России в глобальную цифровизацию» посвящен месту России в глобальной цифровизации и государственной политике нашей страны в области обеспечения международной информационной безопасности.

Российская Федерация придает ключевое значение комплексному осмыслению и освоению всей проблематики внедрения высокотехнологичных решений. При Президенте страны действует Совет по науке и образованию, который решает упомянутые задачи. Такой подход позволяет обеспечивать подлинную технологическую независимость с опорой на национальные интересы, способствует укреплению лидерских позиций страны по целому ряду научных направлений. Для его реализации упор делается на эффективность и продуктивность технологий и на обеспечение доверия к технологиям.

Основные направления научно-технологического развития Российской Федерации нашли свое отражение в соответствующей Стратегии, утвержденной в 2024 году Президентом Путиным. Президент России считает чрезвычайно важным «собрать в единый кулак весь наш научный, технологический,

образовательный и производственный потенциал» и призывает обеспечить технологическое лидерство России.

С целью создания условий для такого лидерства руководство страны предпринимает комплексные меры по актуализации действующих и утверждению новых направлений в области цифровой трансформации всех отраслей экономики, социальной сферы и бизнеса. Существенной предпосылкой лидерства являются не только прорывные передовые технологии, но и инновационные подходы к системе образования и обучения кадров. Этому вопросу уделяется самое серьёзное внимание в технических и гуманитарных вузах страны.

По нашему мнению, большого внимания заслуживает последний раздел монографии «КНР в процессе мировой цифровой революции». Он написан представителями университета Цинхуа, который в соответствии с международными рейтингами признается лучшим техническим вузом Азии.

Подготовленные китайскими экспертами главы представляют собой уникальный материал, раскрывающий организацию и правовое регулирование в КНР информационного общества, акцентированное развитие национального потенциала в области искусственного интеллекта и связи пятого поколения, передовой опыт строительства цифровой экономики, крупных цифровых корпораций, сопоставимых с американскими цифровыми гигантами, а также формирование инфраструктуры национального интернета, позволяющей ограничить негативное воздействие системы «всемирной паутины», контролируемой США, а также создать барьеры с точки зрения преодоления негативных последствий информационной лавины, накрывшей человечество.

Авторы обоснованно привлекают внимание читателей к ряду серьезных идей Китая – Международной инициативе сотрудничества в области цифровой экономики – «Один пояс, один путь», Глобальной инициативе по обеспечению безопасности данных и Проекту создания сообщества единой судьбы в киберпространстве.

При понимании, что в СНГ и БРИКС реализуется концепция единого научно-технологического пространства, Россия в ходе председательства в этих структурах могла бы в число собственных инициатив включить проект распространения в университетах стран-членов этих объединений монографии «Информационно-коммуникационные технологии для глобального мира» и других упомянутых в рецензии книг МГИМО и Дипакадемии. Считаю, что студенты в государствах «глобального большинства» с интересом воспримут изложенную в этих книгах позицию лидеров многополярного мира России и Китая по актуальным вопросам международной жизни.

DOI:10.21681/2311-3456-2024-4-145-147

CYBERSECURITY ISSUES

SCIENTIFIC PEER-REVIEWED JOURNAL

2024, № 4 (62)

Cybersecurity Issues is a research periodical scientific and practical publication specializing in information security.
Published six times a year

https://cyberrus.info

The journal is being published from 2013 (Registration Certificate PI No. FS 77-75239).
CrossRef number (DOI): 10.21681/2311-3456

The journal is included in the Russian list of peer-reviewed academic publications of the Higher Attestation Commission (VAK), it is registered in the Russian Science Citation Index (RSCI/RINTs) on the Web of Science (WoS) platform and holds the 1st place in its cyber security rating. The journal's articles are available in full text

Founder and publisher
JSC «NPO «Echelon»
Postal address: Elektrozavodskaya str., 24, bld. 1, 107023, Moscow, Russia
E-mail: editor@cyberrus.info

CONTENTS

SAFE ARTIFICIAL INTELLIGENCE

PROMISING DIRECTIONS FOR APPLYING ARTIFICIAL INTELLIGENCE TECHNOLOGIES IN INFORMATION PROTECTION
Meshcheryakov R. V., Melnikov S. Yu., Peresypkin V. A., Horev A. A. 2

THEORETICAL FOUNDATIONS OF INFORMATICS

PREDICTING THE SIZE OF THE SOURCE CODE OF A BINARY PROGRAM IN THE INTERESTS OF ITS INTELLECTUAL REVERSE ENGINEERING
Izrailov K. E. 13

APPLICATION OF THE LOGICAL-PROBABILISTIC METHOD IN INFORMATION SECURITY. Part 5
Kalashnikov A. O., Anikina E. V., Bugajskij K. A., Birin D. S., Deryabin B. O., Tsependa S. O., Tabakov K. V. 26

CYBERSECURITY TESTING AND MONITORING

METHOD FOR ENSURING COMPATIBILITY OF TECHNICAL COMPONENTS WHEN CREATING A SYSTEM FOR MONITORING INFORMATION SECURITY INCIDENTS
Devitsyna S. N., Pilkevich P. V. 38

METHODS AND MEANS OF CODING

ANALYSIS REQUIREMENTS OF APPLICATION AND TECHNOLOGICAL CAPABILITIES OF RADIO SIGNALS, PROMISING FOR 6G NETWORKS
Baraboshin A. Y., Luchin D. V., Maslov E. N. 45

CRYPTOGRAPHIC METHODS OF PROTECTION

ANALYSIS OF EXISTING APPROACHES TO THE SYNTHESIS OF PSEUDO-DYNAMIC SBOX
Prudnikov V. A. 57

OPTIMIZATION OF COMPUTATIONS OVER POLYNOMIALS IN POST-QUANTUM SIGNATURE SCHEME
Ivanenko V. G., Ivanova I. D., Ivanova N. D. 65

APPLICATION OF CODING AND CRYPTOGRAPHY METHODS

A METHOD FOR STRENGTHENING SIGNATURE RANDOMIZATION IN SIGNATURE ALGORITHMS ON NON-COMMUTATIVE ALGEBRAS
Moldovyan D. N., Kostina A. A. 71

SECURITY OF THE META-INTERNET

STRUCTURAL AND FUNCTIONAL ANALYSIS OF THE CONFLICT SITUATION BETWEEN THE STATE INFORMATION SECURITY SYSTEM AND A FOREIGN SYSTEM OF DESTRUCTIVE INFLUENCES
Starodubtsev Yu. I., Zakalkin P. V. 82

INFORMATION SECURITY RISK MANAGEMENT

DETECTING WEB ATTACKS USING MACHINE LEARNING ALGORITHMS
Lapina M. A., Movzalevskaya V. V., Tokmakova M. E., Babenko M. G., Sajid M. 92

CRITICAL INFORMATION INFRASTRUCTURE SECURITY

ALGORITHM FOR SIMULATING DYNAMIC TRAFFIC CHARACTERISTICS WEB SERVICE
Gorbachev A. A., Lysenko D. E. 104

METHODS OF MATHEMATICAL MODELING

DEVELOPMENT OF A HARDWARE AND SOFTWARE SYSTEM FOR MODELLING MULTI-LABELED COMPUTER ATTACKS
Sheluhin O. I., Rakovskiy D. I. 116

ALGORITHM FOR ASSESSING THE LEVEL OF DIGITAL AUTONOMY OF DIGITAL SPACE INFRASTRUCTURE COMPONENTS
Ryzhenko A. A., Seleznev V. M. 131

CRITICAL INFORMATION INFRASTRUCTURE SECURITY

USING DIGITAL TWINS TO ENSURING INFORMATION SECURITY OF CYBERPHYSICAL SYSTEMS
Vodopyanov A. S. 140

REVIEWS

INFORMATION & COMMUNICATION TECHNOLOGIES FOR A GLOBAL WORLD
Streltsov A. A. 145

ОСНОВЫ ТЕОРИИ СОСТАВНЫХ СЕТЕЙ ПЕТРИ – МАРКОВА И ИХ ПРИМЕНЕНИЯ ДЛЯ МОДЕЛИРОВАНИЯ ПРОЦЕССОВ РЕАЛИЗАЦИИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

Вышла в свет монография известных специалистов в области информационной безопасности.

АВТОРЫ:

Язов Юрий Константинович: доктор технических наук, профессор, главный научный сотрудник Государственного научно-исследовательского испытательного института ФСТЭК России, автор более 330 научных трудов, включая 10 монографий. Сферой научных интересов является аналитические моделирование процессов реализации угроз безопасности информации в информационных системах и организация защиты информации от них.

Анищенко Александр Владимирович: доктор технических наук, старший научный сотрудник, начальник Государственного научно-исследовательского испытательного института ФСТЭК России, автор более 200 научных трудов, включая 6 монографий, по защите информации от ее перехвата техническими средствами.

Суховерхов Александр Сергеевич: кандидат технических наук, доцент, начальник управления Государственного научно-исследовательского испытательного института ФСТЭК России, автор более 50-ти научных трудов. Сферой научных интересов является исследование перспективных способов и средств защиты объектов критической информационной инфраструктуры от угроз безопасности информации.

Монография посвящена актуальным вопросам разработки методологии количественной оценки возможностей реализации угроз безопасности информации в информационных системах от несанкционированного доступа. Сегодня для этого используются экспертные процедуры, что обусловливает невозможность учета фактора времени, то есть динамики реализации угроз как без применения, так и в условиях применения мер защиты от них. В монографии показывается необходимость моделирования указанной динамики и дается сравнительный анализ возможностей применения для этого аппаратов марковских, полумарковских процессов, традиционных сетей Петри – Маркова, а также нового, практически не применявшийся ранее для моделирования стохастических процессов, в том числе процессов реализации угроз в информационных системах, аппарата составных сетей Петри – Маркова, позволяющего учитывать не только временной фактор и параллельность выполнения парциальных процессов в ходе реализации угроз, но и логические условия такой реализации. Приведены многочисленные примеры моделей с аналитическими соотношениями для расчета вероятностно-временных характеристик процессов реализации угроз. Описывается целый ряд расширений аппарата составных сетей Петри – Маркова, таких как введение предикатных условий срабатывания логических переходов, назначение приоритетов для парциальных процессов, использование ингибиторных дуг, введения нечетких вероятностно-временных характеристик парциальных процессов, что существенно повышает его моделирующие возможности.

Монография предназначена для специалистов, занимающихся вопросами моделирования процессов реализации угроз безопасности информации в информационных системах или смежными исследованиями в этой области, для преподавателей, а также для аспирантов, студентов и слушателей, обучающихся по данной тематике.

ISBN: 978-5-6052111-2-9. —

https://doi.org/10.32415/scientia_978-5-6052111-2-9

Издательский дом «Сциентиа», Санкт-Петербург, 2024

CYBERSECURITY ISSUES
VOPROSY KIBERBEZOPASNOSTI

№4 2024

DOI: 10.21681/2311-3456

- Safe Artificial Intelligence
- Binary source size prediction
- Digital twins for information security

www.cyberrus.info
edItor@cyberrus.Info