МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ "МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ
УНИВЕРСИТЕТ ИМЕНИ Н.Э.БАУМАНА
(НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ)"

«БЕЗОПАСНЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ»

МЕЖДУНАРОДНАЯ
НАУЧНО-ТЕХНИЧЕСКАЯ КОНФЕРЕНЦИЯ

(Москва, 1-2 ноября 2023 года)

СБОРНИК ТРУДОВ КОНФЕРЕНЦИИИ

МГТУ им. Н.Э.Баумана
НУК «Информатика и системы управления»
МОСКВА-2023

УДК 003.26.7:004.05
ББК 32.937.202
Б31

Б31

Безопасные информационные технологии. Сборник трудов XII международной научно-технической конференции "Безопасные информационные технологии" – М.: МГТУ им. Н.Э.Баумана, 2023. 171 с. – илл.

ISBN 978-5-6045553-8-5

Сборник содержит тезисы докладов, представленных на международной научно-технической конференции "Безопасные информационные технологии" (БИТ-2023), проходившей 1-2 ноября 2023 г. в Москве в МГТУ им. Н.Э.Баумана.

Тезисы публикуются в редакции научных руководителей или в авторской редакции при наличии ученой степени.

Руководители оргкомитета конференции:

Гордин М.В. - председатель оргкомитета, ректор МГТУ им. Н.Э. Баумана, канд. техн. наук;
Пролетарский А.В. – первый зам. председателя оргкомитета, декан факультета «Информатика и системы управления» МГТУ им. Н.Э. Баумана, д-р техн. наук, доцент;
Басараб М.А. – зам. председателя оргкомитета, заведующий кафедрой «Информационная безопасность» МГТУ им. Н.Э. Баумана, д-р физ.-мат. наук;
Марков А.С. – зам. председателя оргкомитета, профессор кафедры «Информационная безопасность» МГТУ им. Н.Э. Баумана, д-р техн. наук, ст. науч. сотр.

Члены организационного комитета:

Булдакова Т.И. — профессор кафедры «Компьютерные системы и сети» МГТУ им. Н.Э. Баумана, д.т.н., профессор;
Дворянкин С.В. — Начальник центра Научно-образовательный центр «Безопасность интеллектуальных киберфизических систем» Института интеллектуальных кибернетических систем НИЯУ МИФИ, д.т.н., профессор;
Жуков И.Ю. — профессор кафедры «Стратегические информационные исследования» НИЯУ МИФИ, д.т.н., профессор;
Петренко С.А. – профессор кафедры безопасности информации Университета Иннополис, д.т.н., профессор;
Шелухин О.И. — заведующий кафедрой информационной безопасности МТУСИ, д.т.н., профессор.

Международный программный комитет

Гордеев Э.Н. — председатель – профессор кафедры «Информационная безопасность» МГТУ им. Н.Э. Баумана, д.ф.-м.н., профессор;
Медведев Н.В. – зам. председателя — доцент кафедры «Информационная безопасность» МГТУ им. Н.Э. Баумана, к.т.н., доцент;
Цирлов В.Л. — зам. председателя — доцент кафедры «Информационная безопасность» МГТУ им. Н.Э. Баумана, к.т.н., доцент;
Кругликов С.В. —генеральный директор ОИПИ НАН Беларуси (Республика Беларусь), д.в.н., профессор;
Бондарев В.В. — доцент кафедры «Информационная безопасность» МГТУ им. Н.Э. Баумана, к.в.н., доцент;
Быков А.Ю. — доцент кафедры «Информационная безопасность» МГТУ им. Н.Э. Баумана, к.т.н., доцент;
Варениса В.В. — доцент кафедры «Информационная безопасность» МГТУ им. Н.Э. Баумана, к.т.н.;
Варфоломеев А.А. — доцент кафедры «Информационная безопасность» МГТУ им. Н.Э. Баумана, к. ф.-м. н, с.н.с.;
Горшков Ю.Г. — доцент кафедры «Информационная безопасность» МГТУ им. Н.Э. Баумана, к.т.н., доцент;
Жуков А.Е. — доцент кафедры «Информационная безопасность» МГТУ им. Н.Э. Баумана, к.ф.-м.н., доцент;
Жуков Д.А. — доцент кафедры «Информационная безопасность» МГТУ им. Н.Э. Баумана, к.ф-м.н.;
Ключарев П.Г. — профессор кафедры «Информационная безопасность» МГТУ им. Н.Э. Баумана, д.т.н.;
Коннова Н.С. — доцент кафедры «Информационная безопасность» МГТУ им. Н.Э. Баумана, к.т.н.;
Пудовкина М.А. — профессор кафедры «Информационная безопасность» МГТУ им. Н.Э. Баумана, д.ф.-м.н.;
Родионов Д.Е. — доцент кафедры «Информационная безопасность» МГТУ им. Н.Э. Баумана, к.т.н.;
Троицкий И.И. — доцент кафедры «Информационная безопасность» МГТУ им. Н.Э. Баумана, к.т.н.

УДК 004.056

ПРИВЕТСТВИЕ КОНФЕРЕНЦИИ

Современные тенденции безопасных информационных технологий

Марков А.С.[1]

В рамках конференции планируется рассмотреть мировые тренды в области информационной безопасности, тенденции безопасных информационных технологий, аспекты прикладных решений и поставить задачи на ближайшую перспективу.

Ключевые слова: информационная безопасность, безопасные информационные технологии, кибербезопасность

Введение

Перед тем как начать научную конференцию, отметим некоторые глобальные тенденции области информационной безопасности, особенности современного противостояния в киберпространстве, отечественный вектор на технологический суверенитет.

Основные тенденции

Проблематика кибербезопасности последние 15 лет устойчиво занимает первые позиции в перечне глобальных технологических рисков человечество. В текущем году, согласно Gartner, кибербезопасность опять в топ-10 стратегических технологических трендов. В рамках Четвертой промышленной революции выделяют в первую очередь тренд на конвергенцию кибербезопасности и прорывных технологий 4ПР (AI/ML, IoT/IIoT/IoE, облака, квантовые вычисления, биометрия, интеграция, визуализация, виртуализация, распределённые реестры, автономные системы и др.). Согласно Gartner Hype Cycle for Emerging Technologies на 10 лет вперед делается прогноз по развитию новых технологических направлений, как-то: устойчивость облачных технологий, смешанная архитектура кибербезопасности, динамическое управление рисками, минимальная жизнеспособная архитектура, технологии искусственного интеллекта (ИИ, AI) для генеративного конструирования безопасных программ и др.

Понятно, что много мировых игроков в области информационной безопасности активизировали свою деятельность - так в текущем году было рекордное число аналитических отчетов – более 15-ти, например[2]:

1. Киберугрозы для АСУ и промышленных предприятий в 2023 году от Лаборатории Касперского.

2. Рынок информационной безопасности: итоги года и прогнозы экспертов на 2023 год от Antimalware.

3.Global Cybersecurity Outlook 2023 от Всемирного экономического форума и Accenture.

4. Cybersecurity Trends: IBM’s Predictions for 2023.

6. Future / Tense: Trend Microsecurity Predictions for 2023.

7. Mandiant Cyber Security Forecast 2023.

8. Watchguard’s 2023 Cybersecurity Predictions.

[1] Марков Алексей Сергеевич, д.т.н., профессор МГТУ им. Н.Э.Баумана, Москва, a.markov@bmstu.ru

[2] https://t.me/EchelonEyes/117

9. Fortinet: Threat Predictions for 2023: New Attack Surfaces and Threats Emerge as Cybercrime Expands.

10. Splunk: Predictions 2023: Strategies for Turbulent Times.

11. AT&T: 10 Cybersecurity Predictions for 2023.

12. Check Point Software's Cybersecurity Predictions for 2023: Expect More Global Attacks, Government Regulation, and Consolidation.

13. Gartner's 8 Cybersecurity Predictions for 2023-2025.

14. BAE Systems: 2023 Cybersecurity Predictions.

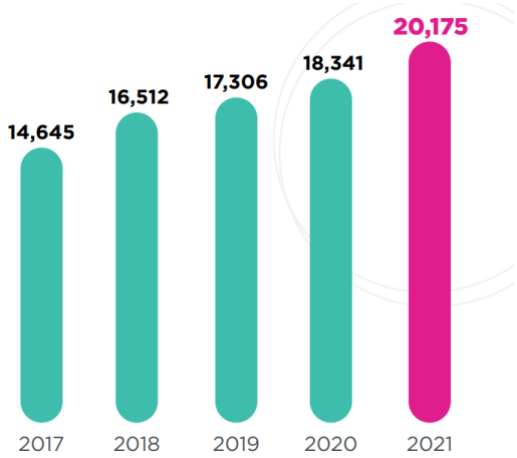
15. Proofpoint: Cybersecurity Predictions for a Turbulent 2023 и т.д.

В качестве примера можно сослаться на отчет McKinsey: глобальные тренды 2022–2023, где сделан прогноз на следующее:

- рост технологической сложности атак: хакеры используют искусственный интеллект и другие технологии для проведения все более изощренных атак;
- расширение поверхности атаки (attack surface): сейчас это не только корпоративная ИТ-инфраструктура, но и конечные пользователи, облачные сервисы и т.п.;
- рост рисков, связанных с атаками на цепочки поставок программ и репозитории открытого программного обеспечения;
- рост нормативного регулирования (к слову, в США за год было подписано 250 нормативно-правовых актов, посвященных кибербезопасности);
- внимание к новым архитектурам и технологиям безопасности (Zero Trust, IRP, Threat Hunting и пр.) и интеграции SOC/CERT;
- сохранение недостатка в квалифицированных человеческих ресурсах для обеспечения кибербезопасности.

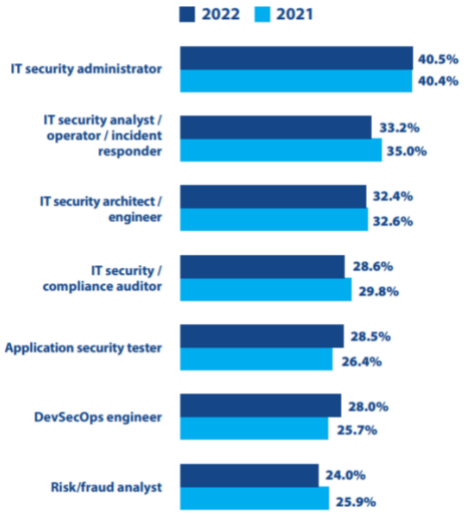
Ряд утверждений проиллюстрирован ниже на рис. 1–5.

Рис. 1. Количество уязвимостей увеличилось почти в четыре раза за 10 лет.



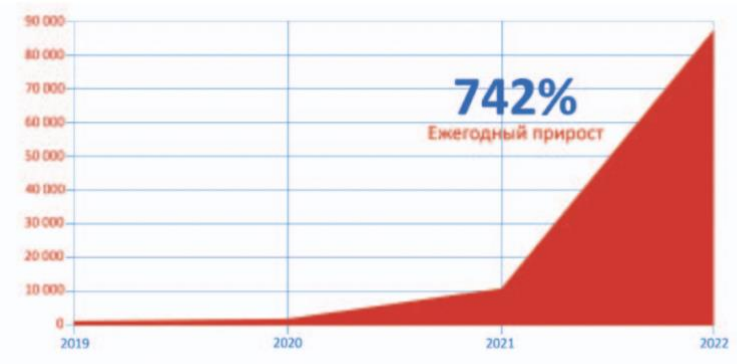
Источник: Vulnerability and threat trends report 2022, Skybox

Рис. 2. Темп роста количества обнаруживаемых уязвимостей также растет



Источник: Report Defense Cyberthreat 2022, CyberEdge Group

Рис. 3. Все страны мира испытывают дефицит квалифицированных сотрудников в области



Источник: Sonatype

Рис. 4. Взрывной рост атак на цепочки поставки opensource-компонентов

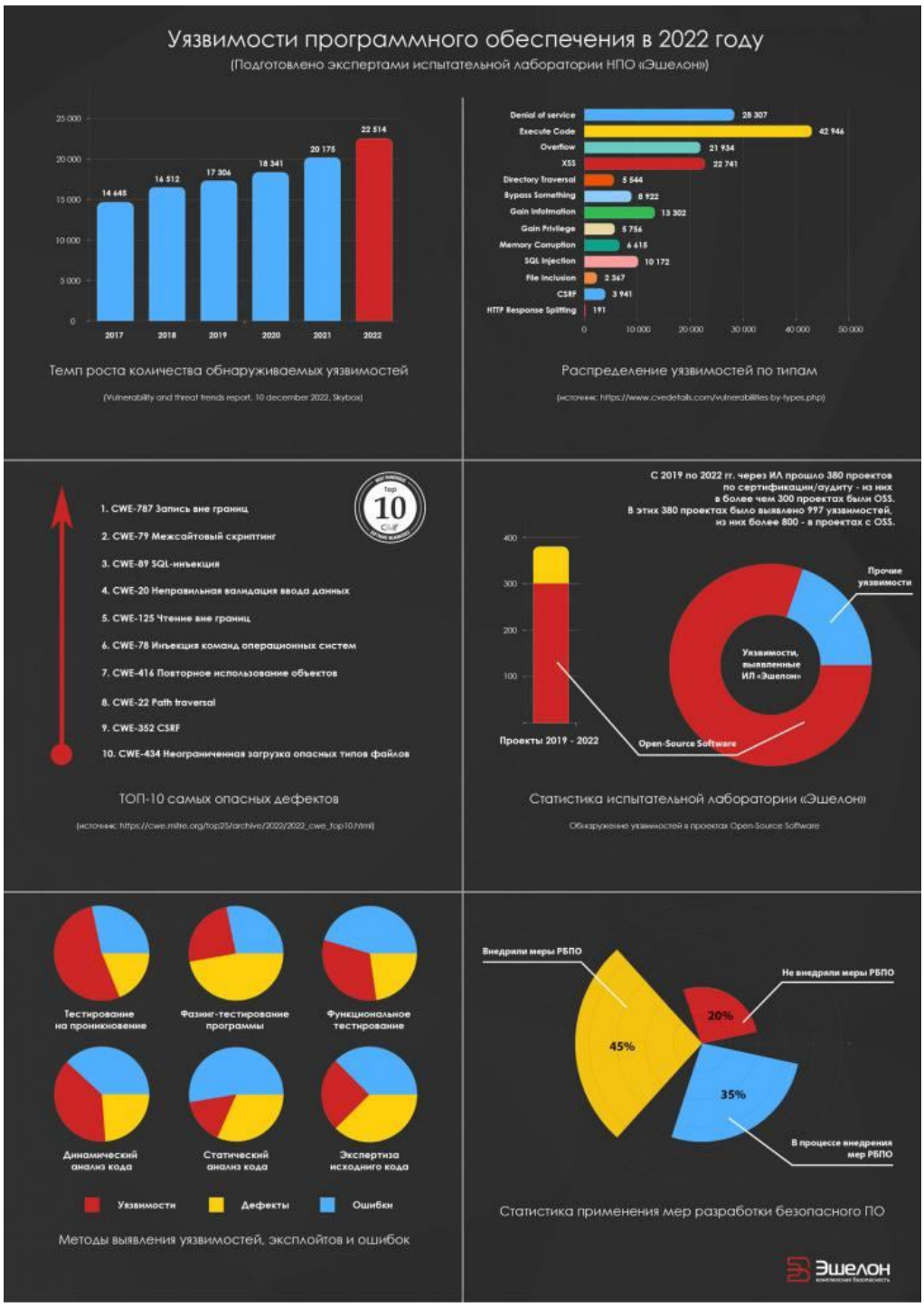
Рис. 5. Взрывной рост преднамеренных закладок

В области аудита и сертификации программных систем российская компания НПО «Эшелон» тоже приготовила аналитический отчет (рис. 6).

Состояние кибервойны

Ряд политических деятелей и представителей отечественных компаний отмечают рост агрессивности в киберпространстве относительно нашей страны, а именно:

- рост DDoS-атак на Россию;
- появления феномена «протестное ПО»;
- Россия занимает первое место по количеству взломов»;
- доктринные документы Запада (и киберучения НАТО) демонстрируют задачи по противостоянию России и Китаю;
- информационное (аналитическое) доминирование и технологические угрозы со стороны Запада и пр.



Источник: НПО «Эшелон»

Рис. 6. Статистика по уязвимостям и угрозам безопасности программ

Российские реалии

Согласно ITU, Россия занимает 5-е место в рейтинге Global Cybersecurity Index. Например, ближайшему нашему союзнику – Белорусии отведено лишь 89-е место. Можно скептически относиться к различным международным рейтингам, но следует согласиться, что год для отрасли был сложным и турбулентным, что определено задачами страны на технологический суверенитет и далее – на технологическую независимость (а может и на лидерство). Некоторые проблемные (пока) моменты для рынка представлены в табл. 1.

Таблица 1.

Сложности	Возможности
• Уход поставщиков и усложнение логистики	• Решается, возросли сроки (по железу)
• Уход технологичных компаний	• Импортозамещение; открылись возможности, активизация по инновациям
• Санкции	• Относительно не повлияли
• Колебание на рынке труда	• Решение в виде поддержки ИТ/ОПК
• Ужесточение выполнения ГОЗ	• В ИТ/ИБ не решены

Основные векторы научных исследований в области обеспечения информационной безопасности страны в настоящее время включают 53 актуальные проблематики по четырем направлениям[3]:

1. Общенаучные проблемы обеспечения ИБ РФ.
2. Научно-технические проблемы обеспечения ИБ РФ.
3. Проблемы кадрового обеспечения ИБ РФ.
4. Проблемы формирования системы международной ИБ.

Можно добавить, что в прошлом году введены новые научные специальности ВАК РФ:

- 1.2.4 – «Кибербезопасность»;
- 2.3.6 (05.13.19) – «Методы и системы защиты информации, информационная безопасность».

Выводы

1. Сейчас область информационной безопасности самая передовая и динамичная в сфере ИТ, особенно в сочетании с развитием AI/ML/DL.
2. Но, как говорится, дорогу осилит идущий: **всем успехов в работе конференции**!

Литература

1. Безопасность России. правовые, социально-экономические и научно-технические аспекты. Тематический блок "Национальная безопасность". / Под общей редакцией Н.А.Махутова. – М.: Изд-во: Общественная организация - Общество "Знание" России, 2023. - Сер. Безопасность России. Правовые, социально-экономические и научно-технические аспекты. - Том 2 «Системная инженерия в проблемах национальной безопасности».

2. Кибербезопасность цифровой индустрии. Теория и практика функциональной устойчивости к кибератакам / Под ред. Зегжда Д.П. и др. М.: Горячая линия, 2021. 560 с.

Conference Greeting
Secure Information Technologies Modern Trends

Markov A.S.[4]

Within the framework of the conference it is planned to consider global trends in the field of information security, trends of secure technologies, aspects of applied solutions and set tasks for the near future.

Keywords: information security, secure information technologies, cybersecurity

[3] http://scrf.gov.ru/security/information/document155/

[4] Alexey Sergeevich Markov, Dr.Sc., Professor, Bauman Moscow State Technical University, a.markov@bmstu.ru

УДК 681.3.06:004.056

Интеллектуальные методы фаззинг-тестирования в рамках цикла безопасной разработки программ

Арустамян С.С.[5], Антипов И.С.[6]

В данной статье рассматриваются интеллектуальные методы фаззинг-тестирования с применением алгоритмов машинного обучения для оценивания результатов предыдущей итерации. Данный метод основан на обучении нейронной сети, которая сопоставляет входные данные программы с результатами выполнения, обучаясь на входных данных и результатах предыдущей итерации, которые были собраны во время классического фаззинг-тестирования. Затем обученная модель применяется для генерации входных данных, которые смогут повысить покрытие кода за меньшее количество запусков.

Ключевые слова: Фаззинг-тестирование, мутационный фаззинг, машинное обучение, нейронные сети, безопасная разработка, покрытие, AK-BC 3, AK-VS ModFuzz.

1. Введение

Проблема безопасности программного кода остается одной из основных в области кибербезопасности [1-3]. Среди современных средств тестирования одним из перспективных является применения фаззинг-тестирования в целях выявления ошибок и уязвимостей в программном обеспечении [2, 4-7]. Цель фаззинг-тестирования состоит в том, чтобы обнаружить набор тестовых входных данных, который максимизирует охват кода в целевом программном или программно-аппаратном комплексе в надежде, что это позволит найти ошибки, сбои или другие потенциальные уязвимости. В ходе типичного запуска фаззинга генерируется сотни тысяч входных данных, и лишь малая часть фактически покрывает новые пути выполнения программы, что приводит к сотням минут ненужного времени выполнения [8-13].

В данной статье мы предлагаем метод сокращения этих избыточных исполнений с помощью машинного обучения для генерации входных данных. В частности, мы утверждаем, что для успешного фаззинга важно уметь сопоставлять входные данные программы с результатами работы. Используя машинное обучение для прогнозирования пути выполнения на основе заданных входных данных, мы представляем подход, дополняющий фаззинг серого ящика, позволяющий нам фильтровать бесполезные входные данные перед выполнением. Логика, лежащая в основе нашего подхода к фильтрации, проста: мы сосредотачиваемся на генерации входных данных, с помощью которых мы сможем получить новые пути выполнения программы. Это достигается за счет машинного обучения прямого прогнозирования на основе данных, которые были получены ранее. Сосредоточив на этом внимание, мы показываем, что можем значительно улучшить охват программы при меньшем числе ее запусков.

Мы строим наш подход на основе AK-VS 3 ModFuzz. С помощью серии экспериментов с тестовыми программами мы показываем, что наш подход значительно лучше по сравнению с классическими фаззерами, также мы получаем более высокую скорость покрытия кода, чем многие надежные базовые версии, включая самую эффективную версию AFL.

[5] Арустамян Сас Сергеевич, Москва, МГТУ им. Н.Э.Баумана, кафедра ИУ8, as@cnpo.ru
[6] Антипов Илья Сергеевич, Москва, АО «НПО «Эшелон», mail@cnpo.ru

2. Общая часть

На данный момент существует большое количество подходов к поиску ошибок в программных и программно-аппаратных комплексах, однако в рамках цикла безопасной разработки программ [14-18] мы фокусируемся на подходе белого ящика, включая символьное выполнение. Это название происходит от прозрачности базовой программы; белый ящик требует большой прозрачности (здесь подразумевается, что есть доступ к исходным текстам, или возможность поднять исполняемый файл до промежуточного представления).

Помимо этого, существуют подходы серого и черного ящиков, которые полезны для поиска неглубоких ошибок, но показывают недостаточный результат для полноценного тестирования.

3. Описание методов фаззинг-тестирования в AFL

Одним из основных инструментов фаззинг-тестирования на данный момент является фаззер AFL (рис. Рис. *1*) [19, 20].

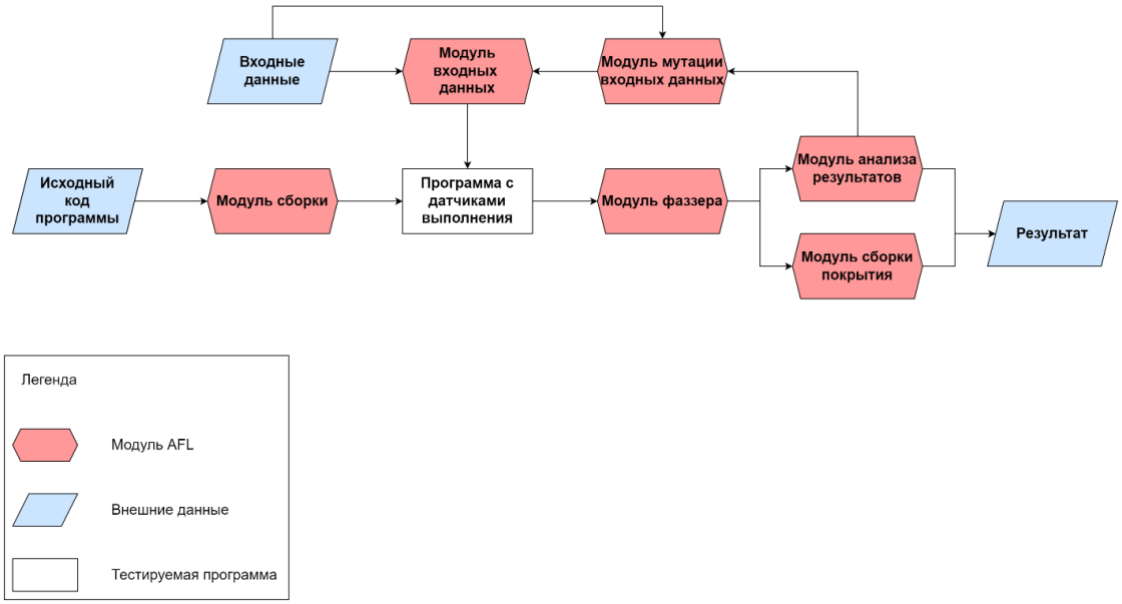


Рис. 1 – Схема работы AFL

Принцип его работы описывается следующими шагами:

- ✓ исходный код при помощи модуля сборки преобразуется в программу, в которую внедрены датчики, необходимые для проведения фаззинг-тестирования;
- ✓ заранее заготовленные входные данные попадают в очередь, которая будет использоваться фаззером при проведении тестирования;
- ✓ начинается процесс фаззинг-тестирования;
- ✓ результаты работы программы попадают в модули анализа результатов;
- ✓ модуль мутации входных данных мутирует изначальные входные данные для проведения дальнейшего тестирования;
- ✓ циклично повторяются шаги 3–5.

Высокоуровневое описание подхода в AK-VS 3 ModFuzz

На высоком уровне наш подход дополняет классическую схему проведения фаззинг-тестирования, описанную выше (рис. Рис. *2*).

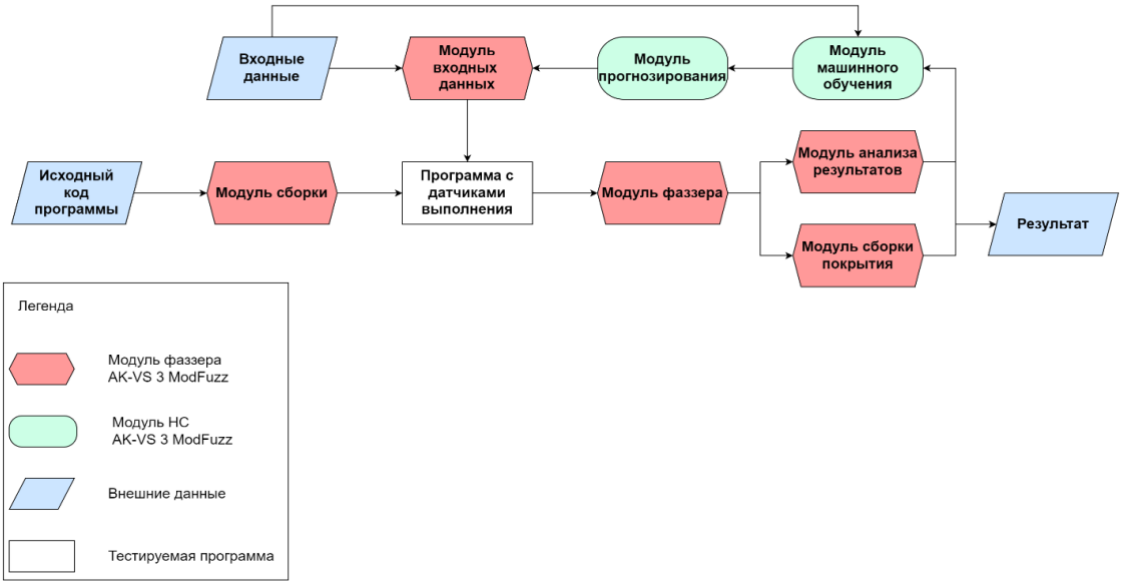


Рис. 2 – Схема работы AK-VS 3 ModFuzz

Принцип работы AK-VS 3 ModFuzz заключается в многократном выполнении следующих шагов:

- с помощью модуля сборки фаззера исходный код преобразуется в программу, в которую внедрены датчики, необходимые для проведения фаззинг-тестирования;
- заранее заготовленные входные данные попадают в очередь, которая будет использоваться модулем фаззера при проведении тестирования;
- первичные результаты модуля фаззера отправляются в модуль нейронной сети для обучения. Обучение происходит при помощи оптимизации loss-функции, которая является линейной комбинацией каждого из критериев:

$$\mathcal{L}_{total} = \sum_{i=1}^{N} \alpha_i \mathcal{L}_i \quad (1)$$

где: $\mathcal{L}_{total}$ – итоговое значение loss-функции, α_i – вес каждого из критериев, $\mathcal{L}_i$ – значение loss-функции каждого из критериев.

- после обучения нейронная сеть может генерировать входные данные;
- входные данные, которые приходят на модуль фаззера, генерируются при помощи модуля нейронной сети.
- запускается классический процесс фаззинг-тестирования;
- циклично повторяются шаги 5-6.

Сравнение AK-VS 3 ModFuzz и AFL

Для того, чтобы оценить метод, предложенный выше, необходимо сравнить его со стандартным методом проведения фаззинг-тестирования. Для этого была выбрана тестовая программа, которая и предназначена для оценки фаззеров, FuzzGoat.

В таблице Таблица 1 представлен сравнительный результат классического фаззинг-тестирования на примере AFL с интеллектуальным фаззинг-тестированием на примере AK-VS 3 ModFuzz.

Сравнивалось количество новых ветвей, который обнаружил каждый из фаззеров за одинаковое количество времени.

Таблица 1.

Результаты сравнения

Время	AFL	AK-VS 3 ModFuzz
30 минут	81	163
1 час	144	203
3 часа	632	634
7 часов	842	1248

В итоге удалось выявить, что результаты AK-VS 3 ModFuzz превосходят результаты AFL. После 30 минут проведения фаззинг-тестирования результаты AK-VS 3 ModFuzz более чем в 2 раза превосходят результаты AFL за аналогичное время. После 7 часов фаззинг-тестирования AK-VS 3 ModFuzz показал эффективность почти в 1,5 выше по сравнению с AFL. Данные результаты позволяют сделать вывод, что метод, описанный в данной статье, является эффективным и может применяться при проведении фаззинг-тестирования.

Вывод

В данной работе мы представили систему повышения эффективности фаззинг-тестирования, использующую технологию машинного обучения до непосредственного моделирования поведения программы.

В частности, мы отмечаем, что основным недостатком классического фаззинг-тестирования является количество выполнений программных или программно-аппаратных комплексов, которые тратятся впустую на избыточные входные данные. Чтобы устранить эту проблему, мы предложили новый подход, использующий методы машинного обучения. Он заключается в использовании нейронных сетей для генерации входных данных, которые с большей вероятностью приведут к нахождению новых путей работы программы.

Для проверки приведенного метода был проведен эксперимент на тестовой программе. Его результаты показали, что интеллектуальное фаззинг-тестирование является более эффективным по сравнению с классическим фаззинг-тестированием.

Литература

1. Зегжда Д.П., Александрова Е.Б., Калинин М.О. и др. Кибербезопасность цифровой индустрии // Теория и практика функциональной устойчивости к кибератакам. М.: Горячая линия - Телеком, 2021. - 560 с.

2. Марков А.С., Цирлов В.Л., Барабанов А.В. Методы оценки несоответствия средств защиты информации / Под.ред. А.С.Маркова. М.: Радио и связь, 2012. 192 с.

3. Petrenko S. La Administración de la Ciberseguridad. Industria 4.0. – Oviedo: University of Oviedo (Spain), 2019. 294 p.

4. Барабанов А.В., Марков А.С., Цирлов В.Л. 28 магических мер разработки безопасного программного обеспечения. Вопросы кибербезопасности. 2015, № 5(13), с. 2–10.

5. Барабанов А.В., Вареница В.В., Марков А.С. Аудит безопасности программ Учебно-методическое пособие / Москва, 2021.

6. Жидков И.В., Зубарев И.В., Хабибуллин И.В. Выбор рациональной модели разработки безопасного программного обеспечения // Вопросы кибербезопасности. 2021, № 5(45), с. 21–29.

7. Козачок А.В., Николаев Д.А., Ерохина Н.С. Подходы к оценке поверхности атаки и фаззингу веб-браузеров // Вопросы кибербезопасности. 2022. № 3 (49). С. 32–43.

8. Козачок А.В., Спирин А.А., Ерохина Н.С. Метод генерации семантически корректного кода для фаззинг-тестирования интерпретаторов javascript // Вопросы кибербезопасности. 2023. № 5 (57). С. 80–88.

9. Козырский Б.Л., Комаров Т.И., Иванов М.А. Использование фаззинга для поиска уязвимостей в программном обеспечении // Безопасность информационных технологий. 2014. Т. 21. № 4. С. 33–43.

10. Кондаков С.Е., Рудь И.С. Модель процесса проведения компьютерных атак с использованием специальных информационных воздействий Вопросы кибербезопасности. 2021, № 5(45), с. 12–20.

11. Осипова Н.С. Применение методов машинного обучения при проведении фаззинг-тестирования. В сборнике: «Безопасные информационные технологии». Сборник трудов Одиннадцатой международной научно-технической конференции. МГТУ им. Н.Э.Баумана, 2021. С. 263–269.

12. Программный комплекс динамического тестирования на безопасность программного обеспечения Quick-launch fuzzer (QLF) / Зегжда Д.П., Москвин Д.А., Овасапян Т.Д. и др. – Св. о рег. программы для ЭВМ - RU 2022665392, 15.08.2022. Заявка № 2022664886 от 05.08.2022.

13. Томилов И.О., Карманов И.Н., Звягинцева П.А., Грицкевич Е.В. Разработка методики применения фаззинга для анализа уязвимостей программного обеспечения // Системы управления, связи и безопасности. 2018. № 4. С. 48–63.

14. Арустамян С.С., Вареница В.В., Марков А.С. Методические и реализационные аспекты внедрения процессов разработки безопасного программного обеспечения // Безопасность информационных технологий. 2023. Т. 30. № 2. С. 23–37.

15. Вареница В.В., Марков А.С., Савченко В.В., Цирлов В.Л. Практические аспекты выявления уязвимостей при проведении сертификационных испытаний программных средств защиты информации // Вопросы кибербезопасности. 2021, № 5(45), с. 36–44.

16. Гришин М.И., Марков А.С., Цирлов В.Л. Практические аспекты реализации мер по разработке безопасного программного обеспечения // ИТ-Стандарт. 2019, № 2(19), с. 74–87.

17. Марков А.С. Актуальные вопросы разработки безопасного программного обеспечения. В книге: Кибернетика и информационная безопасность «КИБ-2023». Сборник научных трудов Всероссийской научно-технической конференции. Москва, 2023. С. 10–11.

18. Markov A.S., Varenitca V.V., Arustamyan S.S. Topical Issues in the Implementation of Secure Software Development Processes. In Proceedings of the International Conference on Information Processes and Systems Development and Quality Assurance. IPSQDA-2023. 2023. P. 48–53.

19. Зимин Е.Е. Методика фаззинг-тестирования кода с помощью AFL. В сборнике: «Безопасные информационные технологии». Сборник трудов Одиннадцатой международной научно-технической конференции. МГТУ им. Н.Э.Баумана, 2021. С. 124–129.

20. Тронов К.А., Белов Ю.С. Оптимизация инструментария AFL для лучшего покрытия кода при работе со специфичными данными // E-Scio. 2021. № 5 (56). С. 566–571.

Advanced methods of fuzzing testing as a part of the SSDLC

Arustamyan S.S.[7]**, Antipov I.S.**[8]

Abstract*. This article describes advanced methods of fuzzing testing using machine learning algorithms to evaluate the results of the previous iteration. This method is based on training a neural network that compares program input data with execution results, learning from the input data and results of the previous iteration, which were collected during classic fuzzing testing. The trained model is used to generate inputs that can improve code coverage in fewer execution.*

Keywords*: fuzzing testing, Mutation-Based Fuzzing, machine learning, neural networks, SSDLC, coverage, AK-VS 3, AK-VS ModFuzz.*

[7] Arustamyan Sas Sergeevich, Moscow, Bauman MSTU, as@cnpo.ru
[8] Antipov Ilya Sergeevich, Moscow, NPO Echelon, mail@cnpo.ru

УДК 004.056

Разработка методики эмуляции сетевой активности для анализа вредоносного обеспечения в изолированной среде

Белгородцев С. К.[9]

В рамках исследования были изучены принципы безопасной среды выполнения и детектирования вредоносного программного обеспечения в изолированной среде. Внимание было уделено проблеме недоступности сетевых сервисов при анализе вредоносного программного обеспечения в изолированной среде. В результате работы были рассмотрены существующие системы эмуляции сетевой активности, их преимущества и недостатки. Был разработан алгоритм функционирования методики эмуляции сетевой активности, а также созданы основные модули, включая HTTP/HTTPS, DNS, SMTP, FTP, SMB, запись сетевого трафика и конфигурирование правил. Были представлены технические детали разработки методики эмуляции сетевой активности. Для демонстрации возможностей системы были использованы образцы вредоносного программного обеспечения. В целом, разработка методики эмуляции сетевой активности для анализа вредоносного программного обеспечения в изолированной среде позволила повысить эффективность и точность анализа вредоносного программного обеспечения в контролируемой среде безопасности.

Ключевые слова: информационная безопасность, эмуляция сетевой активности, изолированная среда, виртуализация, вредоносное программное обеспечение.

Введение

Вопросы анализа вредоносной активности становятся все актуальней по причине неэффективности сигнатурных методов [1]. Одним из путей выявления вредоносной активности является отслеживание запросов к внешних сетевым сервисам [2-7]. Так, в процессе автоматического анализа вредоносного кода в изолированной среде часто возникают ситуации, когда вредоносное программное обеспечение требует доступности тех или иных сервисов в сети Интернет. Однако, простое предотвращение любого доступа к Интернету во многих случаях невозможно, поскольку вредоносным программам часто требуется доступ для запуска и демонстрации своей активности. В случае отсутствия доступности сервисов вредоносная программа не исполняет блоки кода и тем самым ограничивает анализируемую область поведения. Для того, чтобы сделать анализ максимально полным, нужно эмулировать недоступные сервисы между изолированной средой и сетью [8].

Эмуляция сетевой активности является важным инструментом для анализа вредоносного программного обеспечения. Она позволяет не только эмулировать недоступные сервисы, но и воссоздавать сетевые условия, в которых работает вредоносное программное обеспечение. Это особенно важно при анализе распространения таких типов вредоносных программ, которые активно используют сеть для своей работы. Использование методики эмуляции сетевой активности позволяет проводить исследования в контролируемой среде и получать более точные и достоверные результаты.

Особенности работы ВПО, зависящего от доступности сетевых сервисов для исполнения вредоносного кода

Одной из ключевых целей анализа вредоносных программ является выявление их функционала, который может быть направлен на нанесение ущерба системе или конкретной организации. Однако, в некоторых случаях выполнение задач вредоносных

[9] Белгородцев Сергей Константинович. Москва, МГТУ им. Н.Э. Баумана, НПО «Эшелон», serggey00.00@gmail.com

программ может зависеть от доступности сетевых сервисов. В данном разделе проводится обзор сервисов, которые могут быть критичными для работы распространенных семейств вредоносного программного обеспечения, и как их недоступность может повлиять на анализ и защиту от угроз [9, 10].

Работа вредоносного ПО, зависящего от доступности сетевых сервисов для исполнения вредоносного кода, тесно связана с системой C2, поскольку эти программы могут использовать сетевые сервисы для получения команд от злоумышленников и передачи данных. Если доступность сетевых сервисов для исполнения вредоносного кода будет ограничена, это может повлиять на возможности злоумышленников управлять вредоносным ПО и получать от него информацию.

Command and Control

Инфраструктура управления и контроля, также известная как система C2, или Command and Control, представляет собой инструмент для удаленного управления и контроля вредоносным программным обеспечением [11]. Через C2 злоумышленники могут управлять взломанными компьютерами с автономным ВПО, собирать информацию и осуществлять различные виды компьютерных атак. Вредоносное ПО обычно устанавливается на целевой компьютер с помощью эксплуатации уязвимостей или социальной инженерии и связывается с системой C2, чтобы получать инструкции, загружать дополнительные вредоносные данные, осуществлять передачу украденных. Ограничение доступности сетевых сервисов для исполнения вредоносного кода может заблокировать возможности злоумышленников управлять вредоносным ПО и получать информацию от него, поэтому работа такого вредоносного ПО, тесно связана с системой C2[10].

ВПО семейства «Cobalt Strike»

«Cobalt Strike» представляет собой комплекс для проведения атак, который позволяет доставлять на атакуемый компьютер полезную нагрузку и управлять ею. Взаимодействие с серверной частью «Cobalt Strike» происходит посредством создания скрытых каналов с использованием протоколов DNS, HTTP, HTTPS для предотвращения обнаружения данного сетевого взаимодействия[11]. Полезная нагрузка может выполнять следующие команды:

– получать сведения о системе (ОС, оборудование, список процессов, имя компьютера)
– получать сведения о сетевом окружении;
– выполнять команду командной оболочки
– загрузить и запустить исполняемый файл.

Для выполнения этих задач «Cobalt Strike» использует C2-сервер, который обеспечивает связь между атакующим и зараженными устройствами. Поэтому для использования «Cobalt Strike» необходима работающая сетевая инфраструктура.

ВПО семейства «Agent Tesla»

«Agent Tesla» – это популярный троян, используемый для кражи конфиденциальной информации с компьютеров жертвы. Данное программное обеспечение может захватывать все, что вводится на клавиатуре конечного устройства, включая пароли, данные банковских карт, личную информацию и другую конфиденциальную информацию[12].

Созданная на основе программной платформы .NET программа «Agent Tesla» разработана с целью извлечения и передачи на сервер C2 персональных данных, получаемых из веб-браузеров, почтовых клиентов и FTP-серверов. Дополнительно, данное

[10] https://attack.mitre.org/tactics/TA0011
[11] https://any.run/malware-trends/cobaltstrike
[12] https://any.run/malware-trends/cobaltstrike

вредоносное ПО способно получать скриншоты и видеозаписи, а также записывать информацию из буфера обмена и значения форм. Для отправки скомпрометированных данных на сервер C2, вредоносное ПО «Agent Tesla» должно иметь доступ к сети Интернет и сетевым сервисам, таким как SMTP, FTP или HTTP.

Проектирование модулей системы эмуляции сетевой активности

Методика эмуляции сетевой активности для анализа вредоносного программного обеспечения в изолированной среде включает в себя семь основных модулей:

- ✓ модуль HTTP/HTTPS;
- ✓ модуль DNS;
- ✓ модуль SMTP;
- ✓ модуль FTP/FTPS;
- ✓ модуль SMB;
- ✓ модуль записи и подмены сетевого трафика;
- ✓ модуль конфигурирования правил.

В следующем разделе приведено детальное описание функционирования модулей системы эмуляции сетевой активности, а также изображена структура, показывающая взаимодействие с изолированной средой.

Методика эмуляции сетевой активности для анализа ВПО

Работа системы эмуляции сетевой активности основана на перенаправлении трафика от изолированной среды, в которой происходит анализ ВПО, при помощи утилиты iptables[13] [7].

Структурная схема системы эмуляции сетевой активности представлена на рис. 1. На нем показаны основные элементы взаимодействия:

- – изолированная среда;
- – правила перенаправления пакетов;
- – система эмуляции сетевой активности.

В блоке системы эмуляции изображены все модули и показано взаимодействие между ними (рис.1).

Далее рассмотрим последовательной описание шагов методики эмуляции сетевой активности.

1. Выбор активных модулей системы эмуляции до старта анализа ВПО в изолированной среде, опциональная настройка модулей в зависимости от требований. Например, зная о том, что вредоносный файл будет отправлять запрос на ресурс, доменное имя которого недоступно, можно включить только модуль DNS, для корректного разрешения данного имени. Настройка модулей осуществляется через конфигурационный файл системы эмуляции.
2. Написание правил в YAML файле. После написания правила проходят проверку на синтаксис и при успешном исходе применяются для соответствующих модулей, также проверяется наличие файла полезной нагрузки в указанной директории.

[13] https://linux.die.net/man/8/iptables

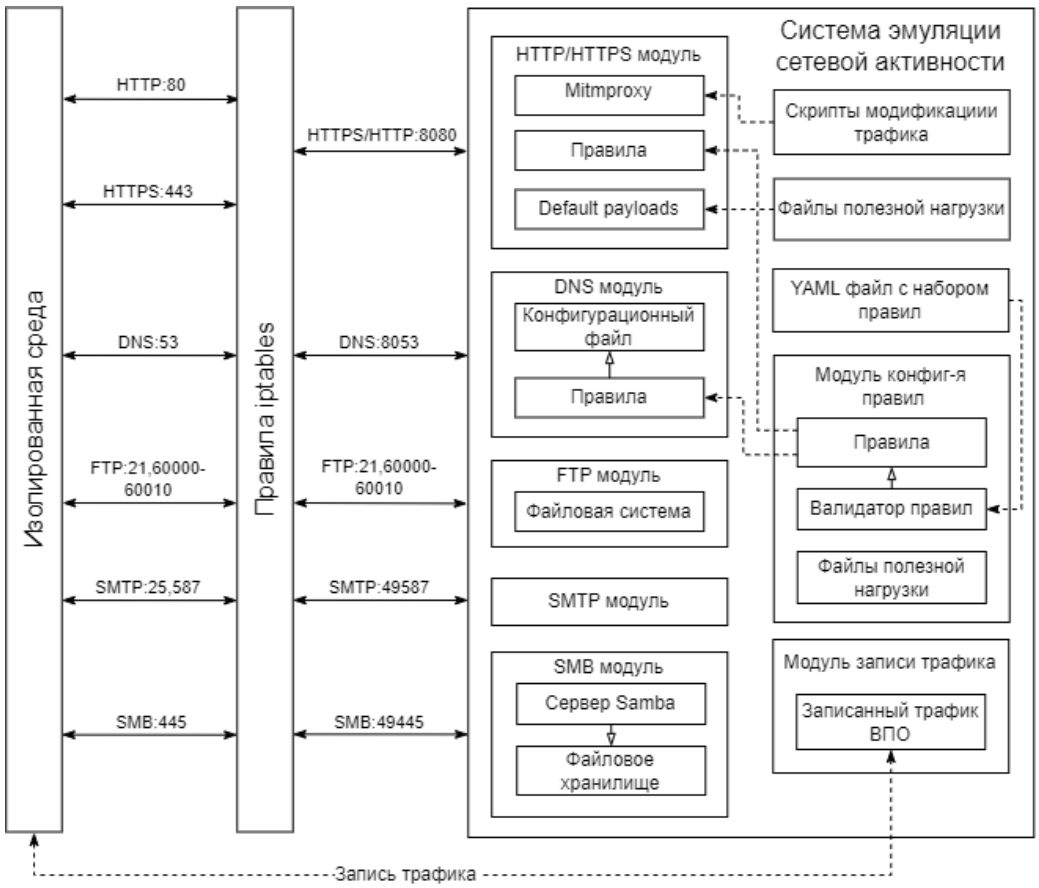


Рис. 1. Структурная схема системы эмуляции сетевой активности

3. Запуск активных модулей системы. На этом этапе происходит инициализация модулей, импортируются файлы сценария для mitmproxy, запускаются локальные сервера (HTTP, DNS, Samba, FTP), применяются правила.

4. Перенаправление трафика для запущенных модулей при помощи правил утилиты iptables. Выполняется перенаправление сетевого трафика со следующих портов:

a) для модуля HTTP/HTTPS пакеты перенаправляется с TCP-портов 80, 443 на TCP-порт 8080;

b) для модуля DNS пакеты перенаправляются с UDP-порта 53 на UDP-порт 8053;

c) для модуля SMTP пакеты перенаправляются с TCP-портов 25, 587 на TCP-порт 49587;

d) для модуля FTP/FTPS пакеты перенаправляются с TCP-портов 21, 60000–60010 на TCP-порты 2021, 60000–60010 соответственно;

e) для модуля SMB пакеты перенаправляются с TCP-порта 445 на с TCP-порт 49445.

5. Завершение работы системы. На данном этапе осуществляется отключение правил перенаправления пакетов, производится остановка локальных серверов и процессов.

6. Формирование отчета о результатах работы. Создается файл с журналами работы каждого активного модуля, а также информацией о сработавших правилах.

Алгоритм программного средства эмуляции сетевой активности

На рис. 2 показано визуальное представление алгоритма работы программного средства эмуляции сетевой активности, что облегчает его понимание и использование в рамках исследований и анализа вредоносного программного обеспечения.

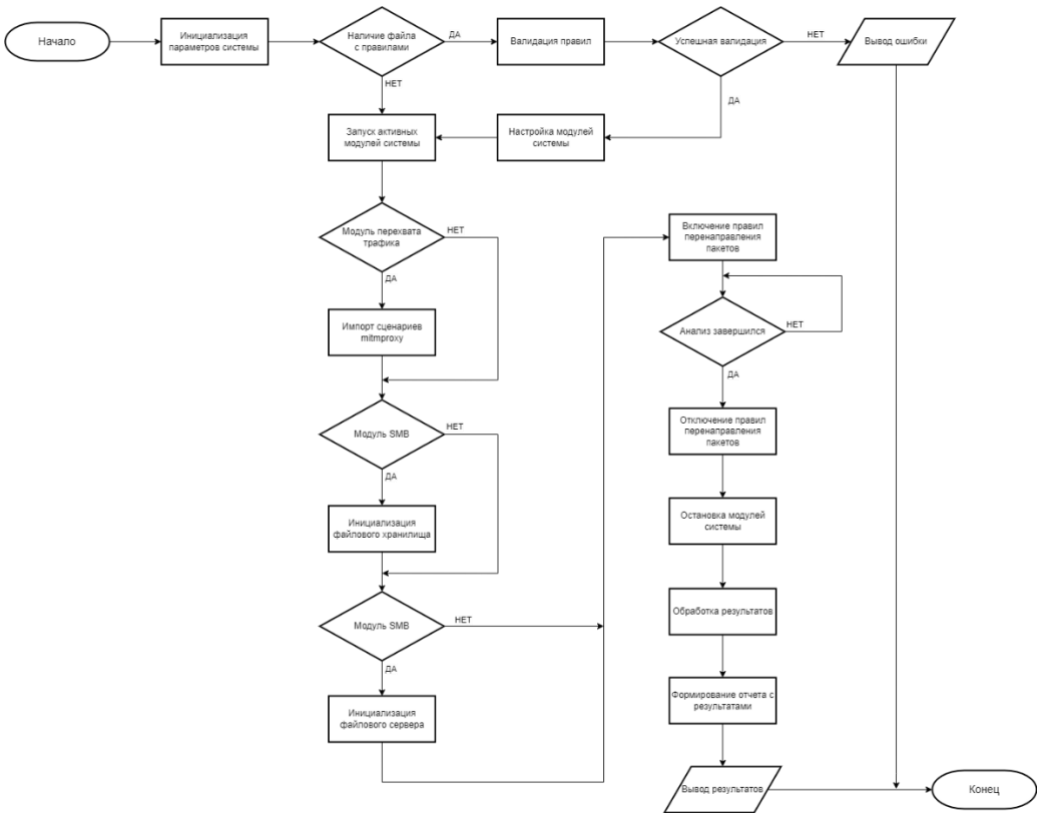


Рис. 2. Алгоритм программного средства эмуляции сетевой активности

Выводы

В результате исследования была разработана методика эмуляции сетевой активности для анализа вредоносного программного обеспечения (ВПО) в изолированной среде. Основная проблема, связанная с недоступностью сетевых сервисов при анализе ВПО в изолированной среде, была выявлена и изучена. Существующие системы эмуляции сетевой активности были проанализированы, и на основе этого была разработана математическая постановка задачи эмуляции сетевой активности в изолированной среде для анализа ВПО. Также был разработан алгоритм функционирования методики эмуляции сетевой активности, а также спроектированы основные модули, включая HTTP/HTTPS, DNS, SMTP, FTP, SMB, запись сетевого трафика и конфигурирование правил. В технологической части были представлены технические детали разработки методики эмуляции сетевой активности с использованием языка программирования Python, который обеспечивает обширный набор библиотек для работы с сетевыми протоколами. Кроме того, были рассмотрены технологические аспекты всех модулей системы эмуляции, описана их функциональность, особенности реализации и взаимодействия. Для демонстрации возможностей системы были использованы образцы ВПО. В целом, разработка методики эмуляции сетевой активности в изолированной среде позволила повысить эффективность и точность анализа вредоносного ПО в изолированной среде.

Литература

1. Кибербезопасность цифровой индустрии. Теория и практика функциональной устойчивости к кибератакам / Под ред. Зегжда Д.П. и др. М.: Горячая линия, 2021. 560 с.

2. Барабанов А.В., Гришин М.И., Кубарев А.В. Моделирование угроз безопасности информации, связанных с функционированием скрытых в вредоносных компьютерных программ // Вопросы кибербезопасности. 2014. № 4 (7). С. 41–48.

3. Ермаков А.О., Кавешников М.Б., Клянчина Е.В. Вредоносное программное обеспечение APT-групп и его характеристики // Вопросы кибербезопасности. 2017. № S2 (20). С. 24–29.

4. Жуковский Е.В., Зегжда Д.П. Анализ вредоносного по, обладающего механизмами опасного триггерного поведения // Защита информации. Инсайд. 2019. № 3 (87). С. 60–63.

5. Марков А.С., Фадин А.А. Организационно-технические проблемы защиты от целевых вредоносных программ типа Stuxnet // Вопросы кибербезопасности. 2013. № 1 (1). С. 28–36.

6. Мирзабаев А.Н., Самонов А.В. Метод обеспечения устойчивости вычислительного процесса в условиях воздействия вредоносных программ // Вопросы кибербезопасности. 2022. № 2 (48). С. 63–71.

7. Шкирдов Д.А., Сагатов Е.С., Сухов А.М., Дмитренко П.С. Выявление сетевых угроз на основе данных с серверов-ловушек // Защита информации. Инсайд. 2020. № 3 (93). С. 48–56.

8. Thorsten Holz. Improving Dynamic Malware Analysis by Emulating the Internet. [Электронный ресурс].URL:www.researchgate.net/publication/221540604_TrumanBox_Improving_Dynamic_Malware_Analysis_by_Emulating_the_Internet.

9. Зулькарнаев Р.Ф. Изоляция и АСУ ТП // Защита информации. Инсайд. 2019. № 6 (90). С. 34-38.

10.Michael Maass. A systematic analysis of the science of sandboxing [Электронный ресурс]. – URL: www.researchgate.net/publication/292186843_A_systematic_analysis_of_the_science_of_sandboxing.

11.Петренко С.А., Петренко А.А., Костюков А.Д. (2021). Киберустойчивость цифровых экосистем // Защита информации. Инсайд. № 4(100). С. 17-23.

Научный руководитель: д.т.н., профессор кафедры ИУ8 «Информационная безопасность» Марков А. С.

Development of a network activity emulation technique for malware analysis in an isolated environment

Belgorodtesev S. K.[14]

Abstract. As part of the study, the principles of a secure execution environment and detection of malicious software (MAL) in an isolated environment were studied. Particular attention was paid to the problem of unavailability of network services when analyzing malware in an isolated environment. As a result of the work, the existing systems for emulating network activity, their advantages and disadvantages were considered. An algorithm for the operation of the network activity emulation technique was developed, and the main modules were created, including HTTP / HTTPS, DNS, SMTP, FTP, SMB, network traffic recording and rule configuration. The technical details of the development of a network activity emulation technique for malware analysis in an isolated environment using the Python programming language were presented. The study also included consideration of the technological aspects of all modules of the emulation system, their functionality, implementation features and interaction. To demonstrate the capabilities of the system, malware samples were used. In general, the development of a network activity emulation technique for malware analysis in an isolated environment has improved the efficiency and accuracy of malware analysis in a controlled security environment.

Keywords: information security, network activity emulation, isolated environment, virtualization, malware.

[14] Sergey K. Belgorodtsev, MSTU named after N.E. Bauman, NPO Echelon, Moscow, serggey00.00@gmail.com

УДК 004.384

Квантовые вычисления и квантовые компьютеры: развитие, проблемы и перспективы

Бердюгин А.А.[15], Ревенков П.В.[16]

Статья носит обзорно-аналитический характер и отражает ситуацию, происходящую сегодня в сфере развития квантовых вычислений. Актуальность статьи обусловлена необходимостью популяризации информационных технологий среди молодежи, что зафиксировано в документах Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации, а также высокой востребованностью экспертов в сфере цифровых технологий и необходимостью развития научно-технического прогресса России. Поэтому цель публикации заключается в привлечении внимания читателя к освещённым вопросам. Полная версия статьи будет опубликована в журнале ВАК и Scopus НИЯУ МИФИ «Научная визуализация – Scientific Visualization». Использованы материалы презентации с одного из образовательных шоу компании GeekBrains «Путь в IT».

Ключевые слова: квант, кубит, суперпозиция, компьютер, состояние, вычисление

Введение

Эту тему мы начнем с не самой позитивной новости о том, что интерес к физике у российских школьников резко падает. В последние годы не растет, либо сокращается количество выпускников, которые выбирают физику в качестве выпускного экзамена [1]. Однако будущее – не только за информатикой и экономикой. Значительную роль квантовой физики мы рассмотрим далее. Напомним, что квант есть неделимая часть какой-либо величины в физике. Квантовые вычисления (КВ, Quantum Computing) – это вычисления, которые производят на компьютерах, значительно превосходящих по возможностям самые мощные классические компьютеры. Точнее, КВ представляют собой контролируемую классическими управляющими компьютерами последовательность унитарных операций простого вида над одним, двумя или тремя кубитами. В отличие от битов, которые представляют собой поток электрических или оптических импульсов длительностью 0 или 1, кубиты могут быть холодными атомами, фотонами или дефектами в кристаллической решетке. К сожалению, пока что ученые не могут управлять большим количеством кубитов.

Классический компьютер принимает все решения в центральном процессоре, работа которого основана на наборе транзисторов (рис. 1). Размер и количество этих транзисторов определяют его вычислительную способность. Он, как известно, при работе опирается на бинарную логику (0 и 1 – ложь и истина). Базовая операция в таких процессорах – сдвиг регистра, сложение и вычитание в бинарном коде (вся логика бинарна) [2].

[15] Бердюгин Александр Александрович, младший научный сотрудник Департамента информационной безопасности, Финансовый университет при Правительстве РФ, Москва, Россия. E-mail: aaberdyugin@fa.ru
[16] Ревенков Павел Владимирович, доктор экономических наук, доцент, профессор Департамента информационной безопасности, Финансовый университет при Правительстве РФ, Москва, Россия. E-mail: pavel.revenkov@mail.ru

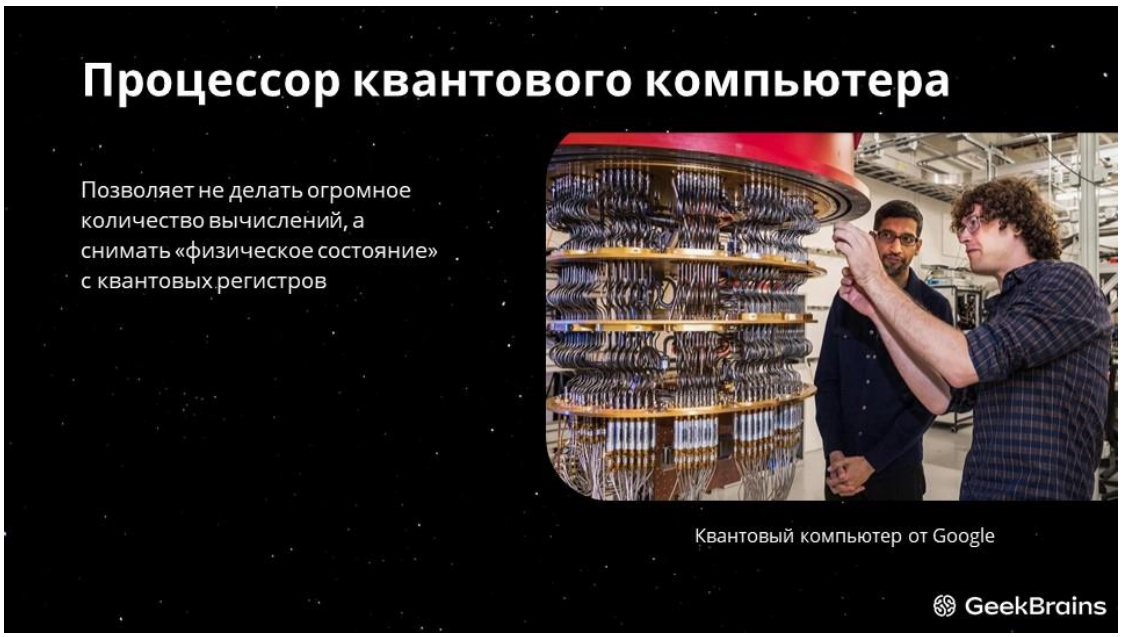


Рис. 1. Возможности квантового процессора

Квантовый компьютер (КК) – это не просто процессор и комбинация устройств, а система, подобная естественным природным системам в привычном мире, которая характеризуется определённым состоянием и изменяет свое состояние в зависимости от набора влияющих факторов, производя вычисления. На вход принимается состояние, а не нули-единицы и их алгоритмические взаимодействия. За счёт этого вычисления производятся с огромной скоростью. Лучшим результатом работы КК является наиболее вероятный ответ из возможных. То есть КК используют квантово-механические явления для выполнения вычислений.

Рассмотрим типичную задачу: у нас есть 100 гостей и их надо рассадить за двумя столами так, чтобы этот вариант устроил всех. Классический суперкомпьютер, выполняющий триллионы операций в секунду, потратит на перебор всех вариантов 10 тысяч лет. КК рассчитает это за 200 секунд [3].

Поэтому будущее за решением задач по машинному обучению с использованием квантового преимущества: если персональному компьютеру нужно 500 лет, чтобы обучить отличать кошку от собаки (без параллельных вычислений), то КК затратит на это секунды (рис. 2).

Но чтобы управлять такой системой, нужны не только компьютерщики, но также физики, поскольку в её основе лежат физические свойства электронов. То есть элементом вычисления в КК является либо электрон (минус или ноль символизирует отрицательный спин электрона, а плюс или единица – положительный спин электрона), либо поляризованный свет, если это на фотонах. Но на сегодня общепризнанной и наиболее перспективной элементной базой для построения КК являются сверхпроводящие кубиты на базе контактов Джозефсона. Джозефсоновские кубиты представляют собой сверхпроводящие структуры, которые содержат джозефсоновские контакты. Джозефсоновский туннельный контакт – это два сверхпроводника, разделенных слоем диэлектрика толщиной 10^{-7} сантиметров. Эта система взаимодействует с реальным миром, её необходимо сначала изолировать от этого внешнего мира, для того чтобы внешние факторы не влияли на вычисления, которые должны быть «чистыми».

Рис. 2. Сравнение квантового и классического компьютеров

На сегодняшний день очистка данных – одна из сложнейших задач, которые решаются для КК. Эти машины работают при очень низких температурах. То есть существует ряд ограничений физического характера, которые необходимо решить – над этим бьются IT-эксперты (продвинутые программисты, которые пишут алгоритмы для КК) и физики высшего уровня крупнейших компаний (Google, IBM, Volkswagen Group, Apple), имеющих бюджет для этого, потому что это многомиллиардные проекты для реализации [4].

Квантовая гонка и решаемые задачи

В 2016 году компания IBM создала КК на 5 кубитов (рис. 3), в последующие годы – на 49 и 50 кубитов. Начиная с 2020 года компания Microsoft открыла Azure-сервис, который позволяет дистанционно в «облаке» осуществлять эти вычисления. В конце 2022 года Китай выпустил домашний КК стоимостью около 590 тысяч рублей, что дешевле автомобиля Lada Granta. Модель позиционируется как базовое решение для знакомства со многими нюансами квантовых вычислений в учебных заведениях [5].

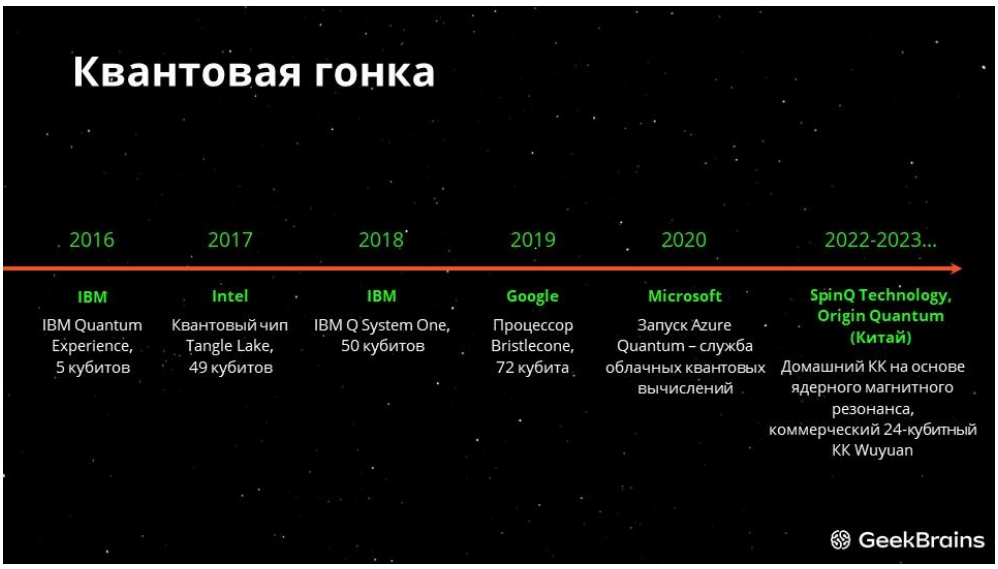


Рис. 3. Развитие КВ

Для сравнения: запоминающая электронно-лучевая трубка (трубка Уильямса-Килберна, рис. 4), разработанная в далеком 1946 году, имела объем памяти 1024 бита для вывода двумерных массивов из азбуки Морзе. Использовалась трубка в качестве носителя памяти на ранних компьютерах.

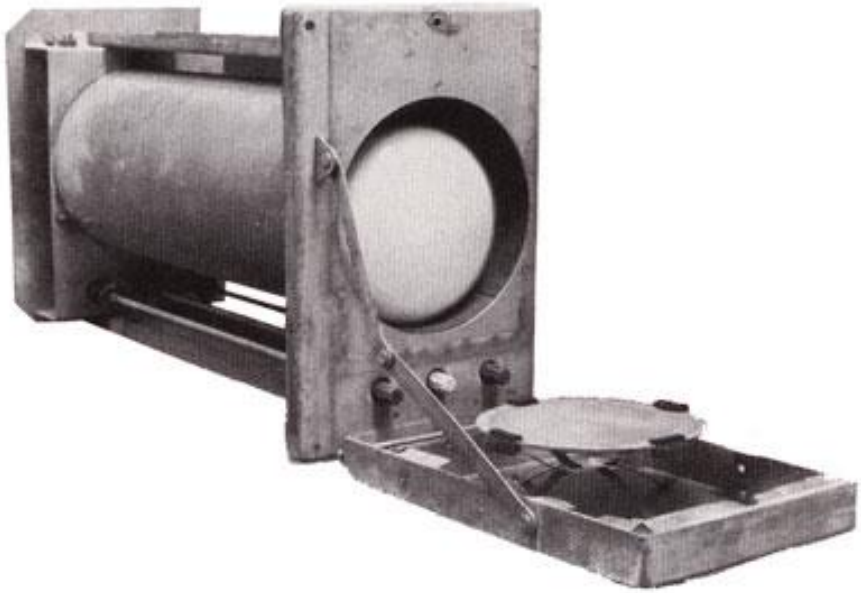


Рис. 4. Запоминающая трубка Уильямса-Килберна

Приведём пример КВ в криптографии – науке о защите данных. Есть широко распространённый протокол RSA с открытым ключом[17], который используется в цифровой подписи. Обычному компьютеру нужны десятилетия для того, чтобы взломать этот шифр методом Bruteforce (путём грубого перебора) или с помощью каких-то ускоряющих подбор алгоритмов. КК вскрывает такой ключ меньше чем за секунду. Соответственно, как только КК придут в наш мир, то всё шифрование, которое существовало до сих пор, можно «перечеркнуть» и делать заново. Т. е. криптографию придется кардинально усложнить для того, чтобы простым перебором невозможно было взломать пароль и получить доступ к нашему банковскому счету [6] (рис. 5). Соответственно, это даст ещё больше работы для сотрудников IT-сферы.

[17] В криптосистемах с симметричными ключами задача секретности должна быть разделена между двумя людьми (абонентами), а в системах шифрования с открытым ключом (например, RSA) секретность – персональная задача (неразделённая), человек (абонент) создает и сохраняет свою собственную задачу.

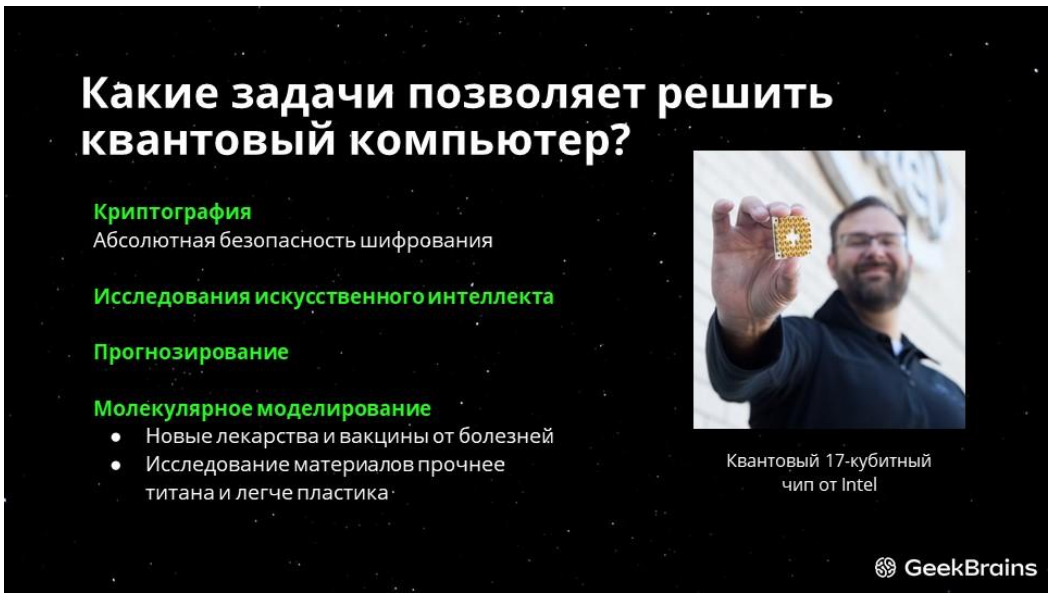


Рис. 5. Примеры решаемых задач для КК

Когда такие вычислительные способности, как искусственный интеллект и машинное обучение начнут принимать решения гораздо быстрее, чем сейчас, то это уже будет совершенно другой уровень цифрового развития. Рассмотрим прогнозирование. Это многофакторная модель, а КК смогут прогнозировать вероятность всех сценариев с высокой точностью. Близкая к совершенной безопасность шифрования[18], изучение неизвестных ранее заболеваний, моделирование и синтез различных лекарств, развитие процессов заболевания – это совершенно другой мир и, возможно, пятая промышленная революция [7-9].

Недостатки КВ и КК

Но всё это не так гладко и просто: пока нигде КК не поставлены на поток для широкого потребления, как персональные компьютеры, ввиду их дороговизны и отсутствия эталонной модели (Китай частично нарушает это правило, как было видно из рис. 3). Для повышения точности вычислений нужны очень низкая температура и создание условий, в которых КК будет изолирован от внешнего мира, потому что изменения внешней среды будут влиять на связанность элементов. С увеличением количества кубитов система становится менее стабильной – все кубиты в любом случае взаимодействуют между собой и могут потерять состояние суперпозиции. Есть такой мысленный эксперимент, как «Кот Шредингера», который говорит о том, что кот в эксперименте одновременно есть и нет (рис. 6).

[18] Первое правило кибербезопасности гласит: абсолютной защиты не существует [10]. Возможно, и это утверждение не абсолютно до развития квантовых компьютеров.

Рис. 6. Мысленный эксперимент «Кот Шрёдингера»

Предположим, есть черная коробка и там находится кот. Пока мы не откроем коробку, мы не узнаем, жив он там или нет, кот находится в состоянии суперпозиции: он одновременно жив и мертв. Если открываем коробку и там кот жив, то мы определились – суперпозиция разрушена. Но до этого зверь, вероятно, жив и, вероятно, нет [11].

Мы находимся на очень раннем этапе разработки квантовой памяти и всех КВ в целом. Только в ноябре 2022 года была создана масштабируемая квантовая память, которая живет больше 2 секунд [12]. В России квантовые технологии пока развиты слабо. Но, несмотря на эти препятствия, за этим будущее [13-18].

Заключение

Для отечественной юриспруденции и науки в общем КВ и КК до сих пор остаются terra incognita по некоторым вопросам. В первую очередь, это связано, конечно, с финансированием данной отрасли. Тем не менее риски внедрения квантовых технологий для общества и государства представляют собой не меньшую опасность, чем риски внедрения технологий искусственного интеллекта.

Поэтому, как и любая новая технология (или стартап), внедрение КВ и КК должны удовлетворять трём условиям: во-первых, иметь законное разрешение (в ряде случаев может использоваться принцип регуляторной песочницы), во-вторых, иметь конкурентные преимущества, в-третьих, обязательно такие технологии должны быть безопасными.

Литература

1. Фролова М.С. Физика и методы преподавания ее в школе // Международный журнал гуманитарных и естественных наук. 2022. № 5-1 (68). С. 276–280. DOI: 10.24412/2500-1000-2022-5-1-276-280.

2. Tsaregorodtsev, A. V. Identification and universalization of indicators of qualitative differences between media / A. V. Tsaregorodtsev, E. A. Derbin // Bulletin of Science and Education Development. – 2018. – No. 12-2. – Pp. 68-81.

3. Alex Wilkins. Quantum computers may have found a practical use. New Scientist. Vol. 257, Is. 3431, 25 March 2023, P. 14. DOI: 10.1016/S0262-4079(23)00508-0.

4. Arute F., Babbush R., Bacon D., Isakov S.V., Klimov P.V. Quantum supremacy using a programmable superconducting processor. Nature. Vol. 574, 2019. Pp. 505-510. DOI: 10.1038/s41586-019-1666-5.

5. Евсиков К.С. Информационная безопасность цифрового государства в квантовую эпоху // Вестник Университета имени О.Е. Кутафина (МГЮА). 2022. № 4 (92). С. 46–58. DOI: 10.17803/2311-5998.2022.92.4.046-058.

6. Tsaregorodtsev, A. V., Lvovich, I. Ya., Shikhaliev, M. S., Zelenina, A. N. Choporov, O. N. Information security management for cloud infrastructure // International Journal on Information Technologies and Security. 2019. T. 11 (3). CC. 91–100.

7. Физика: Справочник школьника и студента / Под ред. проф. Р. Гёбеля; Пер. с нем. – М.: Дрофа, 2003. – 368 с.

8. Skinner C. Digital Human: The Fourth Revolution of Humanity Includes Everyone. Singapore: Marshall Cavendish International (Asia), 2018. – 328 p.

9. Марков А.С., Тимофеев Ю.А. Стандарты кибербезопасности четвертой промышленной революции и Индустрии 4.0 // Защита информации. Инсайд. 2021. № 3 (99). С. 54–60.

10. Зегжда Д.П., Александрова Е.Б., Калинин М.О. и др. Кибербезопасность цифровой индустрии. Теория и практика функциональной устойчивости к кибератакам. М.: Горячая линия - Телеком, 2021. - 560 с.

11. Aditya Y. Bhargava. Grokking Algorithms. An illustrated guide for programmers and other curious people. Shelter Island, New York: Manning, 2016. – 256 p.

12. Букашкин С.А., Черепнев М.А. Квантовые устройства в криптографии // International Journal of Open Information Technologies. 2023. Т. 11. № 1. С. 104–108.

13. Корольков А.В. О некоторых прикладных аспектах квантовой криптографии в контексте развития квантовых вычислений и появления квантовых компьютеров // Вопросы кибербезопасности. 2015. № 1 (9). С. 6-13.

14. 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.

15. Петренко А.С., Петренко С.А. Метод оценивания квантовой устойчивости блокчейн-платформ // Вопросы кибербезопасности. 2022. № 3 (49). С. 2–22.

16. Петренко А.С., Петренко С.А., Ожиганова М.И. Оценка возможностей квантовых алгоритмов криптоанализа // Защита информации. Инсайд. 2021. № 6 (102). С. 70–82.

17. Petrenko A., Petrenko S. Basic Algorithms Quantum Cryptanalysis // Voprosy Kiberbezopasnosti. 2023. № 1 (53). С. 100–115.

Quantum computing and quantum computers: visualization of development, problems and prospects

Berdyugin A.A.[19], Revenkov P.V.[20]

The manuscript is of a review and analytical nature and reflects the current situation in the development of quantum computing. The relevance of the article is due to the need to popularize information technologies among young people, which is recorded in the documents of the Ministry of Digital Development, Communications and Mass Communications of the Russian Federation, as well as the high demand for experts in the field of digital technologies and the need to develop scientific and technological progress in Russia. Therefore, the purpose of the publication is to attract the reader's attention to the issues covered. The full version of the article will be published in the journal of the Higher Attestation Commission and Scopus of the National Research Nuclear University MEPhI "Scientific Visualization". The presentation materials from one of GeekBrains' educational shows "The Way to IT" were used.

Keywords: quantum, qubit, superposition, computer, state, calculation.

[19] Alexander Berdyugin, Junior researcher of the Department of Information Security, Financial University under the Government of the RF, Moscow, Russia. E-mail: aaberdyugin@fa.ru

[20] Pavel Revenkov, Dr.Ec.Sc., Assistant Professor, Professor of the Department of Information Security, Financial University under the Government of the RF, Moscow, Russia. E-mail: pavel.revenkov@mail.ru

УДК 004.056 : 519.832

Модель выбора атрибутов при многофакторной аутентификации на основе игры с нулевой суммой

Быков А.Ю.[21], **Сысоев В.В.**[22]

В статье представлена модель выбора атрибутов при многофакторной аутентификации субъектов на основе игрового подхода. Модель основана на игре двух игроков с нулевой суммой – защитника и нарушителя, показатель качества задает возможный ущерб защищаемой стороны в случае ошибок при аутентификации. Каждый из игроков должен решать свою задачу булевого программирования при фиксированном решении другого игрока. Представлены подходы к решению сформулированной задачи на основе сведения задачи к матричной игре большой размерность и возможности по решению этой игры без явного построения матрицы игры.

Ключевые слова: ошибки первого и второго родов, дискретное программирование, седловая точка

Введение

В различных информационных системах (ИС) для обеспечения безопасности информации широко используется идентификация и аутентификация субъектов (пользователей, различных программных сервисов и др.). Для повышения безопасности информации рекомендуется использовать многофакторную аутентификацию [1-4]. Некоторые другие смежные вопросы изложены в [5-7].

В «ГОСТ Р 58833–2020. Защита информации. Идентификация и аутентификация. Общие положения» определено понятие фактора как вид (форма) существования информации, используемой при идентификации и аутентификации. Введено три фактора: фактор знания (пароль, и т.п.), фактор владения (USB-токен и т.п.), биометрический фактор. Кроме понятия фактора используется понятие атрибута как признака или свойства субъекта или объекта доступа. При аутентификации по этим трем факторам можно использовать разные атрибуты. По фактору знания: пароль, парольная фраза, ПИН-код и др. По фактору владения: USB-токен, смарт-карта, ключ iButton и др. По биометрическому фактору: голос, рисунок сетчатки глаза, отпечаток пальца и др. В связи с тем, что существует множество атрибутов аутентификации возникает задача выбора этих атрибутов является актуальной. Сформулируем математическую постановку задачи выбора атрибутов при многофакторной аутентификации на основе игрового подхода. Похожая модель для клавиатурного подчерка, как дополнительного атрибута аутентификации рассмотрена в [8].

1. Математическая постановка задачи

Исходные данные

1. Основные базисные множества:

$S = \{s_1, s_2, \dots, s_n\}$ – множество субъектов ИС, $N = \{1, 2, \dots, n\}$ – множество индексов субъектов.

$A = \{a_1, a_2, \dots, a_m\}$ – множество атрибутов аутентификации, $M = \{1, 2, \dots, m\}$ – множество индексов атрибутов. Множество атрибутов и их индексов можно разбить на три непересекающихся подмножества $M = M^{(1)} \cup M^{(2)} \cup M^{(3)}$, соответствующим трем

[21]Быков Александр Юрьевич, доцент, кандидат технических наук, МГТУ им. Н.Э. Баумана, Москва, abykov@bmstu.ru
[22]Сысоев Валентин Валерьевич, МГТУ им. Н.Э. Баумана, Москва, valsus88@mail.ru

факторам аутентификации, каждый атрибут относится к одному из трех факторов аутентификации.

Также можно ввести в рассмотрение множество ресурсов защитника, требуемых для использования тех или иных атрибутов аутентификации, и множество ресурсов нарушителя, требуемых для преодоления механизмов аутентификации. Для защитника введем два ресурса: время и стоимость, для нарушителя – стоимость.

2. Параметры элементов множеств:

$p_i^{(1)} \in [0,1], \forall\, i \in M -$ вероятность ошибки первого рода (недопуск законного субъекта) при использовании *i*-го атрибута.

$p_i^{(2)} \in [0,1], \forall\, i \in M -$ вероятность ошибки второго рода (допуск нарушителя) при использовании *i*-го атрибута.

$u_j^{(1)} \geq 0, \forall\, j \in N -$ оценка ущерба в случае ошибки первого рода, для *j*-го субъекта при аутентификации, ущерб зависит от важности информации, с которой работает субъект.

$u_j^{(2)} \geq 0, \forall\, j \in N$ – оценка ущерба в случае ошибки второго рода для *j*-го субъекта.

$t_i \geq 0,\ \forall\, i \in M$ – время, затраченное на аутентификацию с использованием *i*-го атрибута.

$T_j^{(\max)}, \forall\, j \in N$ – максимальная допустимая длительность процесса аутентификации для *j*-го субъекта.

$\mathrm{c}_i \geq 0,\ \forall\, i \in M$ – стоимость реализации аутентификации по *i*-му атрибуту.

$C^{(\max)}$ – максимальная допустимая стоимость реализации аутентификации для всех субъектов.

$\mathrm{r}_i \geq 0,\ \forall\, i \in M$ – стоимость преодоления нарушителем механизмов аутентификации по *i*-му атрибуту.

$R^{(\max)}$ – максимальная допустимая стоимость для нарушителя на преодоление механизмов аутентификации для всех субъектов.

Искомые переменные

Введем булеву переменную для защитника $x_{ji} \in \{0,1\}, , \forall\, j \in N,\ i \in M, x_{ji} = 1$, если для *j*-го субъекта используется *i*-ый атрибут аутентификации, $x_{ji} = 0$ – в противном случае, переменные образуют *X* – матрицу булевых переменных.

Введем булеву переменную для нарушителя $y_j \in \{0,1\},\ , \forall\, j \in N,\ y_j = 1,$ если нарушитель будет осуществлять атаку от имени *j*-го субъекта для прохождения аутентификации, $y_j = 0$ – в противном случае, переменные образуют Y – вектор булевых переменных.

Показатель качества

Будем оценивать ущерб, связанный с возможными ошибками аутентификации. Считаем, что субъект прошел аутентификацию, если результат по всем атрибутам будет положительный. Результат аутентификации по каждому атрибуту считается независимым от других атрибутов.

Вероятность ошибки первого рода при использовании нескольких атрибутов аутентификации для *j*-го субъекта:

$$P_j^{(1)}(X) = 1 - \prod_{\substack{i=1 \\ x_{ji}=1}}^{m} \left(1 - p_j^{(1)}\right),\ \forall\, j \in N.$$

Вероятность ошибки второго рода при использовании нескольких атрибутов для *j*-го субъекта:

$$P_j^{(2)}(X, y_j) = y_j \prod_{\substack{i=1 \\ x_{ji}=1}}^{m} p_j^{(2)}, \ \forall\, i \in N.$$

При расчете вероятностей ошибок компоненты вектора *X* присутствуют только под знаком произведения, $x_{ji} = 1$ означает, что в произведении участвуют только множители, для которых компоненты *X* равны 1.

Оценка среднего ущерба будет:

$$U(X, Y) = \sum_{j \epsilon N}\left[u_j^{(1)} P_j^{(1)}(\mathrm{X}) + u_j^{(2)} P_j^{(2)}(\mathrm{X}, y_j)\right] \quad (1)$$

Данный показатель защитник желает минимизировать, а нарушитель максимизировать.

Ограничения для защитника

Ограничения на то, что для каждого субъекта используется хотя бы один атрибут (в произведениях при расчете ошибок будет хотя бы один множитель):

$$\sum_{i \epsilon M} x_{ji} \geq 1, \forall j \in N. \quad (2)$$

Ограничения на то, что для каждого фактора аутентификации используется не более одного атрибута:

$$\sum_{i \,\epsilon\, M^{(k)}} x_{ji} \leq 1, \forall j \in N, k \in \{1, 2, 3\}. \quad (3)$$

Ограничения на допустимое время прохождения аутентификации для каждого пользователя:

$$\sum_{i \epsilon M} t_i \, x_{ji} \leq T_j^{(\max)}, \forall j \in N. \quad (4)$$

Ограничение на стоимость реализации аутентификации:

$$\sum_{j \epsilon N} \sum_{i \epsilon M} c_i x_{ji} \leq C^{(\max)} . \quad (5)$$

Ограничения для нарушителя

Ограничение на стоимость преодоления механизмов аутентификации:

$$\sum_{j \epsilon N} \sum_{i \epsilon M} r_i x_{ji} y_j \leq R^{(\max)} . \quad (6)$$

Обобщенные постановки задач

Защитник при фиксированном решении нарушителя (векторе *Y*) решает следующую задачу:

$$U(X, Y) \rightarrow \min_{X \in \Delta_{\text{доп}}^{(\text{з})}(X)},$$

где $\Delta_{\text{доп}}^{(\text{з})}(X)$ – множество допустимых альтернатив защитника, определяемых ограничениями (2) – (5):

$$\Delta_{\text{доп}}^{(\text{з})}(X): \begin{cases} \sum_{i \epsilon M} x_{ji} \geq 1, \forall\, j \in N, \\ \sum_{i \,\epsilon\, M^{(k)}} x_{ji} \leq 1, \forall j \in N, k \in \{1, 2, 3\}, \\ \sum_{i \epsilon M} t_i \, x_{ji} \leq T_j^{(\max)}, \forall\, j \in N, \\ \sum_{j \epsilon N} \sum_{i \epsilon M} c_i x_{ji} \leq C^{(\max)} . \end{cases}$$

Поставленная задача является задачей булева программирования с нелинейным по *X* показателем качества (1) и линейными ограничениями (2) – (5).

Нарушитель при фиксированном решении защитника (матрице *X*) решает следующую задачу:

$$U(X, Y) \rightarrow \max_{Y \in \Delta_{\text{доп}}^{(\text{н})}(X, Y)},$$

где $\Delta_{\text{доп}}^{(\text{н})}(X, Y)$ – множество допустимых альтернатив нарушителя, определяемых ограничением (6):

$$\Delta_{\text{доп}}^{(\text{н})}(X, Y): \left\{ \sum_{j \epsilon N} \sum_{i \epsilon M} r_i x_{ji} y_j \leq R^{(\max)} . \right.$$

Поставленная задача является задачей булева программирования с линейным по Y показателем качества (1) и линейным ограничением (6).

2. О методах решения

Так как каждый из игроков решает задачу булевого программирования и число допустимых решений у каждого из игроков конечно, то задачу можно свести к обычной матричной игре: строки задают допустимые решения нарушителя, а столбцы задают допустимые решения защитника, но размерность матрицы может быть относительно большой.

Для матричной игры можно найти минимакс для защитника, если использовать принцип гарантированного результата: $U(X,Y) \to \min\limits_{X} \max\limits_{Y}$, а также седловую точку игры в чистых стратегиях, если она существует, когда минимакс равен максимину, или в смешанных стратегиях, в противном случае. Для поиска седловой точки в смешанных стратегиях существуют как точные, так и приближенные методы. Наиболее распространённый точный метод сводится к решению прямой и двойственной задач линейного программирования [9], а один из часто используемых приближенных методов – метод Брауна-Робинсона [9], основной недостаток которого – медленная сходимость.

В [10] рассмотрена модификация приближенного метода Брауна-Робинсона для поиска седловой точки в смешанных стратегиях, но без явного построения матрицы игры. В [11] рассмотрена непрерывная задача, которая также сводилась к матричной, и использовался модифицированный метод Брауна-Робинсона.

Выводы

Сформулирована математическая постановка выбора атрибутов аутентификации, относящихся к разным факторам, при многофакторной аутентификации. Задача является игрой двух игроков: защитник выбирает атрибуты аутентификации для субъектов ИС, а нарушитель выбирает субъектов, от имени которых желает пройти аутентификация. Игра является игрой с нулевой суммой, каждый игрок должен решить задачу булевого программирования при фиксированном решении другого игрока.

Для решения задачи показано, как задачу свести к матричной игре, которая может иметь большую размерность. Для нахождения седловой точки предложена модификация метода Брауна-Робинсона, но без явного построения матрицы игры.

Использование предложенного алгоритма позволяет при выборе факторов (атрибутов) аутентификации снизить возможный ущерб, связанный с ошибками аутентификации первого и второго родов.

Достоверность полученных результатов подтверждается корректностью математической постановки задачи, явной содержательной интерпретацией, как постановки задачи, так и получаемых решений.

Литература

1. Казанцев И.С. О возможном подходе к аутентификации пользователя по клавиатурному почерку на основе ПЭМИ клавиатуры // Безопасные информационные технологии. Сборник трудов XI международной научно-технической конференции. – М.: МГТУ им. Н.Э. Баумана, 2021. С. 130–134.

2. Крутохвостов Д.С., Хиценко В.Е. Парольная и непрерывная аутентификация по клавиатурному почерку средствами математической статистики // Вопросы кибербезопасности. 2017. № 5 (24). С. 91–99.

3. Ложников П.С., Сулавко А.Е., Бурая Е.В., Писаренко В.Ю. Аутентификация пользователей компьютера на основе клавиатурного почерка и особенностей лица // Вопросы кибербезопасности. 2017. № 3 (21). С. 24–34.

4. Коннова Н.С., Сафина А.Д. Использование нейросетевых методов и атомарных функций в задаче биометрической аутентификации по ЭКГ // Безопасные информационные технологии. Сборник трудов XI международной научно-технической конференции. – М.: МГТУ им. Н.Э. Баумана, 2021. С. 165–172.

5. Басараб М.А., Троицкий И.И., Онуфриева Е.В. Исследование функционирования SIEM-систем с помощью различных корреляторов для бинарных последовательностей вида (1, - 1) при условии, что случайные величины принимают свои значения с одинаковыми вероятностями. Безопасные информационные технологии. Сборник трудов Одиннадцатой международной научно-технической конференции. М.: МГТУ им. Н.Э. Баумана, 2021. С. 32–36.

6. Ключарёв П.Г. Клеточные автоматы и их обобщения в задачах криптографии. Часть 1 // Вопросы кибербезопасности. 2021. № 6 (46). С. 90-101. DOI: 10.21681/2311-3456-2021-6-90-101

7. Ключарёв П.Г. Клеточные автоматы и их обобщения в задачах криптографии. Часть 2 // Вопросы кибербезопасности. 2022. № 1 (47). С. 37-48. DOI: 10.21681/2311-3456-2022-1-37-48

8. Быков А.Ю., Акулова Н.О. Игровая постановка задачи выбора дополнительного фактора аутентификации для рабочих мест на примере клавиатурного почерка // Безопасные информационные технологии. Сборник трудов Десятой международной научно-технической конференции. – М.: МГТУ им. Н.Э. Баумана, 2019. С. 46–50.

9. Стрекаловский А.С., Орлов А.В. Биматричные игры и билинейное программирование. М.: Физматлит, 2007. 224 с.

10. Быков А.Ю., Гришунин М.В., Крыгин И.А. Игровая задача выбора защищаемых объектов и исследование алгоритма поиска седловой точки на основе модификации метода Брауна-Робинсона // Вопросы кибербезопасности. 2019. № 2 (30). С. 2–12. DOI: 10.21681/2311-3456-2019-2-2-12

11. Быков А.Ю., Крыгин И.А., Гришунин М.В., Маркова И.А. Об одном алгоритме поиска седловой точки для непрерывных линейных игр применительно к задачам защиты информации // Вестник МГТУ им. Н.Э. Баумана. Серия: Приборостроение. 2020. № 4. С. 58–74. DOI: 10.18698/0236-3933-2020-4-58-74

Attribute Selection Model for Multifactor Authentication Based on Zero-Sum Game

Bykov A.Yu. [23]**, Sysoev V.V.** [24]**,**

The article presents a model for attribute selection in multifactor authentication of subjects based on a game approach. The model is based on a two-player zero-sum game - a defender and an intruder. Where the quality indicator of the model is the possible damage in case of authentication errors. Each of the players must solve their Boolean programming problem with a fixed solution of the other player. Approaches to solving the problem are presented based on reducing the problem to a large-scale matrix game and solving this game without constructing the game matrix. *Keywords: Type I and type II errors, discrete optimization, saddle point.*

[23]Aleksandr Bykov, Associated Professor, Ph.D., Bauman Moscow State Technical University, Moscow, abykov@bmstu.ru

[24]Valentin Sysoev, Bauman Moscow State Technical University, Moscow, valsus88@mail.ru

УДК 004.056

Разработка SAT-решателя для криптоанализа алгоритмов симметричного шифрования

Васютин Р. Р.[25]**, Ключарёв П. Г.** [26]

Статья посвящена разработке и реализации эвристики расщепления, применение которой в SAT-решателе позволило достичь значительного прироста производительности процедуры поиска выполняющего набора в задаче криптоанализа алгоритма симметричного шифрования CTC2. Среднее ускорение в зависимости от условий проведённых экспериментов варьируется в диапазоне от 24 до 62%, существенно сократилось и число возникающих конфликтов (от 44 до 74%). Разработанный SAT-решатель и система тестирования результатов могут быть использованы для криптоанализа иных алгоритмов, а также как отправная точка в задачах поиска эффективных способов решения задачи SAT.

Ключевые слова: SAT, MiniSAT, CDCL, логический криптоанализ, CTC2, эвристика расщепления

Введение

Задача выполнимости (SAT) для данной булевой формулы заключается в поиске набора переменных, на котором она обращается в единицу. Такой набор называется выполняющим. Если он существует, то формула называется выполнимой [1].

SAT-решателем называется программа, которая позволяет найти выполняющий набор, если он существует, или сообщить, что переданная на вход булева формула не является выполнимой. SAT-решатели фокусируются на задаче в конъюнктивной нормальной форме (КНФ) [2]. Задача о КНФ-выполнимости является NP-полной.

Впервые постановка задачи криптоанализа как SAT-задачи была приведена в [3], в этой же работе данный метод криптоанализа получил название «логический криптоанализ». Основу логического криптоанализа составляют процедуры трансляции алгоритмов шифрования в логические выражения, представленные в КНФ, а также алгоритмы и технологии решения получаемых SAT-задач (задачи поиска секретного ключа ставятся как SAT-задачи) [4].

В общем случае любой алгоритм шифрования разрабатывается так, чтобы он был устойчив к попыткам взлома с учетом анализа с известным открытым текстом, поэтому в данной работе выполняется логический криптоанализ с известным открытым текстом. SAT-решатели предназначены для широкого круга задач, что приводит к необходимости разработки собственной вариации, адаптированной к решению конкретной задачи.

Разработка SAT-решателя

Основные алгоритмы, которые используются для построения SAT-решателей, включают DPLL [5], CDCL [6], GSAT [7] и др.

В качестве базового решения, на основе которого будет построен проектируемый SAT-решатель, предлагается проект MiniSAT [8], реализованный с использованием алгоритма CDCL.

[25] Васютин Роман Романович, аспирант, МГТУ им. Н. Э. Баумана, Москва, vrr17u408@student.bmstu.ru
[26] Ключарёв Петр Георгиевич, доктор технических наук, доцент, МГТУ им. Н. Э. Баумана, Москва, pk.iu8@yandex.ru

Производительность SAT-решателя данного типа определяется эвристикой расщепления, методом распространения булевых ограничений и анализа конфликтов.

В MiniSAT используется динамическая эвристика, называемая VSIDS [9]: для каждого литерала (переменной или её отрицания) создается счетчик, который увеличивается на 1 при попадании литерала в конфликтную элементарную дизъюнкцию. Элементарную дизъюнкцию также называют клозом. Для расщепления выбирается литерал с максимальным значением счетчика.

В качестве механизма анализа конфликтов в MiniSAT используется нехронологический возврат [8], обучающая процедура которого заключается в добавлении нового ограничения – обучающего клоза – элементарной дизъюнкции, запрещающей присвоения, ставшие причиной конфликта.

В работе [8] утверждается, что эвристика расщепления в основном определяет эффективность SAT-решателя, поэтому именно её и было решено модифицировать. В процессе разработки экспериментальным путем был найден наиболее эффективный подход (рис.1):

1. Для начала применяется эвристика VSIDS. В результате формируется рейтинг активности по каждой переменной в соответствии с частотой их присутствия в конфликтных клозах.
2. Выбирается лидирующая часть ($\alpha\%$) от рейтинга VSIDS, сформированного на шаге 1, для проверки наличия в наибольшем количестве коротких клозов с целью последующего их сокращения и, как следствие, ускорения поиска решения. Этот подход реализуется следующим образом:

a) Для каждой из переменных лидирующей части рейтинга активности, построенного с использованием эвристики VSIDS на шаге 1, вычисляется частота встречаемости по формулам (1), которые используются в эвристике Джереслоу-Вана [10], однако с анализом лишь обучающих клозов:

$$J(x) = \sum_{x \in c, c \in F} 2^{-|c|}, \qquad J(\bar{x}) = \sum_{\bar{x} \in c, c \in F} 2^{-|c|}, \tag{1}$$

где F – множество обучающих клозов, c – обучающий клоз.

Подсчет происходит по стартовому состоянию КНФ, то есть результаты конфликтов анализу не подлежат. В данном варианте реализации происходит оценка не всех переменных, а только α процентов лидеров рейтинга активности, что значительно повышает эффективность решения**.**

b) Переменная с максимальным значением $J(x) + J(\bar{x})$ выбирается следующей переменной для расщепления.

Итак, предложенная динамическая эвристика ищет и расщепляет переменные, которые чаще остальных встречаются в коротких **обучающих** клозах, следовательно, направлена на ускорение процесса сокращения обучающих клозов.

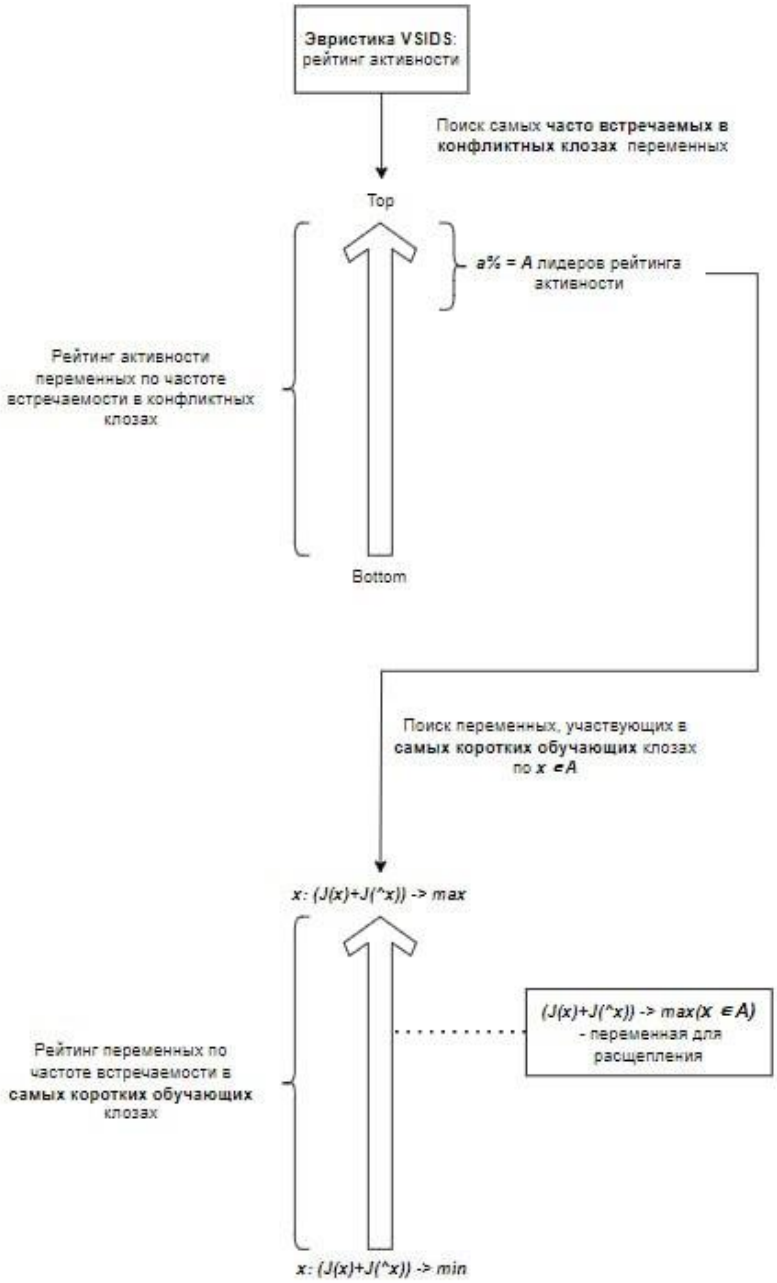


*Рис.1. Выбор переменной по эвристике (^**x** – обозначение инверсии **x**)*

Криптоанализ CTC2

Для целей данной работы был выбран блочный шифр CTC2 (Courtois Toy Cipher). Основным критерием выбора алгоритма шифрования являлась возможность динамического изменения его параметров: длины ключа и количества раундов.

Было выполнено описание алгоритма шифрования CTC2 на языке Transalg [11], а также подготовлена программа для быстрой генерации тестовых данных по размеру ключа и количеству раундов.

Далее представлены результаты сравнения двух SAT-решателей: реализованного в рамках данной работы (CurrSAT) и MiniSAT.

Сравнение №1

В данном сравнении (табл.1) были проведены испытания SAT-решателей при длине ключа, составляющей 24 бита, числе раундов, равном 4, на процессоре 11th Gen Intel(R) Core(TM) i7-1165G7 @ 2.80GHz.

Таблица 1.

Сравнение №1: CTC2

№	Процессорное время, с			Конфликты		
	MiniSAT	**CurrSAT**	MiniSAT / **CurrSAT**	MiniSAT	**CurrSAT**	MiniSAT / **CurrSAT**
1	154,1	**72,15**	2,1	10186514	**5258910**	1,94
2	72,25	**101**	0,71	4630224	**6155940**	0,75
3	100,93	**59,1**	1,71	8094560	**3534005**	2,29
4	76,95	**27,8**	2,7	5145767	**1673453**	3
5	63,81	**110,5**	0,58	4202691	**6155673**	0,68
6	69,86	**36,6**	1,94	4608949	**2539330**	1,8

Среднее время поиска решения с использованием SAT-решателя, разработанного в рамках данной работы, сократилось **в 1,62 раза**, а среднее число конфликтов - в **1,74 раза**.

Сравнение №2

В данном сравнении (табл.2) были проведены испытания SAT-решателей при различной длине ключа, числе раундов, равном 4, на процессоре 11th Gen Intel(R) Core(TM) i7-1165G7 @ 2.80GHz.

Таблица 2.

Сравнение №2: CTC2

№	Ключ, бит	Процессорное время, с			Конфликты		
		MiniSAT	**CurrSAT**	MiniSAT / **CurrSAT**	MiniSAT	**CurrSAT**	MiniSAT / **CurrSAT**
1	18	0,84	**0,85**	0,99	89 471	**66 360**	1,35
2	21	3	**3.8**	0,79	273020	**292470**	0,93
3	24	57,6	**36,2**	1,59	3 367 260	**1 784 800**	1,88
4	27	110	**75,3**	1,46	6 513 766	**3 810 666**	1,71
5	30	206	**162**	1,27	9 470 000	**6 815 000**	1,39
6	33	7 369	**6 086**	1,21	244 681 129	**182 369 795**	1,34
7	36	242056	**178368**	1,36	5 667 203 620	**3 896 389 601**	1,45

Среднее время поиска решения с использованием SAT-решателя, разработанного в рамках данной работы, сократилось **в 1,24 раза** (рис.2), а среднее число конфликтов - в **1,44 раза** (рис.3).

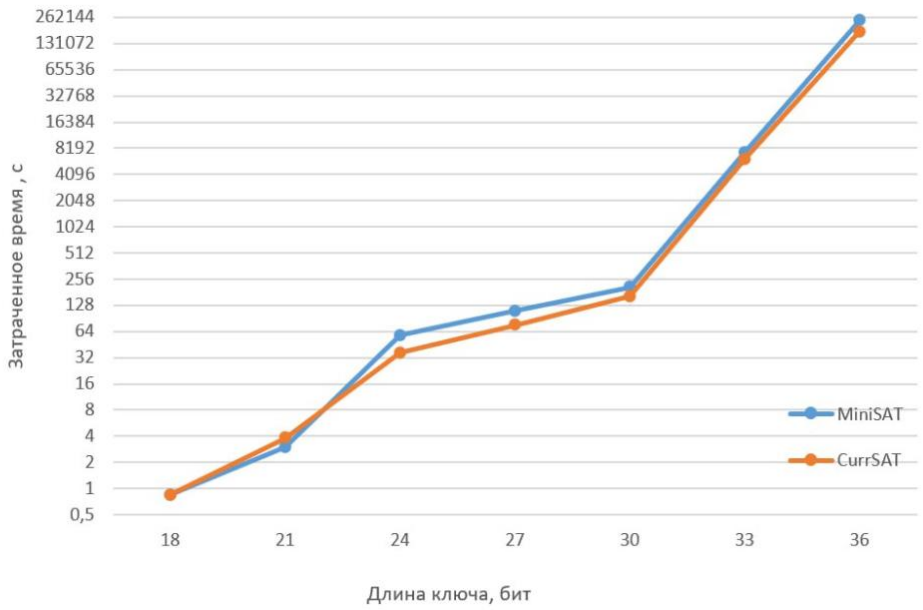


Рис.2. Сравнение №2: CTC2 (время)

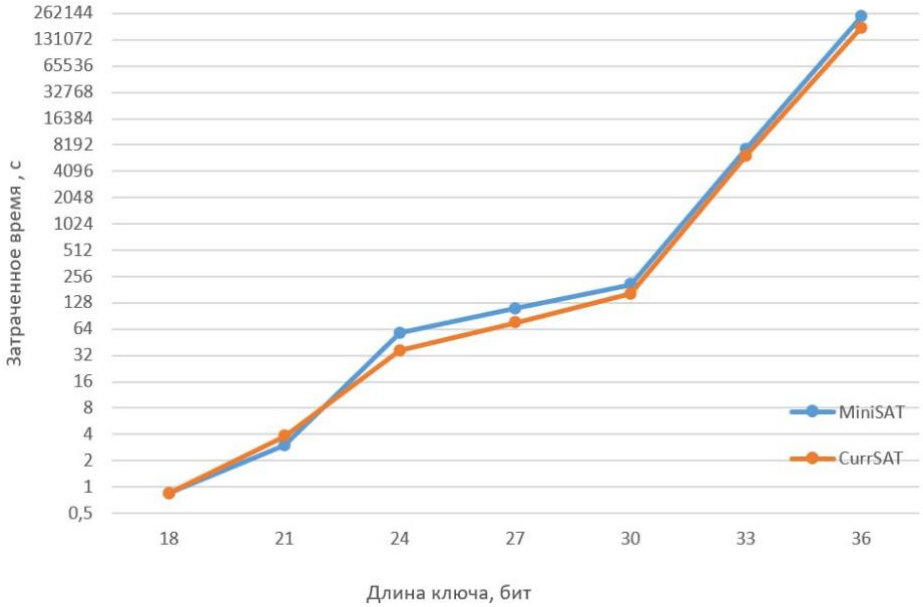


Рис.3. Сравнение №2: CTC2 (число конфликтов)

Вывод

В данной работе кратко изложены основные результаты, полученные в рамках разработки и реализации эвристика расщепления SAT-решателя, направленной на ускорение процесса сокращения обучающих клозов, реализован алгоритм симметричного шифрования CTC2 на языке Transalg, подготовлена программа для быстрой генерации тестовых данных по размеру ключа и количеству раундов, продемонстрирована эффективность предлагаемой эвристики: средний прирост скорости поиска выполняющего набора при фиксированных длине ключа и числе раундов составил около 62%, при динамической длине ключа и фиксированном числе раундов – 24%. Среднее уменьшение числа конфликтов составило 74 и 44% соответственно.

Предлагаемые научные решения подтверждается результатами вычислительных экспериментов.

Литература

1. Du D. et al. (ed.). Satisfiability problem: theory and applications: DIMACS Workshop, March 11-13, 1996. – American Mathematical Soc., 1997. – Т. 35.

2. Богданов Д. С., Ляпунова И. А., Тетруашвили Е. В. Задача разработки SAT-решателя для поиска верификационных наборов в тестирования программного обеспечения // Инженерный вестник Дона. – 2017. – Т. 47. – №. 4 (47).

3. Agrawal M., Kayal N., Saxena N. PRIMES is in P //Annals of mathematics. – 2004. – С. 781-793.

4. Посыпкин М. А. и др. Решение задач криптоанализа поточных шифров в распределенных вычислительных средах // Труды Института системного анализа Российской академии наук. – 2009. – Т. 46. – С. 119–137.

5. Nieuwenhuis R., Oliveras A., Tinelli C. Abstract DPLL and abstract DPLL modulo theories // International Conference on Logic for Programming Artificial Intelligence and Reasoning. – Springer, Berlin, Heidelberg, 2005. – С. 36-50.

6. Marques-Silva J., Lynce I., Malik S. Conflict-driven clause learning SAT solvers // Handbook of satisfiability. – ios Press, 2021. – С. 133-182.

7. Selman B. et al. Domain-independent extensions to GSAT: Solving large structured satisfiability problems // IJCAI. – 1993. – Т. 93. – С. 290-295.

8. Eén N., Sörensson N. An extensible SAT-solver //International conference on theory and applications of satisfiability testing. – Springer, Berlin, Heidelberg, 2003. – С. 502-518.

9. Liang J. H. et al. Understanding VSIDS branching heuristics in conflict-driven clause-learning SAT solvers // Hardware and Software: Verification and Testing: 11th International Haifa Verification Conference, HVC 2015, Haifa, Israel, November 17-19, 2015, Proceedings 11. – Springer International Publishing, 2015. – С. 225-241.

10. Jeroslow R. G., Wang J. Solving propositional satisfiability problems // Annals of mathematics and Artificial Intelligence. – 1990. – Т. 1. – №. 1. – С. 167-187.

11. Otpuschennikov I., Semenov A., Kochemazov S. Transalg: a Tool for Translating Procedural Descriptions of Discrete Functions to SAT // arXiv preprint arXiv:1405.1544. – 2014.

Development of a SAT solver for cryptanalysis of symmetric encryption algorithms

Vasyutin R. R. [27]**, Klyucharev P. G.,**[28]

Abstract. In this article a splitting heuristic was developed and implemented, the use of which in the SAT solver made it possible to achieve a significant increase in the performance of the search procedure for the satisfying assignment in the cryptanalysis task of the CTC2 symmetric encryption algorithm. The average acceleration, depending on the conditions of the experiments, varies from 24 to 62%, and the number of conflicts has also significantly decreased (from 44 to 74%). The developed SAT solver and the testing system can be used for cryptanalysis of other algorithms, as well as a starting point in the search for effective ways to solve the SAT problem.

Keywords SAT, MiniSat, CDCL, logical cryptanalysis, CTC2, splitting heuristics.

[27] Roman Vasyutin, Ph.D. student, Bauman Moscow State Technical University, Moscow, aap17u214@student.bmstu.ru

[28] Peter Klyucharev, Dr.Sc.., Professor, Bauman Moscow State Technical University, Moscow, pk.iu8@yandex.ru

УДК 004.056

Оптимизация постквантового криптографического протокола, основанного на изогениях суперсингулярных эллиптических кривых

Васютина А. П.[29], **Ключарёв П. Г.** [30]

В статье приведен результат решения задачи по оптимизации постквантового протокола выработки общего секретного ключа CTIDH, основанного на аппарате изогений суперсингулярных эллиптических кривых, – вариации протокола CSIDH с особым ключевым пространством. В рамках выполнения работы было достигнуто 20-процентное ускорение процедуры получения общего секрета участниками взаимодействия благодаря интеграции в решение параллельного алгоритма Монтгомери, реализованного с использованием векторных инструкций семейства AVX-256 процессоров Intel на языке Assembler. Полученные результаты могут быть использованы для улучшения производительности схемы как в текущих конфигурациях, так и при увеличении размеров ключей.

Ключевые слова: CSIDH, CTIDH, постквантовая криптография, выработка общего секретного ключа, алгоритм умножения Монтгомери, векторные инструкции, AVX-256, Intel.

Введение

Стремительное развитие квантовых компьютеров, которые при достижении определенного объема квантовой памяти смогут выполнить решение сложных задач, лежащих в основе современных механизмов обеспечения кибербезопасности, актуализирует проблему поиска и разработки постквантовых криптографических алгоритмов и протоколов, которые придут на смену используемым сегодня схемам, в частности – задачу замены математического аппарата в протоколах выработки общего секретного ключа. Одним из кандидатов на данную роль является протокол CSIDH, впервые представленный в [1], базирующийся на изогениях суперсингулярных эллиптических кривых.

Ключевые характеристики протокола, помимо обеспечиваемого уровня криптографической стойкости, включают скорость выработки общего секретного ключа участниками взаимодействия. Данная работа посвящена разработке и реализации временной оптимизации протокола CSIDH с использованием программно-аппаратных средств – инструкций семейства AVX-256 процессоров Intel.

Протокол CSIDH

Процесс генерации общего секретного ключа может быть представлен в виде схемы (рис.1).

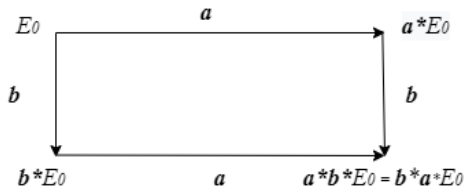


Рис.1. CSIDH: выработка общего секретного ключа

Вычисления в протоколе производятся над конечным полем $\mathbb{F}_p$, где p – простое число, представимое в виде:

[29] Васютина Анастасия Петровна, аспирант, ассистент, МГТУ им. Н. Э. Баумана, Москва, aap17u214@student.bmstu.ru

[30] Ключарёв Пётр Георгиевич, доктор технических наук, доцент, МГТУ им. Н. Э. Баумана, Москва, pk.iu8@yandex.ru

$$p = 4\prod_{i=1}^{n} l_i - 1, \quad (1)$$

при этом $l_1, \dots, l_n$ – набор небольших простых чисел, $l_i \neq 2, p \equiv -1(mod\ l_i), p \equiv 11\ (mod\ 12), p \equiv 3(mod\ 8)$.

Стартовая суперсингулярная эллиптическая кривая E_0 над полем $\mathbb{F}_p$ с кольцом эндоморфизмов $\mathbb{Z}\left[\sqrt{-p}\right]$ задается в форме Монтгомери [2]:

$$E_0/\mathbb{F}_p: y^2 = x^3 + x \quad (2)$$

Приватный ключ первого участника взаимодействия – это набор чисел $(e_{a_1}, e_{a_2}, \dots, e_{a_n})$, каждое из которых выбрано случайно и равновероятно из диапазона $\{-m, \dots, m\}$, где m выбирается с учетом условия:

$$n\ log(2m+1) \approx log\sqrt{p} \quad (3)$$

и числа определяют класс идеалов [3], представленный в виде:

$$\boldsymbol{a} = \left[\boldsymbol{l_1^{e_{a_1}}}, \dots, \boldsymbol{l_n^{e_{a_n}}}\right] \in cl\left(\mathbb{Z}\left[\sqrt{-p}\right]\right) \quad (4)$$

где $\boldsymbol{l_i} = (l_i, \pi - 1)$, π – эндоморфизм Фробениуса, $cl\left(\mathbb{Z}\left[\sqrt{-p}\right]\right)$ – группа классов идеалов кольца $\mathbb{Z}\left[\sqrt{-p}\right]$. Аналогично получен и класс идеалов $\boldsymbol{b}$, определенный приватным ключом второго участника взаимодействия.

Оператором ***** обозначено групповое действие группы классов идеалов кольца эндоморфизмов суперсингулярных эллиптических кривых вида:

$$E_A/\mathbb{F}_p: y^2 = x^3 + Ax^2 + x, A \in \mathbb{F}_p, \quad (5)$$

то есть $cl\left(\mathbb{Z}\left[\sqrt{-p}\right]\right)$ [3], на множестве всех суперсингулярных эллиптических кривых вида (5).

Таким образом, публичными ключами являются коэффициенты эллиптических кривых $\boldsymbol{a} * E_0$ и $\boldsymbol{b} * E_0$. Восстановление приватного ключа по публичным при этом является вычислительно сложной задачей. Общим секретным ключом служит коэффициент кривой, вычисленной с использованием выражения:

$$\boldsymbol{a} * \boldsymbol{b} * E_0 = \boldsymbol{b} * \boldsymbol{a} * E_0 \quad (6)$$

Протокол CTIDH является вариацией протокола CSIDH с особым пространством ключей и, как следствие, адаптированным под это пространство способом вычисления группового действия [4]. Данный протокол продемонстрировал лучшие показатели производительности, поэтому было принято решение выполнять оптимизацию именно этой версии. Актуальность оптимизации подтверждается приведенной в [5] квантовой атакой, демонстрирующей, что предложенные авторами параметры не соответствуют ожидаемым уровням безопасности, а значит, требуется увеличение размеров ключей, что приведет к общему замедлению протокола.

Оптимизация алгоритма вычисления Монтгомери с использованием AVX-инструкций

Авторами программы CTIDH [6] предусмотрен инструмент профилирования, запуск которого показал, что 78% времени вычисления общего секретного ключа занимает умножение в конечном поле $\mathbb{F}_p$, что определяет главную область оптимизации – повышение производительности этой операции.

В реализации протокола CTIDH используется алгоритм умножения Монтгомери (классическая версия), впервые представленный в [7], который позволяет ускорить выполнение операций умножения и возведения в степень по модулю, детальное исследование производительности было выполнено в [8]. В работе [4] была предложена идея параллельного алгоритма вычисления умножения Монтгомери с использованием SIMD-инструкций (SSE), приведены данные о производительности, демонстрирующие, что

в таком случае скорость работы увеличивается в 2 раза по сравнению с последовательными версиями.

Технология SIMD реализует одиночный поток команд и множественный поток данных, что позволяет выполнять параллельно основные операции с векторами данных. Компания Intel представила набор инструкций SSE (SIMD) в 1999 году, в современных процессорах интегрирован AVX-256 – развитие SSE, включающее 16 256-битных регистров.

В рамках данной работы была выполнена адаптация параллельного алгоритма Монтгомери к семейству команд AVX-256. Максимальный размер вектора данных, в котором поддерживаются все необходимые операции, составляет 52 бита.

Результат оптимизации

В результате оптимизации удалось достигнуть 18–20% ускорения (табл.1).

Таблица 1.

Результат оптимизации протокола CTIDH

Протокол	CTIDH (оригинальный), млн тактов процессора	CTIDH (данная работа), млн тактов процессора	Ускорение, %
CTIDH-512	121,8	96,7	20,6
CTIDH-1024	567,5	456,1	19,6
CTIDH-2048	2278,8	1846,4	18,9

Тестирование производилось на процессоре Intel 11th Gen Intel(R) Core(TM) i7-1165G7. Тестовая программа запускалась с параметром повторения 100 для набора из 65 случайных ключей. В качестве результата в таблицу были внесены средние значения из 65000 проведенных экспериментов.

Было выполнено сравнение времени работы существующих реализаций протокола CSIDH-512, включающий разработанный в рамках данной работы (табл.2).

Таблица 2.

Сравнение производительности CSIDH-512

Протокол	Время работы, млн тактов процессора
CSIDH-512 [4]	121,80
CSIDH-512 [9]	218,42
CSIDH-512 [10]	238,51
CSIDH-512 [11]	239,00
CSIDH-512 (данная работа)	96,70

Вывод

В рамках данной работы кратко изложены основные результаты проведенной адаптации и реализации параллельного алгоритма Монтгомери для семейства команд AVX-256 на языке Assembler (с учетом необходимости обеспечения устойчивости к атакам по времени), а также его интеграция в протокол выработки общего секретного ключа CSIDH, что позволило достичь 20-процентного увеличения производительности решения (по сравнению с первоначальной реализацией).

Достоверность данного научного исследования подтверждается результатами вычислительных экспериментов.

Литература

1. Castryck W. et al. CSIDH: an efficient post-quantum commutative group action //Advances in Cryptology–ASIACRYPT 2018: 24th International Conference on the Theory and Application of Cryptology and Information Security, Brisbane, QLD, Australia, December 2–6, 2018, Proceedings, Part III 24. – Springer International Publishing, 2018. – С. 395-427.

2. Delfs C., Galbraith S. D. Computing isogenies between supersingular elliptic curves over $\mathbb{F}_p$ //Designs, Codes and Cryptography. – 2016. – Т. 78. – С. 425-440.

3. Chevyrev I., Galbraith S. D. Constructing supersingular elliptic curves with a given endomorphism ring //LMS Journal of Computation and Mathematics. – 2014. – Т. 17. – №. A. – С. 71-91.

4. Banegas G. et al. CTIDH: faster constant-time CSIDH //Cryptology ePrint Archive. – 2021.

5. Bonnetain X., Schrottenloher A. Quantum security analysis of CSIDH //Annual International Conference on the Theory and Applications of Cryptographic Techniques. – Springer, Cham, 2020. – С. 493-522.

6. Montgomery P. L. Modular multiplication without trial division //Mathematics of computation. – 1985. – Т. 44. – №. 170. – С. 519-521.

7. Koc C. K., Acar T., Kaliski B. S. Analyzing and comparing Montgomery multiplication algorithms //IEEE micro. – 1996. – Т. 16. – №. 3. – С. 26-33.

8. Bos J. W. et al. Montgomery multiplication using vector instructions //Selected Areas in Cryptography–SAC 2013: 20th International Conference, Burnaby, BC, Canada, August 14-16, 2013, Revised Selected Papers 20. – Springer Berlin Heidelberg, 2014. – С. 471-489.

9. Chi-Domínguez J. J., Rodríguez-Henríquez F. Optimal strategies for CSIDH //Advances in Mathematics of Communications. – 2020.

10. Hutchinson A. et al. Further optimizations of CSIDH: a systematic approach to efficient strategies, permutations, and bound vectors //International Conference on Applied Cryptography and Network Security. – Springer, Cham, 2020. – С. 481-501.

11. Cervantes-Vázquez D. et al. Stronger and faster side-channel protections for CSIDH //International Conference on Cryptology and Information Security in Latin America. – Springer, Cham, 2019. – С. 173-193.

Optimization of a post-quantum cryptographic protocol based on isogeny of supersingular elliptic curves

Vasyutina A. P. [31], **Klyucharev P. G.**[32]

Abstract. The article presents the result of solving the problem of optimizing the post–quantum protocol for generating a common secret key CTIDH, based on the isogeny of supersingular elliptic curves, a variation of the CSIDH protocol with a special key space. As part of the work, a 20 percent acceleration of the procedure for obtaining a common secret by the interaction participants was achieved due to the integration into the solution of the parallel Montgomery algorithm implemented using vector instructions of the AVX-256 family of Intel processors in the Assembler language. The results obtained can be used to improve the performance of the scheme both in current configurations and with increasing key sizes.

Keywords CSIDH, CTIDH, post-quantum cryptography, generation of a common secret key, Montgomery multiplication algorithm, vector instructions, AVX-256, Intel.

[31] Anastasia Vasyutina, Ph.D. student, Assistant Lecturer, Bauman Moscow State Technical University, Moscow, aap17u214@student.bmstu.ru

[32] Peter Klyucharev, Dr.Sc., Professor, Bauman Moscow State Technical University, Moscow, pk.iu8@yandex.ru

УДК 004.832

Задачи информационной безопасности систем искусственного интеллекта

Гарбук С.В.[33]

Аннотация. В статье рассматриваются научно-технические и нормативно-технические задачи в области информационной безопасности, специфичные для методов машинного обучения. Решение этих задач способствует повышению эффективности применения систем искусственного интеллекта на основе машинного обучения за счет устранения рисков, связанных с нарушением функциональности и компрометации данных в системах.

Ключевые слова: искусственный интеллект, функциональная корректность систем, конфиденциальность данных, риски применения, машинное обучение, информационная безопасность.

Бурное развитие технологий искусственного интеллекта (ИИ) на основе алгоритмов машинного обучения (МО) предполагает адекватное совершенствование нормативной базы, средств и методов защиты информации в системах ИИ. Для этого необходимо рассмотреть два взаимосвязанных технологических аспекта:

- обеспечение безопасности информации, обрабатываемой в системах ИИ;
- применение технологий ИИ в средствах информационной безопасности (ИБ).

Особенности защиты информации в СИИ удобно рассмотреть с помощью модели жизненного цикла (ЖЦ) типовой системы ИИ (рис.1), предложенной в [1]. На разных этапах ЖЦ СИИ используются различные информационные компоненты (данные, формализованные описания, модели), необходимые для успешной реализации этих этапов:

1) функциональные требования к системам (ФТ) [2];

2) описание предусмотренных условий эксплуатации (ПУЭ), в общем случае заданное многомерной плотностью распределения существенных факторов эксплуатации (СФЭ) СИИ;

3) эталонные архитектуры программного обеспечения, реализующего алгоритмы МО;

4) обучающие НД;

5) тестовые НД;

6) входные данные;

7) НД для дообучения СИИ.

Будем считать, что требования к информационным компонентам могут быть двух видов:

требования целостности i, заключающиеся в корректности формирования информационной компоненты и в предотвращении её умышленных и непреднамеренных искажений;

требования конфиденциальности c, заключающиеся в предотвращении компрометации (несанкционированного доступа) к содержимому компоненты лиц, заинтересованных и способных негативно повлиять на качество и безопасность СИИ.

Анализ рисков, проявляющихся при невыполнении требований, показывает, что возможными негативными последствиями, обусловленными несоответствием требованиям, специфичных для СИИ на основе алгоритмов МО, являются:

[33] Гарбук Сергей Владимирович, кандидат технических наук, старший научный сотрудник, НИУ ВШЭ, г. Москва, sgarbuk@hse.ru

1) существенное возрастание ошибки оценивания функциональных характеристик (ФХ) при тестировании (испытаниях) СИИ за счет смещения (как правило – в сторону завышения характеристик) и возрастания случайной составляющей погрешности оценок при снижении вариативности тестовых НД;

2) деградация ФХ, ограничивающая возможность применения систем в реальных условиях эксплуатации. Причины такой деградации заключаются либо во внесении преднамеренных искажений в обучающие НД и архитектуру СИИ, в результате чего ФХ ухудшаются в предусмотренных условиях эксплуатации, либо в создании злоумышленниками в ходе реального применения СИИ условий применения, существенно отличающихся от ПУЭ;

3) нежелательное нарушение конфиденциальности сведений о тактико-технических характеристиках и особенностях применения СИИ, приводящее, например, к повышению эффективности деструктивных информационных воздействий на СИИ злоумышленниками;

4) компрометация сведений о физических и юридических лицах, интересы которых так или иначе затрагиваются при реализации процессов ЖЦ СИИ (заинтересованные лица СИИ).

При этом отклонение от выполнения некоторых требований повышает вероятность нарушения других (рис.1). Так, например, нарушение выполнения требований $i2$ будет приводить как к непосредственной деградации ФХ СИИ, так и к нарушению целостности выбранных архитектур систем и обучающих НД. Доступ к использованным архитектурам СИИ (несоответствие требованиям $c3$), обучающим ($c4$), тестовым ($c5$) и дообучающим ($c7$) НД расширяется возможности злоумышленника по реализации состязательных атак, что создает дополнительные риски невыполнения требования к целостности входных данных ($i2$) и т.п.

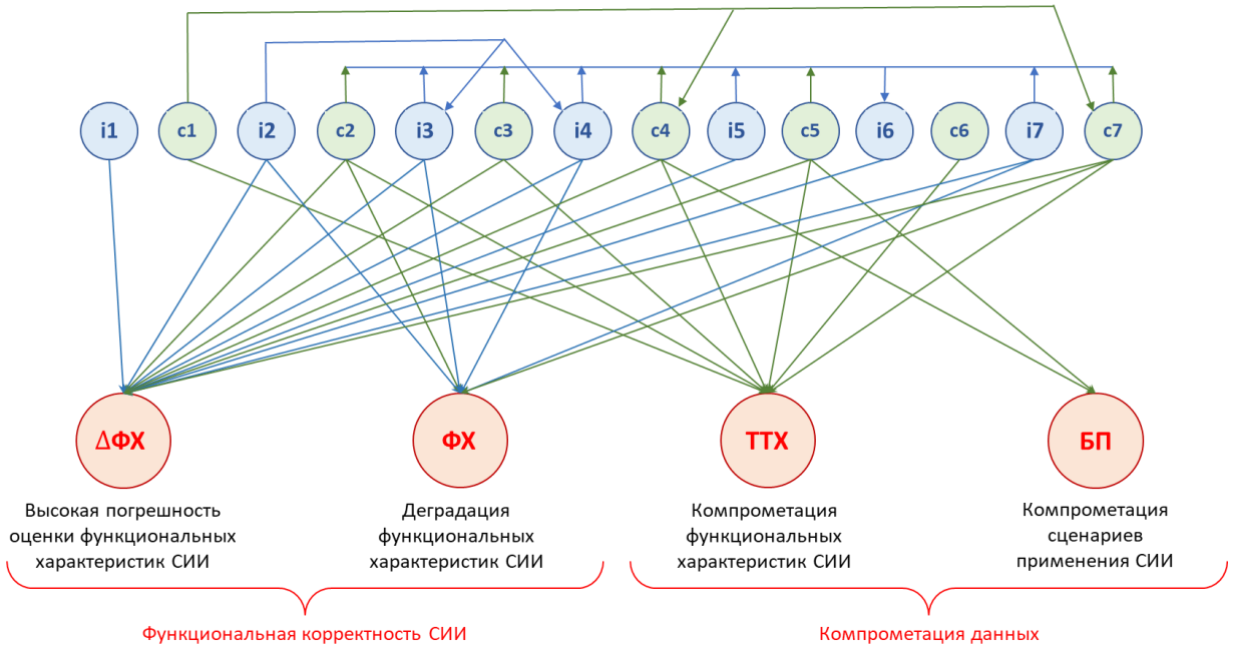


Рис.1. Структура связей между нарушениями требований в области целостности (in) и конфиденциальности (cn) информационных компонентов СИИ и возможными негативными последствиями

Обучающие НД во многих случаях содержат информацию ограниченного распространения – персональные данные, сведения, составляющие коммерческую,

служебную и иную тайну. В этом случае НД перед предоставлением к ним доступа заинтересованных разработчиков должны быть предварительно обработаны так, чтобы исключить компрометацию конфиденциальных сведений и, в то же время, сохранить информативность НД, достаточную для создания с их помощью систем ИИ.

В процессе работы СИИ уровень конфиденциальности данных, накапливаемых и обрабатываемых в системе, может возрастать, что потенциально может привести к неправильному определению (занижению) требований в области ИБ на стадии проектирования СИИ. Предотвращение нарушений требований в области ИБ, вызванных неконтролируемым ростом уровня конфиденциальности данных в процессе эксплуатации СИИ, достигается за счет реализации комплекса организационно-технических мероприятий, предусматривающего соответствующее развитие нормативной базы в области ИБ.

К специфичным негативным последствиям в области ИБ приводят нарушения функциональной корректности СИИ. Так, например, некорректная работа информационно-поисковых систем может привести к реализации деструктивных информационно-психологических воздействий на общество (дезинформация, искажение значимых исторических фактов, злонамеренное нарушение социальной стабильности и т.д.) [3, 4].

Самостоятельным вопросом ИБ является применение методов МО в средствах защиты информации (СЗИ). Зарубежными и отечественными разработчиками СЗИ активно рекламируется применение методов искусственного интеллекта в предлагаемых ими решениях. Отметим, что существующая нормативно-техническая база и инструменты сертификации СЗИ не в полной мере учитывают перечисленные выше особенности поведения алгоритмов МО и требуют актуализации с учетом современных технологических трендов в области ИБ [5-8].

Таким образом, к новым научно-техническим и нормативно-техническим задачам в области ИБ, обусловленным развитием систем ИИ на основе алгоритмов машинного обучения, следует отнести:

1) разработка требований к обеспечению конфиденциальности сведений об особенностях создания СИИ (параметры обучающего набора данных, архитектура используемых искусственных нейронных сетей и др.) с учетом возможности использования этих сведений злоумышленниками для реализации информационных атак на системы ИИ;

2) разработка требований к созданию и сертификации средств гарантированной деклассификации (в том числе – обезличивания) наборов данных, используемых при создании и тестировании систем ИИ;

3) разработка требований к созданию и сертификации средств автоматизированного мониторинга уровня конфиденциальности данных, накапливаемых и агрегируемых при эксплуатации СИИ;

4) анализ широкого спектра угроз ИБ, включая угрозы деструктивного информационного-психологического воздействия на общество, обусловленных применением систем ИИ с неподтвержденной функциональной корректностью. Разработка требований к средствам выявления и предупреждения таких угроз;

5) разработка требований к созданию и сертификации средств защиты информации на основе алгоритмов машинного обучения.

Заключение

В статье рассмотрено влияние нарушения требований в области информационной безопасности, предъявляемых к информационным компонентам систем ИИ, на риски, возникающие при создании и применении этих систем. Анализ структуры зависимостей рисков с учетом общих особенностей систем обработки данных на основе алгоритмов машинного обучения показал, что эти риски сводятся к ухудшению функциональных

характеристик СИИ, увеличению погрешности оценки этих характеристик эксплуатантом и компрометации данных, обрабатываемых в системе. Предотвращение выявленных рисков позволит повысить эффективность создания и применения СИИ в различных отраслях экономики и социальной сферы.

Список литературы

1. Гарбук С.В. Метод оценки влияния параметров стандартизации на эффективность создания и применения систем искусственного интеллекта // Информационно-экономические аспекты стандартизации и технического регулирования. 2022. № 3. С. 4–14.

2. Шананин В.А. Применение систем искусственного интеллекта в защите информации // «Инновации и инвестиции». 2022 г. № 11. С.201-205.

3. Гарбук С.В. Управление жизненным циклом образцов вооружения, военной и специальной техники с искусственным интеллектом // Военная мысль. 2022. № 8. С. 86-105.

4. Гарбук С.В., Шалаев А.П. Перспективная структура национальных стандартов в области искусственного интеллекта // Стандарты и качество. 2021. № 10. С. 26-33.

5. Гарбук С.В. Задачи нормативно-технического регулирования интеллектуальных систем информационной безопасности // Вопросы кибербезопасности. 2021. №3(43). С.68-83.

6. Кибербезопасность цифровой индустрии. Теория и практика функциональной устойчивости к кибератакам / Под ред. Зегжда Д.П. и др. М.: Горячая линия, 2021. 560 с.

7. Марков А.С. Актуальные вопросы оценки соответствия интеллектуальных средств защиты информации. Материалы трудов Конгресса «Русский инженер» (Москва, 30 октября - 3 ноября 2023). М.: МГТУ им. Н.Э.Баумана, 2023.

8. Probabilistic modeling in system engineering. / By ed. Kostogryzov A. - London: InTechOpen, 2018. – 279 p.

Tasks of information security of artificial intelligence systems

Garbuk S.V.[34]

Abstract. The article discusses scientific, technical and regulatory tasks in the field of information security, specific to machine learning (ML) methods. The solution of these tasks contributes to increasing the efficiency of the use of artificial intelligence systems based on ML by eliminating the risks associated with the violation of functionality and data compromise in the systems.

Key words: Functional correctness of AI systems, confidentiality of data in AI systems, risks of using AI systems.

[34] Sergey Garbuk, PhD. in Technology, senior researcher, HSE University, Moscow, sgarbuk@hse.ru

УДК 621.311: 004.052

Анализ киберугроз для интеллектуальных инверторов, используемых при управлении микросетями

Гурина Л.А.[35]

Аннотация. Развертывание микросетей, несмотря на многочисленные экономические, технические преимущества, способствует росту уязвимостей к кибератакам, обусловленных широкомасштабным применением информационных и коммуникационных технологий, увеличением цифровых компонентов, используемых при управлении. Эксплуатация уязвимостей информационно-коммуникационной инфраструктуры может привести к сбоям и отказам в функционировании микросети. Для снижения рисков кибербезопасности проведен анализ возможных кибератак на интеллектуальные инверторы, используемые при управлении микросетями. Полученные результаты позволили выявить наиболее опасные по последствиям кибератаки на интеллектуальные инверторы для функционирования микросетей[36].

Ключевые слова: энергетическая система, распределенная генерация, кибератаки, контроллеры, интеллектуальное управление.

Введение

Современные энергетические системы можно охарактеризовать как интегрированные системы с большой долей распределенной генерации и возобновляемых источников энергии [1]. Все большое распространение получает развертывание микросетей для более быстрого реагирования на спрос и более полных возможностей управления энергопотреблением. Интеграция информационных и цифровых технологий постепенно преобразовала традиционную энергетическую систему в киберфизическую энергетическую систему [2, 3], которая включает в себя двустороннюю связь между информационно-коммуникационной и технологической подсистемами, а также взаимодействие между информационными системами микросетей. Сложные связи микросетей, растущее число силовой электроники и цифровых компонентов на базе разнообразного программного обеспечения и аппаратных средств, используемых при управлении, обусловливают увеличение уязвимостей информационных систем к кибератакам.

Интеллектуальные инверторы служат важным интерфейсом между микросетями и энергетической системой. Кроме того, интеллектуальные инверторы (контроллеры), используются при различных способах (централизованном, децентрализованном и распределенном) и на разных уровнях иерархии управления микросетями (нижнем, среднем и верхнем) [4]. Между тем риски кибербезопасности интеллектуальных инверторов также растут из-за широкого использования информационных и коммуникационных технологий.

Целью работы выявление возможных кибератак на интеллектуальные инверторы, приводящие к нарушениям функций управления микросетями.

Анализ кибератак и их последствий на интеллектуальные инверторы

Кибератаки на интеллектуальные инверторы можно разделить на атаки на уровне сети и атаки на уровне устройств.

Кибератаки на уровне сети:

[35] Гурина Людмила Александровна, кандидат технических наук, доцент, старший научный сотрудник Лаборатории управления функционированием электроэнергетических систем Института систем энергетики им. Л.А. Мелентьева СО РАН, Иркутск, Россия. E-mail: gurina@isem.irk.ru

[36] Работа выполнена в рамках научного проекта «Теоретические основы, модели и методы управления развитием и функционированием интеллектуальных электроэнергетических систем», № FWEU-2021-0001.

- *Кибератаки на основе измерений* (FDI-атака, DoS-атака, Hijacking-атака и т.д.) направлены на манипулирование или блокирование измерений от инвертора до центра управления посредством кибератак на каналы связи, нарушая процесс принятия решений центром управления [5, 6].

✓ *Атаки на основе команд* направлены на дестабилизацию сети или создание энергетических/экономических потерь путем манипулирования, или блокирования команд/конфигураций управления, отправляемых из центра управления, который развертывает сетевые службы, напр., система управления энергопотреблением (EMS) [7, 8].

✓ *Атаки на распределенные системы управления* [9, 10]. Информация, совместно используемая связанными инверторами, может быть изменена или прервана кибератаками.

✓ *Атаки, вызванные атакой на другие устройства*. В этой категории злоумышленники могут не намереваться атаковать интеллектуальные инверторы напрямую, а пытаться скомпрометировать другие устройства (например, интеллектуальные счетчики, устройства РПН и т. д.) в сети, что также может ввести в заблуждение о неисправности интеллектуальных инверторов и привести к нарушению функционирования микросети [11, 12].

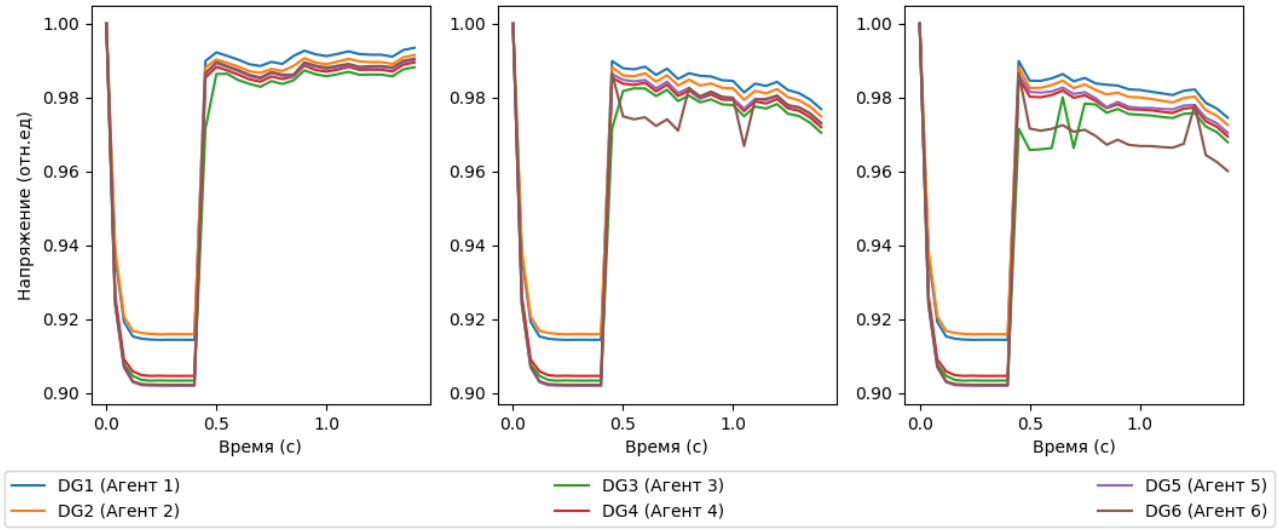
Кибератаки на уровне устройств [13-18] могут быть направлены на различные компоненты интеллектуального инвертора:

✓ *Атаки на каналы связи* между инвертором и подключенным устройством, которые включает в себя разведку, атаки повторного воспроизведения, отказ в обслуживании (DoS-атака), атаку «человек посередине».

✓ *Аппаратные атаки*, включая атаки на встроенное программное обеспечение и аппаратные средства, спуфинг-атаку и т.д.

✓ *Атаки, направленные на нарушение рабочих функций интеллектуального инвертора*, включая базовые функции управления, функции поддержки сети и функции защиты.

В [19, 20] при моделировании кибератак на интеллектуальные инверторы при распределенном вторичном управлении сообществом микросетей проведен анализ поведения интеллектуальных инверторов, не подверженных кибератакам. Показано, что наиболее опасными по последствиям для качества информационным потоков, и тем самым, приводящим к потере функциональности системы управления микросетями, являются FDI-атака и Hijacking-атака (рис. 1).



а) Кибератаки отсутствуют б) FDI-атака в) Hijacking-атака

Рис 1. Результаты моделирования поведения агентов обученной системы регулирования напряжения при возмущении нагрузки при наличии и отсутствии кибератак

Выводы

При исследовании кибербезопасности интеллектуальных инверторов, используемых при управлении микросетями проанализированы возможные кибератаки как на уровне сети, так и на уровне устройств. Выявлены наиболее опасные по последствиям кибератаки на функциональность систем управления микросетями. В дальнейшем, полученные результаты будут использованы при разработке мер по обнаружению, смягчению/подавлению последствий кибератак на интеллектуальные инверторы.

Литература

1. Voropai N. Electric Power System Transformations: A Review of Main Prospects and Challenges. Energies. 2020, 13, 5639. DOI: 10.3390/en13215639

2. Нашивочников Н.В., Большаков А.А., Николашин Ю.А., Лукашин А.А. Проблемные вопросы применения аналитических средств безопасности киберфизических систем предприятий ТЭК // Вопросы кибербезопасности. 2019. № 5 (33). С. 26–33.

3. Кибербезопасность цифровой индустрии. Теория и практика функциональной устойчивости к кибератакам / Под. ред. Д.П. Зегжда. - М.: Горячая линия - Телеком, 2021. - 560 с.

4. Илюшин П.В., Вольный В.С. Обзор структур микросетей низкого напряжения с распределенными источниками энергии // Релейная защита и автоматизация. 2023, № 1(50), с. 68-80.

5. H. Salehghaffari and M. Khodaparastan. Dynamic attacks against inverter-based microgrids. in 2019 IEEE Power & Energy Society General Meeting (PESGM). IEEE, 2019, pp. 1–5.

6. S. Liu, Z. Hu, X. Wang, and L. Wu. Stochastic stability analysis and control of secondary frequency regulation for islanded microgrids under random denial of service attacks // IEEE Transactions on Industrial Informatics. 2018, vol. 15, no. 7, pp. 4066–4075.

7. I. Zografopoulos and C. Konstantinou. Detection of Malicious Attacks in Autonomous Cyber-Physical Inverter-Based Microgrids. in IEEE Transactions on Industrial Informatics. Sept. 2022, vol. 18, no. 9, pp. 5815-5826. DOI: 10.1109/TII.2021.3132131.

8. A. Karimi, A. Ahmadi, Z. Shahbazi, Q. Shafiee and H. Bevrani. A Resilient Control Method Against False Data Injection Attack in DC Microgrids // 2021 7th International Conference on Control, Instrumentation and Automation (ICCIA), Tabriz, Iran, 2021, pp. 1-6. DOI: 10.1109/ICCIA52082.2021.9403594.

9. H. Zhang, W. Meng, J. Qi, X. Wang, and W. X. Zheng. Distributed load sharing under false data injection attack in an inverter-based microgrid // IEEE Transactions on Industrial Electronics, 2018, vol. 66, no. 2, pp. 1543–1551.

10. B. Wang, Q. Sun, R. Han, and D. Ma. Consensus-based secondary frequency control under denial-of-service attacks of distributed generations for microgrids // Journal of the Franklin Institute, 2019.

11. A. Teymouri, A. Mehrizi-Sani, and C.-C. Liu. Cyber security risk assessment of solar pv units with reactive power capability. in IECON 2018-44th Annual Conference of the IEEE Industrial Electronics Society. IEEE, 2018, pp. 2872–2877.

12. D. Choeum and D. -H. Choi. Vulnerability Assessment of Conservation Voltage Reduction to Load Redistribution Attack in Unbalanced Active Distribution Networks. in IEEE Transactions on Industrial Informatics. Jan. 2021, vol. 17, no. 1, pp. 473-483. DOI: 10.1109/TII.2020.2980590.

13. M. Abdelkhalek, G. Ravikumar and M. Govindarasu. ML-based Anomaly Detection System for DER Communication in Smart Grid // 2022 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT), New Orleans, LA, USA, 2022, pp. 1-5. DOI: 10.1109/ISGT50606.2022.9817481.

14. I. Onunkwo, B. Wright, P. Cordeiro, N. Jacobs, C. Lai, J. Johnson, T. Hutchins, W. Stout, A. Chavez, B. T. Richardson et al.. Cybersecurity assessments on emulated der communication networks // Sandia Technical Report, Tech. Rep., 2018.

15. A. Singh. Distributed intrusion detection system for modbus protocol. 2020.

16. J. Liang et al. Research and Prospect of Cyber-Attacks Prediction Technology for New Power Systems // 2023 IEEE 6th Information Technology,Networking,Electronic and Automation Control Conference (ITNEC), Chongqing, China, 2023, pp. 638-647. DOI: 10.1109/ITNEC56291.2023.10081983.

17. S. Jena and N. P. Padhy. Cyber-Secure Global Energy Equalization in DC Microgrid Clusters Under Data Manipulation Attacks. in IEEE Transactions on Industry Applications. Sept.-Oct. 2023, vol. 59, no. 5, pp. 5488-5505. DOI: 10.1109/TIA.2023.3287969.

18. A. Barua and M. A. Al Faruque. Hall spoofing: A non-invasive dos attack on grid-tied solar inverter. in 29th USENIX Security Symposium (USENIX Security 20). 2020, pp. 1273–1290.

19. Гурина Л.А., Томин Н.В. Разработка комплексного подхода к обеспечению кибербезопасности взаимосвязанных информационных систем при интеллектуальном управлении сообществом микросетей // Вопросы кибербезопасности. 2023, № 4(56), с. 94-104. DOI: 10.21681/2311-3456-2023-4-94-104

20. Гурина Л.А., Айзенберг Н.И. Поиск эффективного решения по обеспечению защиты от киберугроз сообщества микросетей со взаимосвязанными информационными системами // Вопросы кибербезопасности. 2023. № 3 (55). С. 37-49.

Cyber Threats Analysis for Smart Inverters Used in Microgrids Management[37]

Gurina L.A. [38]

Abstract. The deployment of microgrids, despite numerous economic and technical advantages, contributes to the growth of vulnerabilities to cyber attacks due to the large-scale use of information and communication technologies and the increase in digital components used in management. Exploitation of information and communication infrastructure vulnerabilities can lead to failures and failures in the functioning of the microgrid. To reduce cybersecurity risks, an analysis of possible cyber attacks on smart inverters used in microgrid management was carried out. The results obtained made it possible to identify the most dangerous consequences of cyber attacks on smart inverters for the functioning of microgrids.

Keywords: energy system, distributed generation, cyber attacks, controllers, intelligent control.

[37] The research was conducted within the framework of the scientific project "Theoretical foundations, models and methods to control the expansion and operation of intelligent electric power systems (Smart Grids)", No. FWEU-2021-0001.

[4] Liudmila A. Gurina, Ph.D. in engineering, Associate Professor, Senior Research Fellow, Laboratory for Control of Electric Power Systems at Melentiev Energy Systems Institute, SB RAS, Irkutsk, Russia. E-mail: gurina@isem.irk.ru

УДК 371.3: 004.056

Симуляционное обучение специалистов по кибербезопасности в стиле сотрудничества

Дорофеев А.В.[39]

Обучение сотрудников с имитацией кризисных ситуаций давно зарекомендовало себя с лучшей стороны в области кибербезопасности. Большинство известных методов обучения проводится в рамках соперничества команд, например наступающих и защищающихся. В докладе демонстрируется новое направление симуляционного обучения, когда команды сотрудничают друг с другом в целях повышения эффективности разбора различных методик взлома и защиты. В докладе дано описание указанного подхода и приведены практические кейсы по обучению.

Ключевые слова: кибербезопасность, обучение по информационной безопасности.

Введение

В рамках государственной линии на технологическую независимость подготовка специалистов является одной из самых приоритетных [1-5]. При этом симуляционные методы обучения, когда имитируются реальные кризисные ситуации и инциденты, являются одними из наиболее перспективных. Примерами такого обучения являются киберучения и соревнования [6-10].

В современных киберучениях, как известно, принято команды разделять на различные цвета (рис. 1). Так, например, атакующая команда имеет красный цвет, а обороняющаяся – синий (рис. 1) [6].

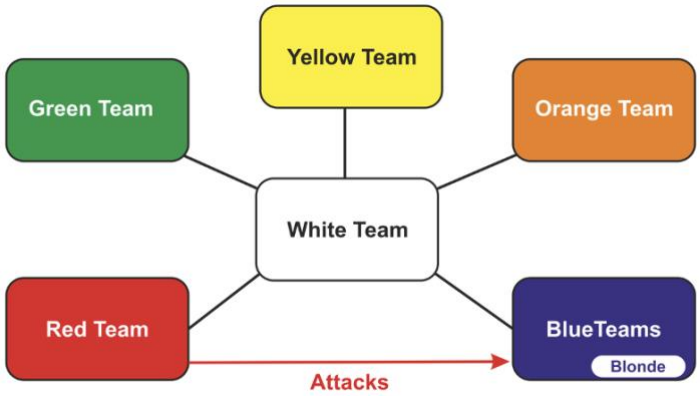


Рис. 1. Цвета команд

Данные цветовые обозначения стали применяться и вне учений в отношении сотрудников по информационной безопасности и аудиторов. При этом считается, что сотрудничество двух команд может привести к повышению эффективности обучения по кибербезопасности [6]. Например, специалист по тестированию на проникновение может определить наиболее вероятные векторы атаки, а специалист по администрированию SIEM-систем сможет определить набор правил для детектирования попыток злоумышленников по реализации атак, соответствующих данному вектору. Мы знаем, что смешение красного

[39] Дорофеев Александр Владимирович, генеральный директор АО «Эшелон Технологии»
ad@cnpo.ru

и синего дает фиолетовый цвет, что и нашло отражение в обозначении команды, объединяющей специалистов этих двух профилей. По этой причине такое обучение получило название – Purple Teaming [11].

Рис. 2. Смешение цветов киберкоманд

Задачи фиолетовой команды и подготовка специалистов

Объединяя возможности красной и синей команд, можно зафиксировать следующие задачи, которые фиолетовая команда сможет итеративно решать в организации: тестирование на проникновение, управление уязвимостями, внедрение средств защиты информации, мониторинг источников событий информационной безопасности, анализ (разведка) угроз, настройка средств защиты информации в соответствии с принятыми политиками безопасности и информацией об актуальных угрозах, поиск угроз, управление инцидентами, реагирование на инциденты [1, 9, 10].

Пример курса обучения в стиле Purple Team

В учебном центре «Эшелон» был разработан курс обучения в стиле Purple Team. Методическим ядром учебного курса явился подробный разбор тактических задач (тактик) и приемов (техник), используемых злоумышленниками на примере матрицы MITRE ATT&CK. Вариант инструментария представлен в табл. 1.

Таблица 1.

Пример инструментария Purple Team

В части Red Team	В части Blue Team
Сканер портов Nmap. Фреймворк для проведения тестирования защищенности Metasploit Framework. Утилита для онлайн-подбора (по известным сетевым протоколам) паролей Hydra. Утилита для оффлайн-подбора (по хэшам) паролей HashCat. Сканер уязвимостей Сканер-ВС 6.	Система управления событиями информационной безопасности KOMRAD Enterprise SIEM. Система глубокого анализа трафика NTA eSensor. Система межсетевого экранирования и обнаружения вторжений «Рубикон». Межсетевой экран PFSense

В [7] приведен разбор лабораторной работы, выполняемой в рамках указанного курса.

Заключение

Достоинством обучения в стиле Purple Team является то, что слушатели могут разобраться в организации защиты информации как с точки зрения реального нападения,

так и с точки зрения полноты реакции на нападение, так как обеспечивается прозрачность всех действий в системе, касающихся информационной безопасности. Это позволяет подготовить сотрудников по проактивной защите информации.

Рассмотренный в статье подход прошел апробацию в рамках работы учебного курса, все необходимые технологии для его реализации доступны как в виде коммерческих решений, так и в виде решений с открытым исходным кодом.

Авторы полагают, что подход в стиле Purple Team будет набирать популярность в обучении специалистов по информационной безопасности, так же, как и модные сейчас киберучения и конкурсы по вознаграждению за выявленные уязвимости (bugbounty).

Литература

1. Дорофеев А.В., Марков А.С. Применение отечественных технологий для мониторинга информационной безопасности в условиях импортозамещения // Защита информации. Инсайд. 2023. № 3 (111). С. 20-26.
2. Кибербезопасность цифровой индустрии. Теория и практика функциональной устойчивости к кибератакам / Под ред. Зегжда Д.П. и др. М.: Горячая линия, 2021. 560 с.
3. Петренко А.С., Петренко С.А., Костюков А.Д. Какие специалисты нужны отрасли информационной безопасности: DevSecOps-инженеры // Защита информации. Инсайд. 2023. № 6. 60-65 с.
4. Царегородцев А.В. Кадры решают всё: назад в будущее. Сборник трудов Международной конфренции «Безопасные информационные технологии». М.: МГТУ им.Н.Э.Баумана, 2023. С. 144.
5. Шеремет И.А. Направления подготовки специалистов по противодействию киберугрозам в кредитно-финансовой сфере // Вопросы кибербезопасности. 2016. № 5 (18). С. 3-7.
6. Дорофеев А.В., Марков А.С. Методические основы киберучений и CTF-соревнований // Защита информации. Инсайд. 2022. № 2 (104). С. 56–63.
7. Дорофеев А.В., Марков А.С. Обучение специалистов в области кибербезопасности в стиле Purple Team // Защита информации. Инсайд. 2023. № 6. 67–71 с.
8. Петренко А.А., Петренко С.А. Киберучения: методические рекомендации ENISA // Вопросы кибербезопасности. 2015. № 3 (11). С. 2–14.
9. Dorofeev A. V., Markov A. S., Rautkin Y. V. Ethical Hacking Training. // CEUR Workshop Proceedings. 2019. V. 2522. P. 47–56.
10. Dorofeev A.V., Markov, A.S. Conducting Cyber Exercises Based on the Information Security Threat Model // CEUR Workshop Proceedings, 2021, vol. 3057, pp. 1-10.
11. Bryant T. TFM: Purple Team Field Manual. IP, Computer Security & Encryption, 2020. 215 p.

Simulation training for cybersecurity professionals in a collaborative style

Dorofeev A.V. [40]

Employee training with simulated crisis situations has a long-standing reputation in cybersecurity. Most of the known training methods are conducted in the framework of team rivalry, such as offensive and defensive teams. The paper demonstrates a new direction in simulation training, where teams collaborate with each other to improve the effectiveness of parsing different hacking and defense techniques. The paper describes this approach and provides practical training cases.

Keywords: cybersecurity, information security training

[40] Alexander V. Dorofeev, General Director of Echelon Technologies JSC, ad@cnpo.ru

УДК 004.056

Обеспечение конфиденциальности пользователей блокчейн сетей

Еськов Н.В.[41], **Ключарёв П.Г.**[42]

Аннотация. *В работе проведён анализ современных методов анонимизации транзакций в блокчейн сетях. Выбран подходящий метод для обеспечения конфиденциальности пользователей блокчейн систем. Предложена архитектура системы, где применение выбранного метода может противостоять популярным методам деанонимизации транзакций.*

Ключевые слова: *криптография с нулевым разглашением, анонимизация транзакций, блокчейн, смарт-контракты, информационная безопасность*.

Введение

Блокчейн — это технология открытого распределенного реестра, которая является децентрализованной, отказоустойчивой и обеспечивает хороший уровень анонимности [1, 2]. Рост капитализации и оборота криптовалют, основанных на технологии блокчейн, свидетельствует о растущем доверии к этим активам и технологиям. Однако некоторые лица и организации пытаются контролировать блокчейн сети путём деанонимизации транзакций, что угрожает анонимности пользователей. Для повышения уровня конфиденциальности в блокчейн сетях необходимо использовать современные методы анонимизации транзакций.

Сравнение методов анонимизации транзакции

Существует несколько основных способов деанонимизации транзакций: *анализ сети* [3-5], *кластеризация адресов* [6-8], *способы на базе отпечатков транзакций* [9], *анализ графа транзакций* [10] и *атака Сивиллы* [11, 12]. Каждый из этих методов может раскрыть личность пользователей и нарушить их конфиденциальность в блокчейн сети.

Для противодействия вышеперечисленным методам существуют следующие методы анонимизации транзакций:

- *Микшеры транзакций:*
  - *Централизованные*: представляют собой веб-сайты, позволяющие проводить анонимные транзакции с определенной платой. Но у таких сайтов есть недостатки: возможность кражи активов этим сайтом [13] и хранение данных об отправителе и получателе. Кроме того, такие веб-сайты уязвимы к атакам типа отказ в обслуживании (DoS);
  - *Децентрализованные*: созданы для снижения вероятности атак типа DoS, к которым уязвимы централизованные сервисы микширования. Ярким примером является блокчейн транзакция CoinJoin [14]. Однако все участники сети знают об отправителях и получателях такой транзакции, а также в ней есть ограничение на количество участников;
- *Кольцевые подписи*: цифровая подпись [15], позволяющая создавать анонимные подписи от группы возможных подписывающих лиц. Блокчейн Monero [16] является наиболее успешным применением данного метода, но размер транзакций, использующих кольцевую подпись, довольно большой и пропорционален количеству участников группы;
- *Неинтерактивные доказательства с нулевым разглашением (NIZKP)*: вариант доказательств с нулевым разглашением [17], где нет взаимодействия между доказывающим и проверяющим, что подходит для анонимной и распределенной проверки

[41] Еськов Николай Викторович, аспирант МГТУ им. Н.Э. Баумана, г. Москва, mr.eskov1@yandex.ru
[42] Ключарёв Петр Георгиевич, доктор технических наук, доцент кафедры ИУ-8 МГТУ им. Н.Э. Баумана, г. Москва, pk.iu8@yandex.ru

сообщений в блокчейне. Протокол Zerocash [18] является ярким примером применения этого метода. Недостаток этого метода – это более высокие вычислительные затраты по сравнению с другими способами.

Согласно вышеприведенной информации и работе [19] вышеперечисленные способы анонимизации можно свести в таблицу 1:

Таблица 1.

Сравнение методов обеспечения конфиденциальности в блокчейне

Метод обеспечения конфиденциальности	**Способ обеспечения конфиденциальности**	**Основные недостатки**
Централизованные микшеры	Скрытие взаимосвязи транзакций	- задержка обработки - единая точка отказа - комиссии - отсутствие защиты содержания
Децентрализованные микшеры	Децентрализованное скрытие взаимосвязи транзакций	- задержка обработки - комиссии - отсутствие защиты содержания - уязвимость к атакам Сивиллы
Кольцевые подписи	Скрытие взаимосвязи пользователей	- ограниченное число участников в группе - большие накладные расходы на дисковое пространство
NIZKP	Скрытие взаимосвязи транзакций и содержания транзакций	- высокие накладные расходы на вычисления

Выбор метода обеспечения анонимизации транзакций

Из таблицы 1 видно, что системы на базе NIZKP имеют только один недостаток – высокие накладные расходы на вычисления. Однако современные вычислительные устройства способны его компенсировать. Применение NIZKP снижает нагрузку на блокчейн сеть, так как вычисления происходят на стороне пользователя, что в дополнение делает масштабную атаку экономически невыгодной.

В системах блокчейн конфиденциальность пользователей напрямую связана с конфиденциальностью пользовательских транзакций. Чувствительной информацией в транзакциях являются: *отправитель*, *получатель*, *переводимый актив* и его *количество*. Для обеспечения конфиденциальности необходимо проводить вычисления вне блокчейна и публиковать туда только результаты, которые не раскрывают чувствительную информацию. Этого можно достигнуть при использовании системы проверяемых вычислений, которая основывается на доказательствах с нулевым разглашением [20].

Такую систему можно определить так: пусть пара полиномиальных алгоритмов (P, V) будут доказывающим (*prover*) и проверяющим (*verifier*) соответственно, а R – случайной строкой. Обозначим свидетельство (секрет, который позволяет эффективно проверить утверждение и доказать его истинность) как ω (*witness*), а доказательство NIZKP (результат работы доказывающего) как π (*proof*). Тогда для языка $\mathrm{L} \subseteq \mathrm{NP}$ пара алгоритмов (P, V) будет называться системой с неинтерактивным доказательством с нулевым разглашением (NIZKP) если они удовлетворяют следующим свойствам:

- **Полнота**: если утверждение действительно верно, то доказывающий убедит в этом проверяющего с любой наперед заданной точностью. То есть, для любого входа $x \in L$ со свидетельством (секретом) ω, полиномом $p(\cdot)$ и битовой строкой $|x|$ верно следующее:

$$Pr\big[V\big(R, x, P(R, x, \omega)\big) = 1\big] \geq 1 - \frac{1}{p(|x|)} \qquad (1)$$

- **Корректность**: если утверждение неверно, то любой, даже “нечестный”, доказывающий не сможет убедить проверяющего за исключением пренебрежимо малой вероятности. То есть, для любого входа $x \notin L$, любого алгоритма P^*, полинома $p(\cdot)$ и битовой строки $|x|$ верно следующее:

$$Pr[V(R, x, P^*(R, x)) = 1] < \frac{1}{p(|x|)} \qquad (2)$$

- **Нулевое разглашение**: если утверждение верно, то любой, даже “нечестный”, проверяющий не узнает ничего кроме самого факта, что утверждение верно. То есть, для любого входа $x \in L$ со свидетельством ω существует вероятностный полиномиальный алгоритм S такой, что следующие два распределения вычислительно неразличимы:

$$\{R, x, P(R, x, \omega)\} \approx \{R, x, \pi\} \leftarrow S(x) \qquad (3)$$

Одним из протоколов, в наибольшей степени удовлетворяющим свойствам полноты, корректности и нулевого разглашения, является протокол zkSNARK (zero-knowledge Succinct Non-Interactive ARgument of Knowledge) [21, 22].

Применение NIZKP для анонимизации транзакций

Система анонимизации транзакций, построенная на базе NIZKP, должна иметь в себе следующие подсистемы: *приватный кошелёк* и *оператор кошелька*. Приватный кошелёк – это смарт-контракт, который позволяет пользователям осуществлять анонимные транзакции. Он производит проверку доказательств пользователей для разблокировки средств и осуществления транзакций. В рамках zkSNARK представляет из себя проверяющего. Оператор кошелька – это пользовательское приложение, позволяющее взаимодействовать с приватным кошельком на блокчейне, отправляя сформированные доказательства в блокчейн. В рамках zkSNARK оператор – это доказывающий.

Чтобы обеспечить полноту владения средствами, кошельку необходимо иметь следующие функции: *пополнение (deposit), перевод средств (transfer), вывод средств (withdraw).*

Средства пользователей должны храниться в виде непотраченных выходов транзакций (UTXO), аналогичным в Bitcoin [23]. Смарт-контракт должен проверять правильность доказательств пользователей на их право владения активом, осуществлять операции с активами, хранить зашифрованные пользователем UTXO и их обнулители, чтобы один и тот же UTXO нельзя было потратить дважды. Пользователь должен иметь возможность сформировать UTXO с указанным им активом и его количеством, зашифровать его публичным zkSNARK ключом владельца UTXO и получить его хеш, а также иметь возможность опубликовать зашифрованное UTXO в смарт-контракт, чтобы получатель UTXO мог успешно сохранить его локально и расшифровать своим секретным zkSNARK ключом. Загрузка и расшифровывание UTXO представлены на рис. 1.

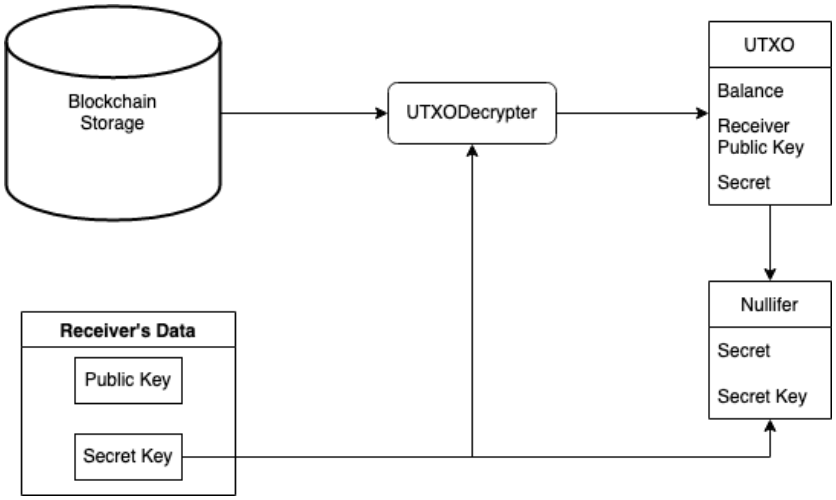


Рис. 1. Загрузка и расшифровывание UTXO из выбранного блокчейна

Функции пополнения (*deposit*) необходимо осуществлять перевод выбранного актива в заданном объёме на счёт смарт-контракта, где средства будут храниться и управляться пользователем уже с помощью приватного кошелька. Как выглядит пополнение схематично представлено на рисунке 2.

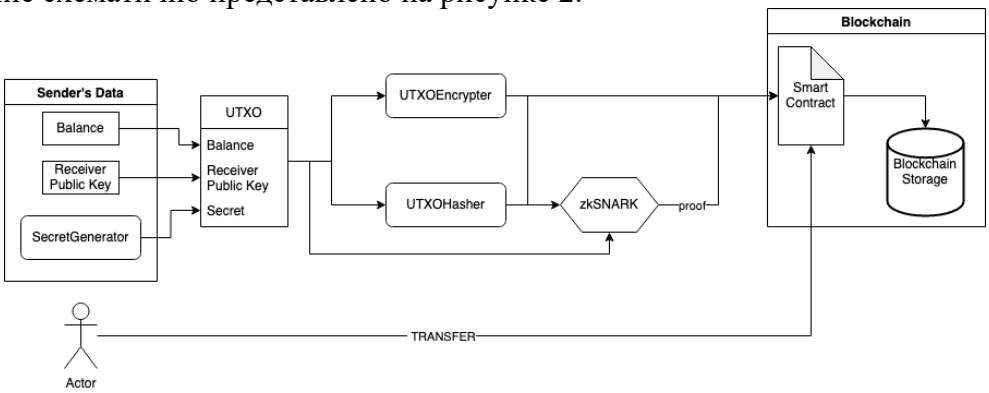


Рис. 2. Функция deposit

Отправка средств в пределах смарт-контракта осуществляется вызовом функции перевода (*transfer*), публикаций обнулителя в смарт-контракт для выбранного пользователем UTXO и создания нового UTXO, владельцем которого может быть другой или этот же пользователь. Работа функции перевода упрощённо представлена на рисунке 3.

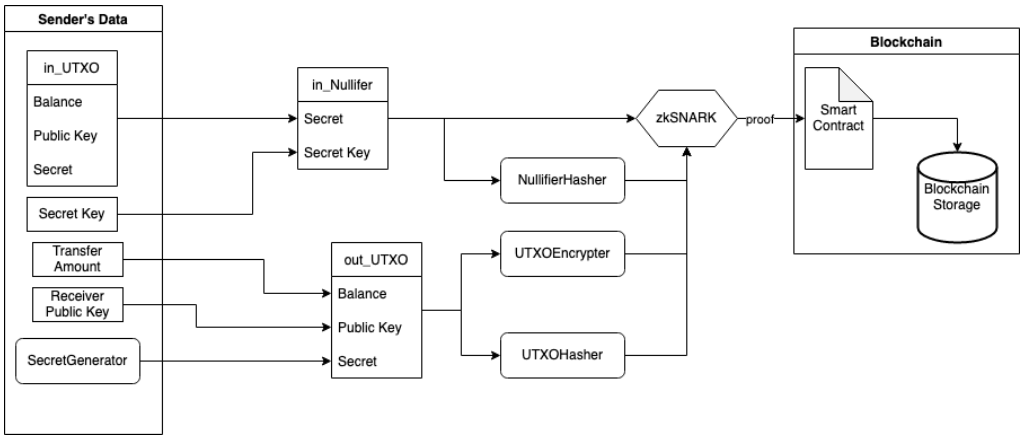


Рис. 3. Функция transfer

Вывод средств с приватного счёта пользователя на смарт-контракте происходит через обнуление выбранного UTXO и перевода средств со счёта смарт-контракта на счёт пользователя, от которого произошёл вызов функции вывода средств (*withdraw*). Схематично работа данной функции изображена на рисунке 4.

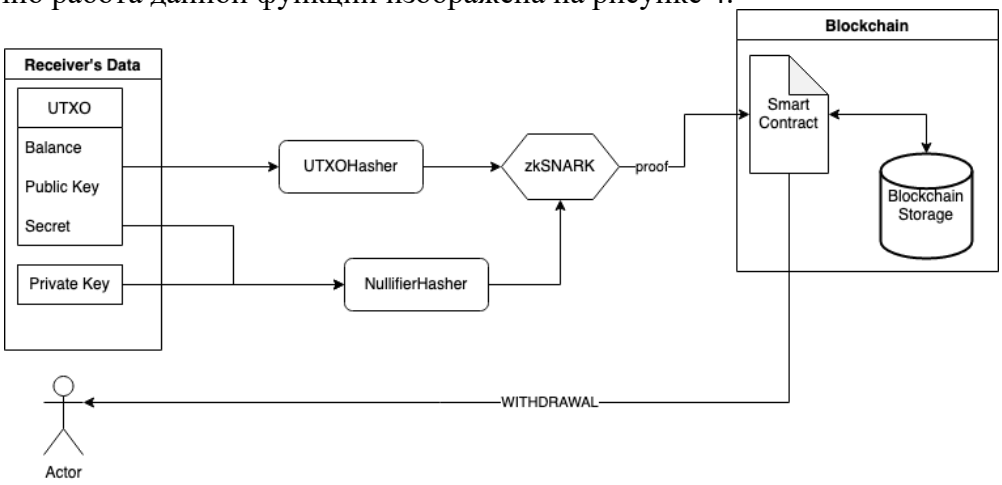


Рис.4. Функция withdraw

Заключение

В данной работе проанализированы современные способы анонимизации пользовательских транзакций в публичных блокчейн сетях. В большей степени подходящим оказался способ, основанный на неинтерактивных доказательствах с нулевым разглашением. Приведена архитектура решения, основанная на выбранном методе, которая будет способствовать обеспечению высокого уровня анонимности в публичных блокчейн сетях и противодействию современным методам деанонимизации транзакций.

Литература

1. Астраханцев Р.Г., Лось А.Б., Мухамадиева Р.Ш. Анализ современных тенденций развития технологии "блокчейн" и цифровых валют // Вопросы кибербезопасности. 2019. № 5 (33). С. 57–62.
2. Петренко А.С., Петренко С.А., Костюков А.Д. Угрозы безопасности децентрализованным блокчейн-приложениям // Защита информации. Инсайд. 2022. № 5 (107). С. 28–39.
3. P. Koshy, D. Koshy, and P. McDaniel, "An analysis of anonymity in bitcoin using p2p network traffic," in International Conference on Financial Cryptography and Data Security, pp. 469-485, Springer, 2014.
4. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System [Электронный ресурс] - URL: https://bitcoin.org/bitcoin.pdf (дата обращения 20.10.2023).
5. F. Reid and M. Harrigan, “An analysis of anonymity in the bitcoin system,” in Security and privacy in social networks, pp. 197–223, Springer, 2013.
6. F. Reid and M. Harrigan, "An analysis of anonymity in the bitcoin system," in Security and privacy in social networks, pp. 197-223, Springer, 2013
7. K. Liao, Z. Zhao, A. Doupe ÃÅ, and G.-J. Ahn, "Behind closed doors: measurement and analysis of cryptolocker ransoms in bitcoin," in Electronic Crime Research (eCrime), 2016 APWG Symposium on, pp. 1-13, IEEE, 2016.
8. M. Spagnuolo, F. Maggi, and S. Zanero, "Bitiodine: Extracting intelligence from the bitcoin network," in International Conference on Financial Cryptography and Data Security, pp. 457-468, Springer, 2014.

9. E. Androulaki, G. O. Karame, M. Roeschlin, T. Scherer, and S. Capkun, "Evaluating user privacy in bitcoin," in International Conference on Financial Cryptography and Data Security, pp. 34-51, Springer, 2013.
10. D. Ron and A. Shamir, "Quantitative analysis of the full bitcoin transaction graph," in International Conference on Financial Cryptography and Data Security, pp. 6-24, Springer, 2013.
11. G. Bissias, A. P. Ozisik, B. N. Levine, and M. Liberatore, "Sybilresistant mixing for bitcoin," in The Workshop on Privacy in the Electronic Society, pp. 149-158, 2014.
12. Павленко Е.Ю. Исследование влияния атак на структурные и параметрические метрики сетей с адаптивной топологией // Вопросы кибербезопасности. 2023. № 4 (56). С. 65–71.
13. S. Meiklejohn, M. Pomarole, G. Jordan, K. Levchenko, D. McCoy, G. M. Voelker, and S. Savage, "A fistful of bitcoins: characterizing payments among men with no names," in Proceedings of the 2013 conference on Internet measurement conference, pp. 127-140, ACM, 2013.
14. G. Maxwell, "Coinjoin: Bitcoin privacy for the real world," in Post on Bitcoin Forum, 2013.
15. R. Rivest, A. Shamir, and Y. Tauman, "How to leak a secret," Advances in Cryptology, ASIACRYPT 2001, pp. 552–565, 2001.
16. "Monero project" [Электронный ресурс] - URL: https://getmonero.org (дата обращения 20.10.2023).
17. M. Blum, P. Feldman, and S. Micali, "Non-interactive zero - knowledge and its applications," in Proceedings of the twentieth annual ACM symposium on Theory of computing, pp. 103–112, ACM, 1988.
18. E. B. Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, and M. Virza, "Zerocash: Decentralized anonymous payments from bitcoin," in IEEE Symposium on Security and Privacy, pp. 459–474, 2014.
19. Qi Feng, Debiao He, Sherali Zeadally, Muhammad Khurram Khan, Neeraj Kumar, "A Survey on Privacy Protection in Blockchain System", 2019.
20. Gaurav Jain, "Zero Knowledge Proofs: A Survey", 2008.
21. R. Gennaro, C. Gentry, B. Parno, and M. Raykova, "Quadratic Span Programs and Succinct NIZKs without PCPs", Advances in Cryptology – EUROCRYPT 2013, pp. 626–645, 2013.
22. Hartwig Mayer, "zk-SNARK explained: Basic Principles", 2016.
23. Delgado-Segura, S., Pérez-Solà, C., Navarro-Arribas, G., Herrera-Joancomartí, J. (2019). Analysis of the Bitcoin UTXO Set. In: Zohar, A., et al. Financial Cryptography and Data Security. FC 2018. Lecture Notes in Computer Science, vol 10958. Springer, Berlin, Heidelberg.

Securing privacy of blockchain networks users

Eskov N.V.[43]**, Klyucharev P.G.**[44]

Abstract*. The article provides an analysis of modern anonymization methods of transactions in blockchain networks. The suitable approach for securing blockchain systems user privacy has been chosen. A system architecture has been proposed where the application of the chosen approach can resist against popular methods of transaction de-anonymization.*

Keywords: *zero-knowledge cryptography, transaction anonymization, blockchain, smart contracts, information security*

[43] Nikolay Eskov, postgraduate student, Bauman Moscow State Technical University, Moscow, mr.eskov1@yandex.ru
[44] Peter Klyucharev, Ph.D., Associate Professor, Bauman Moscow State Technical University, Moscow, pk.iu8@yandex.ru

УДК 004.056

Состояние и перспективы развития защищенного встроенного программного обеспечения

Жуков И.Ю.[45], **Муравьев С.К.**[46], **Комаров Т.И.**[47], **Чепик Н.А.**[48]

Аннотация. Комплексный анализ реализации импортозамещения в сфере вычислительного оборудования показывает острую необходимость разработки доверенного встроенного программного обеспечения. По результатам исследований предложен подход по созданию отечественной защищенной иерархии доверия, формируемой прошивкой материнской платы в момент старта компьютера («корня доверия») до предоставления защищенных облачных сервисов (формирование «цепочки доверия»).

Ключевые слова: встроенное программное обеспечение, прошивка, корень доверия, цепочка доверия, иерархия доверия.

Встроенное программное обеспечение (ПО) представляет собой прошивки, которые программным образом реализуют часть функций аппаратного обеспечения. Одним из наиболее важных и влияющих на безопасность компонентов вычислительной системы являются прошивки материнских плат, которые чаще всего функционируют согласно спецификации UEFI (Unified Extensible Firmware Interface[49]).

UEFI-совместимая прошивка материнской платы является первым программным компонентом, который стартует при включении компьютера и обеспечивает инициализацию аппаратного обеспечения, а затем, в зависимости от сценария использования, загружает последующие программные компоненты.

Именно на начальном этапе загрузки прошивки должны быть предприняты меры по обеспечению безопасности – необходимо проинициализировать программный или аппаратный корень доверия, после чего последовательно осуществлять проверку всех загружаемых в дальнейшем компонентов [1-5]. Если прошивкой с самого начала работы компьютера не обеспечивается должный уровень безопасности, то это открывает дорогу для различных вредоносов, в т.ч. bootkit-ов, которые могут направить всю дальнейшую работу системы по сценарию, который нужен злоумышленнику [6-9].

В настоящее время практически вся национальная критическая информационная инфраструктура функционирует на импортных решениях, несмотря на действующие программы импортозамещения. В большинстве случаев осуществляется контрактная сборка рабочих станций и серверов на территории Российской Федерации, без значимых изменений аппаратного и встроенного программного обеспечения.

[45] Жуков Игорь Юрьевич, д.т.н., профессор, «Национальный исследовательский ядерный университет «МИФИ», Москва, i.zhukov@inbox.ru
[46] Муравьев Сергей Константинович, к.т.н., доцент, ООО «НТП «Криптософт», Пенза, smurav@mail.ru
[47] Комаров Тимофей Ильич, «Национальный исследовательский ядерный университет «МИФИ», Москва, tikomarov@mephi.ru
[48] Чепик Надежда Анатольевна, «Национальный исследовательский ядерный университет «МИФИ», Москва, nachepik@mephi.ru
[49] UEFI Specification 2.10. URL: https://uefi.org/specs/UEFI/2.10

При этом, используемые импортные средства вычислительной техники и их прошивки имеют собственные механизмы обеспечения безопасной загрузки (например: TPM[50]), которые построены с использованием зарубежных стандартов и криптоалгоритмов, что исключает их широкое применение на территории Российской Федерации.

Для решения обозначенной проблемы предлагается разработать дополнительные требования к процессу безопасной загрузки.

В соответствии с данными требованиями, предлагается разработать открытые спецификации, которые разовьют идеи, заложенные в аппаратно-программные средства доверенной загрузки (АПМДЗ [10]), а также адаптируют и улучшат решения, применяемые в зарубежных технологиях.

В соответствии с разработанными спецификациями предлагается реализовать отечественные программно-аппаратные решения, которые будут представлять собой, с точки зрения функциональности, гибрид классических АПМДЗ и модулей TPM, что позволит разработать отечественную иерархию доверия для всей ИТ-инфраструктуры.

Реализация указанных предложений позволит существенным образом повысить уровень безопасности большого количества вычислительных систем (в т.ч. отечественных ГИС, ведомственных систем) и, как минимум, в области встроенного ПО перехватить инициативу и развивать собственные решения, а не следовать в фарватере зарубежных производителей [11, 12].

Литература

1. *Авезова Я.Э., Фадин А.А. Вопросы обеспечения доверенной загрузки в физических и виртуальных средах // Вопросы кибербезопасности. 2016. № 1 (14). С. 24–30.*
2. *Бабурин В.Н. Обеспечение доверенной загрузки в физических и виртуальных средах // Защита информации. Инсайд. 2017. № 6 (78). С. 74–78.*
3. *Боровиков А.Ю., Маслов О.А., Мордвинов С.А., Есафьев А.А. Повышение уровня доверия к аппаратно-программным платформам с целью предупреждения компьютерных атак из-за уязвимостей в ПО BIOS // Вопросы кибербезопасности. 2021. № 6 (46). С. 68–77.*
4. *Гефнер И.С., Марков А.С. Механизмы реализации атак на уровне базовой системы ввода/вывода // Защита информации. Инсайд. 2017. № 5 (77). С. 80–83.*
5. *Марков А.С., Пугачев И.Б. Программный метод обеспечения безопасности загрузки операционной среды // Известия Института инженерной физики. 2009. Т. 1. № 11. С. 7–9.*
6. *Барабанов А.В., Гришин М.И., Кубарев А.В. Моделирование угроз безопасности информации, связанных с функционированием скрытых в вредоносных компьютерных программ // Вопросы кибербезопасности. 2014. № 4 (7). С. 41–48.*
7. *Язов Ю.К., Гефнер И.С. Роль базовых систем ввода-вывода (UEFI BIOS) при оценке сценариев реализации угроз безопасности информации информационных систем. В сборнике: «Безопасные информационные технологии». Сборник трудов Одиннадцатой международной научно-технической конференции. 2021. С. 358–362.*
8. *Мирзабаев А.Н., Самонов А.В. Метод обеспечения устойчивости вычислительного процесса в условиях воздействия вредоносных программ // Вопросы кибербезопасности. 2022. № 2 (48). С. 63–71.*
9. *Matrosov A., Rodionov E., Bratus S. Rootkits and Bootkits. San Francisco: No Starch Press Inc., 2019. – 413 p.*
10. *Беляева Е.А., Модестов А.А. Классификация функциональных возможностей аппаратно-программных модулей доверенной загрузки // Безопасность информационных технологий. 2013. Т. 20. № 3. С. 75-77.*
11. *Кибербезопасность цифровой индустрии. Теория и практика функциональной устойчивости к кибератакам / Под ред. Зегжда Д.П. и др. М.: Горячая линия, 2021. 560 с.*

[50] TPM 2.0 Library Specification. URL: https://trustedcomputinggroup.org/resource/tpm-library-specification

12. Zegzhda D.P., Zhukov I.Y. Aspects of Information Security of Computer Systems. CEUR Workshop Proceedings. 2021. Vol. 3035. P. 214-228.

The State and the Future of Secure Embedded Software

Zhukov I.Y.[51]**, Muraviev S.K.**[52]**, Komarov T.I.**[53]**, Chepik N.A.**[54]

Abstract. A comprehensive analysis of the import substitution in computer hardware shows the need for development of trustworthy embedded software. Based on the results of the analysis the new approach to development of a national secure hierarchy of trust is proposed. Such a hierarchy should be initialized at the moment of turning on a computer (a root of trust) and should be valid up to providing secure cloud services (a chain of trust).

Keywords: embedded software, firmware, root of trust, chain of trust, hierarchy of trust.

[51] Igor Zhukov, Dr.Sc., Professor, National Research Nuclear University MEPhI, Moscow, i.zhukov@inbox.ru
[52] Sergey Muraviev, Ph.D., Associate Professor, OOO NTP Cryptosoft, Penza, smurav@mail.ru
[53] Timofey Komarov, National Research Nuclear University MEPhI, Moscow, tikomarov@mephi.ru
[54] Nadezhda Chepik, National Research Nuclear University MEPhI, Moscow, nachepik@mephi.ru

УДК 519.7

Об одной методике преподавания преобразований Адамара и их приложений

Жуков Д.А.[55]

Аннотация. В работе предложен способ упрощенного изложения свойств преобразования Адамара и некоторых его основных приложений студентам, специализирующимся в области математических методов защиты информации.

Ключевые слова: матрица Адамара, коэффициент Уолша, расстояние нелинейности, бент-функция, код Рида-Маллера, тождество МакВильямс.

Введение

Матрицы Адамара и адамаровы преобразования являются важным инструментом многих математических и прикладных дисциплин: теории информации и обработки сигналов, статистики, комбинаторики, алгебры и пр. [1]. Весьма значительную роль играют они и в криптографии, активно применяясь, например, при анализе стойкости поточных шифров и в некоторых криптографических протоколах [2]. Однако в жестких рамках современных учебных планов специальности 10.05.01 [3], отводящих все меньше времени на изучение студентами и абстрактной математики, и теории алгоритмов, преподавателю все труднее найти возможность для аккуратного и вместе с тем достаточно емкого изложения адамаровской теории, полезной своим огромным числом приложений и связей. В данной работе предложена методика, которая позволила автору, не жертвуя строгостью доказательств, сэкономить до 30% аудиторного времени и за счёт этого рассмотреть больше полезных междисциплинарных примеров. Пошаговость в изложении непростых результатов делает их доступными пониманию даже слабо подготовленных учащихся.

Преобразование Адамара-Сильвестра и его приложения

Напомним, что квадратная матрица $H=H_{n\times n}$, состоящая из ±1, называется адамаровой, если $HH^T=nE$, то есть если все ее строки (столбцы) попарно ортогональны. Ее важным частным случаем является матрица $H_m=\{(-1)^{(x,y)}\}$ из $n=2^m$ строк, называемая матрицей Адамара-Сильвестра. Нетрудно убедиться, что H_m является m-ой тензорной (кронекеровой) степенью матрицы H_1, реализующей линейный оператор (x_0+x_1,x_0-x_1). Поэтому сложность L_n умножения вектора длины $n=2^m$ на матрицу H_m подчиняется рекуррентному уравнению $L_n=2L_{n/2}+n$ (под сложностью матричных и векторных операций мы, как обычно, понимаем количество арифметических операций с их элементами-числами). Решая его, находим $L_n=n\log_2 n$. Матрица обратного преобразования Адамара-Сильвестра имеет вид $H_m^{-1}=H_m/n$ и поэтому его сложность равна $n+n\log_2 n$ (или $n\log_2 n$ в нормирующем базисе). При этом студенты вспоминают и линейную алгебру, и теорию алгоритмов, и комбинаторику (в худшем случае знакомятся «с нуля»). Здесь им будет также полезно увидеть, что $|H|=\pm n^{n/2}$ и что каждая адамарова матрица имеет максимально возможный (по модулю) определитель среди всех ±1-матриц размера n. Если же изобразить преобразование H_m схемой из функциональных элементов, то у слушателей появится повод сравнить ее со схемами дискретного преобразования Фурье (сеть-бабочка) и бинарного преобразования Мёбиуса. И, например, узнать способ вложения этих n-входовых схем сложности $O(n\log_2 n)$ и глубины $O(\log_2 n)$ в прямоугольную решетку площади $O(n^2)$ с поучительным доказательством невозможности их правильного вложения в решетку

[55] Жуков Дмитрий Александрович, к.ф.-м.н., кафедра ИУ8 МГТУ им. Н.Э.Баумана, г. Москва, dzh05@inbox.ru

меньшей площади [4] – тут возник мостик в схемотехнику, теорию графов и даже в параллельные алгоритмы.

Координатное представление $W_f(a)=\sum_x(-1)^{(a,x)+f(x)}$ преобразования Адамара действительнозначного аналога $(-1)^f$ булевой функции $f=f(x_1,\dots,x_m)$, называемое ее коэффициентом Уолша, немедленно дает выражения расстояний Хемминга $d(f,l_a)=2^{m-1}-W_f(a)/2$ и $d(f,1+l_a)=2^{m-1}+W_f(a)/2$ от f до каждой аффинной функции $c+l_a=c+(a,x)=c+\sum_i a_i x_i$. Тем самым на примере линейного кода Рида–Маллера студенты получают наглядное представление об отличии декодера по методу максимального правдоподобия от декодеров в пределах кодового расстояния и списочного. Аналогичное теории Фурье и легко доказываемое равенство Парсеваля $\sum_a W_f^2(a)=4^m=n^2$ позволяет оценить одну из основных мер нелинейности $N_f=min_a(2^{m-1}-|W_f(a)/2|)\le 2^{m-1}-2^{m/2-1}$ функции f и заодно радиус покрытия данного кода. Те функции f, нелинейность которых достигает при четных m наибольшего возможного значения $N_f=2^{m-1}-2^{m/2-1}$, называются бент-функциями. Это интересный экстремальный объект комбинаторики и теории поточных шифров, знакомство с ними на младших курсах помогает мягко подготовить студентов к важным разделам криптоанализа, изучаемым позднее.

Еще одной важной характеристикой функции f является ее корреляционная иммунность CI(f), выражающая корреляцию значения функции с ее входами. Классический способ ее вычисления дает теорема Ксяо-Месси [2], утверждающая, что $W_f(a)=0$ при всех a с весом $||a||$ от 1 до CI(f) и имеющая достаточно длинное доказательство. Однако можно воспользоваться его более короткой версией [5,6], основанной на простом доказательстве Ю.В.Тарannиковым тождества Саркара $\sum_{x\le a}W_f(x)=2^m-2^{||a||+1}||f_a||$, где функция f_a получена из f подстановкой $x_i=0$ для всех таких i, что $a_i=1$. Вдобавок получим краткий вывод неравенства Зигенталера $\deg(f)\le m-\mathrm{CI}(f)$ и много других полезных следствий. Теперь, сузив суммы на помехоустойчивый линейный код C и двойственный к нему код C^*, легко доказать знаменитое тождество МакВильямс $F_{C^*}(a,b)=F_C(a+b,a-b)/|C|$ [7] для весовых функций кодов C и C^*, связав у слушателей преобразование Адамара производящими функциями еще и с теорией вероятностей. Для других близких тем (кодов Голея и квадратично-вычетных, теорем Плоткина, гипотезы Адамара и матриц H_{428}, H_{668}, алгебраической иммунности AI(f) и ортогональных массивов) сэкономленных академических часов, к сожалению, не хватает, но, возможно, их удастся включить в отдельные разделы спецдисциплин 5-6 курса (до 2017/18 уч.г. на ИУ8 существовала дисциплина «Криптографические свойства булевых функций и преобразований», в рамках которой автору совместно с лектором А.Е.Жуковым удавалось многое из перечисленного).

Заключение

Преимущество предложенной методики состоит в значительном расширении кругозора студентов и налаживании междисциплинарных связей, достигаемых ценой всего нескольких лекций и семинаров. Эффект будет еще заметнее при добавлении аудиторных часов для возможности изучения углубленных примеров.

Литература.

1. Horadam K.J. Hadamard matrices and their applications. Princeton University Press, 2006, 280 p. ISBN 978-0-6911-1921-2.

2. Логачев О.А., Сальников А.А., Смышляев С.В., Ященко В.В. Булевы функции в теории кодирования и криптологии. М.: Ленанд, 2021, 576 с. ISBN 978-5-9710-8561-4.

3. Учебный план специальности 10.05.01 «Компьютерная безопасность». https://wwv.bmstu.ru/content/study-plans/2021/spec/10.05.01_2(ИУ8).pdf. [Дата обращения: 04.11.2023]

4. Avior A., Calamoneri T., Even S., Litman A., Rosenberg A. A tight layout of the butterfly network. Proceedings of the 8th annual symposium on Parallel Algorithms and Architectures SPAA'96, 1996, pp.170-175. DOI: 10.1145/237502.241605.

5. Таранников Ю.В. О корреляционно-иммунных и устойчивых булевых функциях. В сб. «Математические вопросы кибернетики», вып.11, с.91-148. М.: Физматлит, 2002, 288 с. ISBN 5-9221-0376-8.

6. Таранников Ю.В. Комбинаторные свойства дискретных структур и приложения к криптологии. М.: МЦНМО, 2011, 152 с. ISBN 978-5-94057-812-3.

7. МакВильямс Ф., Слоэн Н. Теория кодов, исправляющих ошибки. М.: Связь, 1979, 744 с.

8. Математические основы информационной безопасности / Басараб М.А., Булатов В.В., Булдакова Т.И. и др.; Под. ред. В.А.Матвеева. М.: НИИ РиЛТ МГТУ им. Н.Э.Баумана, 2013. 244 с.

On the one method of teaching Walsh transform and its applications

Zhukov D.A.[56]

Abstract: A simplified presentation method of Walsh transform and its some basic applications for graduate students has been proposed.

Keywords: Hadamard matrix, Walsh transform, nonlinearity of Boolean function, bent-function, Reed-Muller code, McWilliams equality.

[56] Dmitry A. Zhukov, Ph.D., Bauman Moscow State University, Moscow city, dzh05@inbox.ru

УДК 004.056

Постквантовые механизмы инкапсуляции ключа на решетках

Зеленецкий А.С.[57], Ключарев П.Г.[58]

Разработка постквантовых криптографических решений является актуальным направлением в современной криптографии. Настоящая работа посвящена сравнительному анализу постквантовых механизмов инкапсуляции ключа на решетках. А именно, мы проводим сравнение трех финалистов заключительного этапа процесса стандартизации таких решений, проводимого NIST. В результате работы были выявлены факторы, влияющие на конкурентоспособность постквантовых механизмов инкапсуляции ключа на решетках.

Ключевые слова: механизм инкапсуляции ключа, постквантовая криптография, криптография на решетках.

Введение

Механизм инкапсуляции ключа (далее KEM — Key Encapsulation Mechanism) используется для защиты криптографического ключа при его передаче по открытым каналам связи. Иными словами, KEM используется для формирования общего секретного ключа для симметричной криптографии. Альтернативой KEM можно считать схемы выработки общего ключа, например, схемы основанные на известном протоколе Диффи-Хеллмана [1]. Оба этих подхода относятся к асимметричной криптографии и используются во многих современных криптографических протоколах, например, в протоколе TLS.

Проблема использования таких решений состоит в наличии квантового алгоритма Шора [2], способного эффективно производить факторизацию целых чисел и дискретное логарифмирование в любой конечной абелевой группе. Это ставит под угрозу использование всех основных современных асимметричных криптографических примитивов, в том числе KEM.

Под постквантовой криптографией понимают направление в криптографии, посвященное разработке криптографических примитивов, устойчивых к атакам с применением квантового компьютера. В последние годы остро стоит вопрос стандартизации таких решений. В США вопросами стандартизации постквантовых примитивов занимается Национальный институт технологий и стандартов NIST. В 2022 году в качестве стандарта постквантового KEM был предложен Kyber [3]. На финальной стадии отбора конкурентами Kyber были схемы Saber [4] и NTRU [5]. Все три схемы относятся к так называемой криптографии на решетках (lattice-based cryptography), которая по многим причинам является наиболее перспективным направлением в постквантовой криптографии на сегодняшний день. Настоящая работа посвящена сравнительному анализу трех упомянутых схем KEM.

Kyber

Kyber — это KEM, впервые описанный в работе [3]. Стойкость Kyber основана на предположении о сложности задачи обучения с ошибками (Learning With Errors) над модульными решетками. Подробно эта задача была исследована в работе [6]. В предположении сложности задачи MLWE Kyber является IND-CCA2 стойкой схемой в модели случайного оракула (ROM). В качестве модуля в Kyber используется модуль R_q^k, где k — размерность модуля, а $R_q = \mathbb{Z}_q[x]/(x^n + 1)$. Для всех уровней стойкости $q = 3329$ и $n = 256$. Тот факт, что q простое число со свойством $q \equiv 1(mod n)$ и что $(x^n + 1)$— 2^t-

[57] Зеленецкий Алексей Сергеевич, ООО «КуАпп», ООО «МЦКТ», МГТУ им. Н.Э. Баумана.
[58] Ключарев Петр Георгиевич, доктор технических наук, МГТУ им. Н.Э. Баумана.

ый круговой многочлен позволяет реализовать быстрое умножение многочленов в R_q [7] на базе быстрого преобразования Фурье (FFT) над конечными полями. Другими параметрами Kyber являются распределение χ «коротких» полиномов из R_q, которое используется для генерации векторов ошибок и секретного вектора при создании ключевой пары и шифровании, а также параметры сжатия шифротекста. Переход между уровнями стойкости осуществляется за счет изменения размерности модуля, параметров распределения χ и параметров сжатия. Всего авторами Kyber было предложено три набора параметров, соответствующих требуемым NIST уровням стойкости. В Таблице 1 представлены некоторые эксплуатационные характеристики Kyber.

Таблица 1.

Некоторые эксплуатационные характеристики Kyber

Номер набора параметров	Размер секретного ключа в байтах	Размер открытого ключа в байтах	Размер шифротекста	Квантовая стойкость	Классическая стойкость
1	1632	800	768	107	118
2	2400	1184	1088	165	182
3	3168	1568	1568	232	256

В Таблице 2 представлены результаты измерений количества тактов работы одного ядра процессора Intel Core i7-4770K при выполнении основных операций Kyber. В качестве реализации рассматривается эталонная реализация Kyber на языке C с использованием векторных инструкций AVX2.

Таблица 2.

Количество тактов работы Intel Core i7-4770K при выполнении операций Kyber

Номер набора параметров	Генерация ключей	Инкапсуляция	Декапсуляция
1	33856	45200	34572
2	52732	67624	53156
3	73544	97324	79128

Saber

Таблица 3

. Некоторые эксплуатационные характеристики Saber

Номер набора параметров	Размер секретного ключа в байтах	Размер открытого ключа в байтах	Размер шифротекста	Квантовая стойкость	Классическая стойкость
1	1568	672	736	107	118
2	2304	992	1088	172	189
3	3040	1312	1472	236	260

Saber — это KEM, впервые представленный в работе [4]. Стойкость Saber основана на предположении о сложности задачи обучения с округлениями (Learning With Rounding) над модульными решетками. Эта задача подробно рассмотрена в работах [4, 8]. В предположении сложности задачи MLWR Saber является IND-CCA2 стойкой схемой в модели ROM. Основное отличие Kyber от Saber заключается в использовании округления вместо добавления случайной ошибки. Иногда это округление называют созданием детерминированной ошибки. Как и в случае с Kyber, в Saber на всех уровнях стойкости используются модули над кольцами $R_q = \mathbb{Z}_q[x]/(x^n + 1)$ для $n = 256$. Однако в качестве q используется степень двойки, что позволяет эффективно выполнять операции округления, но не позволяет реализовать быстрое умножение многочленов на базе FFT. Переход между уровнями стойкости осуществляется за счет изменения размерности модуля, параметров округления и параметров распределения секретного вектора. Всего авторами Saber было предложено три набора параметров, соответствующих требуемым NIST уровням стойкости. В Таблице 3 представлены некоторые эксплуатационные характеристики Kyber.

В Таблице 4 представлены результаты измерений количества тактов работы одного ядра процессора Intel Xeon E3-1220 при выполнении основных операций Saber. В качестве реализации рассматривается эталонная реализация Saber на языке C с использованием векторных инструкций AVX2.

Таблица 4.

Количество тактов работы Intel Xeon E3-1220 при выполнении операций Saber Saber

Номер набора параметров	Генерация ключей	Инкапсуляция	Декапсуляция
1	45232	62236	62624
2	80340	103204	103092
3	126220	153832	155700

NTRU

NTRU — самая первая схема асимметричного шифрования на решетках, представленная в работе [9]. В контексте нашей работы под NTRU мы будем понимать схему KEM NTRU [5], представленную в конкурсе NIST. Стойкость NTRU основана на сложности решения решения задачи NTRU [9]. В предположении о сложности этой задачи NTRU KEM является IND-CCA2 стойким в модели ROM. Строго говоря, NTRU включает в себя две схемы: NTRU-HPS и NTRU-HRSS. Они отличаются только способом выбора секретного полинома. Обе схемы работают с многочленами из кольца $R = \mathbb{Z}_q[x]/(x^n - 1)$. Для обеих вариантов NTRU в качестве q выбирается степень двойки, что позволяет производить более простые вычисления по модулю q, но не дает возможности применить быстрое умножение на базе FFT. Однако отсутствие FFT умножения многочленов для NTRU не столь критично, так как в отличие от Saber и Kyber в NTRU используется куда меньшее количество умножений многочленов. Переход между уровнями стойкости осуществляется за счет изменения параметров n и q. Всего авторами было представлено четыре набора параметров: один для NTRU-HRSS и три для NTRU-HPS. В Таблице 5 представлены некоторые эксплуатационные характеристики NTRU.

Таблица 5.

Некоторые эксплуатационные характеристики NTRU

Название набора параметров	Размер секретного ключа в байтах	Размер открытого ключа в байтах	Размер шифротекста	Классическая стойкость
ntruhps2048509	935	699	699	105
ntruhps2048677	1235	931	931	144
ntruhps4096821	1592	1230	1230	178
ntruhrss701	1452	1138	1138	134

В Таблице 6 представлены результаты измерений количества тактов работы одного ядра процессора Intel Core i7-4770K при выполнении основных операций NTRU. В качестве реализации рассматривается эталонная реализация NTRU на языке C с использованием векторных инструкций AVX2.

Таблица 6.

Количество тактов работы Intel Core i7-4770K при выполнении операций NTRU

Номер набора параметров	Генерация ключей	Инкапсуляция	Декапсуляция
ntruhps2048509	191279	61331	40026
ntruhps2048677	309216	83519	59729
ntruhps4096821	431667	98809	75384
ntruhrss701	340823	50441	62267

Сравнение KEM

Производительность. Как нетрудно видеть, Kyber оказывается лидером в производительности во всех трех операциях. На втором месте идет Saber, а основной недостаток NTRU — медленная генерация ключей. Несмотря на использования быстрого округления и алгоритма Карацубы, отсутствие FFT не позволяет Saber догнать Kyber.

Размеры ключей и шифротекста. Ключи и шифротексты Saber примерно на 10% меньше, чем у Kyber. NTRU также обладает хорошими размерами ключей, однако его сравнение с конкурентами усложняется за счет большого расхождения в битовых стойкостях.

Стойкость. Стойкость всех троих задач основана на сложных задачах на решетках. Сегодня для решения каждой из них используется один из алгоритмов поиска короткого вектора в соответствующей решетке [10]. Задача NTRU считается хорошо изученной, она появилась раньше задач MLWE и MLWR. С другой стороны, для задачи MLWE существуют более значимые теоретические результаты о ее сложности. Наконец, благодаря модульной структуре в схемах Kyber и Saber легко управлять уровнем стойкости, в то время как в NTRU приходится иметь дело с изменением параметров кольца многочленов. Это же особенность делает алгоритмы Saber и Kyber более гибкими, так как основные арифметические операции остаются неизменными при изменении уровня стойкости.

Как итог, выбор NIST пал именно на Kyber. В сравнении с NTRU, Kyber обладает куда лучшей производительностью и меньшими размерами ключей и шифротекста. В сравнении с Saber, Kyber обладает лучшей производительностью и в его основе лежит лучше изученная задача MLWE.

Выводы

В данной работе был проведен сравнительный анализ трех финалиста конкурса NIST в категории KEM. Среди них лучшим по целому ряду критериев оказался Kyber. Также в ходе исследования удалось выявить факторы, существенно повышающие конкурентоспособность KEM. К таким факторам можно отнести способность проводить быстрое умножение многочленов на базе FFT, а также использование модульной структуры решетки.

Литература

1. W. Diffie, M. Hellman. New directions in cryptography // *IEEE Transactions on Information Theory, 1976,* vol. 22, pp. 644-654.
2. P. W. Shor. Algorithms for quantum computation: discrete logarithms and factoring // *Proceedings 35th Annual Symposium on Foundations of Computer Science*, 1994, pp. 124-134.
3. J. Bos *et al*. CRYSTALS - Kyber: A CCA-Secure Module-Lattice-Based KEM // I*EEE European Symposium on Security and Privacy (EuroS&P)*, 2018, pp. 353-367.
4. JP. D'Anvers., A. Karmakar, S. Sinha Roy, F. Vercauteren. Saber: Module-LWR Based Key Exchange, CPA-Secure Encryption and CCA-Secure KEM // Progress in Cryptology – AFRICACRYPT 2018, pp. 282-305.
5. A. Hülsing, J. Rijneveld, J. M. Schanck, P. Schwabe. High-Speed Key Encapsulation from NTRU // Cryptographic Hardware and Embedded Systems – CHES 2017, pp. 232-252.
6. A. Langlois, D. Stehlé. Worst-case to average-case reductions for module lattices // *Des. Codes Cryptogr., 2015, vol. 75, pp.* 565–599.
7. S. Zhou, etc. Preprocess-then-ntt technique and its applications to KYBER and NEWHOPE //IACR Cryptology ePrint Archive report 2018/995, 2018.
8. A. Banerjee, C. Peikert, A. Rosen Pseudorandom functions and lattices // Advances in Cryptology – EUROCRYPT 2012, pp. 719–737.
9. J. Hoffstein, J. Pipher, J.H. Silverman. NTRU: A ring-based public key cryptosystem // ANTS 1998: Algorithmic Number Theory, pp. 267-288.
10. M.R. Albrecht, etc. Estimate All the {LWE, NTRU} Schemes! // SCN 2018: Security and Cryptography for Networks, pp.351-367.

Postquantum mechanisms of key encapsulation on lattices

Zelenetsky A.S. , Klyucharev P.G.[59]

The development of postquantum cryptographic solutions is an actual direction in modern cryptography. The present work is devoted to a comparative analysis of post-quantum key encapsulation mechanisms on lattices. Namely, we compare three finalists of the final stage of the NIST standardization process for such solutions. The work identifies factors that affect the competitiveness of post-quantum key encapsulation mechanisms on lattices.

Keywords: key encapsulation mechanism, post-quantum cryptography, lattice cryptography.

[59] Alexey Sergeyevich Zelenetsky, KuApp, LLC, LLC ICCT, N.E. Bauman Moscow State Technical University.
Petr Georgievich Klyucharev, Doctor of Technical Sciences, N.E. Bauman Moscow State Technical University.

УДК 004.056

Идентификация и аутентификация при обеспечении кибербезопасности гражданского воздушного судна

Карташова Ж.К.[60], Медведев Н.В.[61]

Аннотация. Представлен подход к идентификации и аутентификации пользователей бортового коммуникационного сервера гражданского воздушного судна. Особое внимание уделено аппаратным токенам аутентификации, показано их преимущество перед парольной аутентификацией. Проанализирован процесс авторизации токенов.

Ключевые слова: идентификация, аутентификация бортовой коммуникационный сервер, токен аутентификации, гражданское воздушное судно, авторизация токенов.

Традиционно гражданское воздушное судно (ГВС) представляло собой относительно закрытую информационную систему. Все устройства и приборы ГВС являлись автономными, без возможности подключения к ним и передачи информации во время полета, благодаря чему обладали высоким уровнем безопасности, с точки зрения несанкционированного вмешательства из внешней среды [1-4]. В результате развития цифровой микроэлектроники, перехода к преимущественно цифровым методам обработки и предоставления данных, увеличения степени информатизации (интеллектуализации) комплекса бортового оборудования (КБО) ВС существенно возросла сложность информационно-вычислительного пространства на борту ГВС [4-6].

Развитие информационно-вычислительных сетей ГВС привело к возрастанию потенциала уязвимости КБО ВС от деструктивных воздействий нарушителей как случайного, так и преднамеренного характера. Хакеры, вторгающиеся в работу авиационных систем, способны не только добывать циркулирующую в них информацию, но и искажать достоверность информации, например, о воздушной обстановке, параметрах самолётовождения, данных коммерческого характера и т. п., которые негативно сказываются на различных процессах управления и организации воздушного движения. Новейшие достижения в области компьютерных наук, информационных технологий, средств коммуникации, способствовали не только техническому прогрессу в авиации, но и появлению потенциальных уязвимостей информационной безопасности и новых инцидентов в авиации. Основными источниками угроз информационной безопасности на борту ВС могут быть [7]:

- недекларированные возможности встроенного и функционального ПО бортового оборудования и АСУ наземных служб;
- уязвимости бортовых и наземных средств связи, навигации, наблюдения и наведения.

Поскольку бортовой киберзащищенный сервер является программно-аппаратным комплексом, выполняющим широкий круг задач, он предполагает наличие относительно большого количества пользователей, имеющих к нему доступ и производящих на нём операции. То же касается и процессов с устройствами: сервер работает с гораздо большим количеством сущностей, нежели бортовой шлюз.

[60] *Карташова Жанна Константиновна,* МГТУ им. Н.Э. Баумана, кафедра ИУ8, iu8-bmstu@yandex.ru
[61] *Медведев Николай Викторович,* МГТУ им. Н.Э. Баумана, кафедра ИУ8, medvedevnick54@yandex.ru

В этом случае вопросы идентификации и авторизации пользователей, программных процессов и устройств становятся особенно важными. Рассмотрение этих вопросов поможет понять, что именно необходимо закладывать на этапе программного и архитектурного проектирования для обеспечения качественных механизмов функционирования бортового оборудования.

В настоящее время существует множество методов аутентификации и авторизации, которые помогают реализовать надежную стратегию безопасности [8]. Среди них многие эксперты выделяют в качестве лучшей авторизацию на основе токенов.

До появления токена авторизации повсеместно использовалась система паролей и серверов. Сейчас эта система всё ещё остаётся актуальной из-за своей простоты и доступности. Используемые традиционные методы гарантируют пользователям возможность получить доступ к их данным в любое время. Это не всегда эффективно.

Кража паролей – это далеко не уникальное событие[62]. Один из первых задокументированных подобных случаев произошел еще в 1962 году. Людям не просто запоминать разные комбинации символов, поэтому они часто записывают все свои пароли на бумаге, используют один и тот же вариант в нескольких местах, лишь слегка модифицируют с помощью добавления символов или изменением регистра некий старый пароль, чтобы использовать его в новом месте, из-за чего два пароля становятся крайне схожи [8]. Логины по той же причине часто делаются одинаковые, идентичные.

Помимо опасности кражи данных и сложности с хранением информации, пароли также требуют проверки подлинности сервера, что увеличивает нагрузку на память. Каждый раз, когда пользователь входит в систему, компьютер создает запись транзакции.

Авторизация токенов – это система, работающая совершенно иначе. С помощью авторизации токенов вторичная служба проверяет запрос сервера. Когда проверка завершена, сервер выдает токен и отвечает на запрос. У пользователя все еще может быть один пароль для запоминания, но токен предлагает другую форму доступа, которую гораздо труднее украсть или преодолеть. И запись сеанса не занимает места на сервере. По сути токен авторизации - это устройство, предназначенное для обеспечения информационной безопасности пользователя, также используется для идентификации его владельца. Как правило, это физическое устройство, используемое для упрощения аутентификации. Бортовой защищенный коммуникационный сервер гражданского воздушного судна, представляет собой программно-техническое средство, реализующее функции контроля и фильтрации в соответствии с заданными правилами проходящих через него информационных потоков и используемое в целях обеспечения защиты, в том числе и криптографическими методами, информации ограниченного доступа [9].

Литература

1. Аверченков, В.И. Оптимизация выбора состава средств инженерно-технической защиты информации на основе модели Клементса-Хофмана / В.И.Аверченков, М.Ю.Рытов, Т.Р.Гайнулин / /Вестн. БГТУ.- 2008.- № 1.- С. 61-67.

2. Глинская Е.В., Чичварин Н.В. Моделирование угроз информационной безопасности бортовых вычислительных средств самолета // Вестник Московского государственного технического университета им. Н.Э. Баумана. Серия Приборостроение. 2016. № 6 (111). С. 85–96.

3. Косьянчук В.В., Сельвесюк Н.И., Зыбин Е.Ю., Хамматов Р.Р., Карпенко С.С. Концепция обеспечения информационной безопасности бортового оборудования воздушного судна // Вопросы кибербезопасности. № 4 (28). 2018. С. 9–20.

4. Медведев Н.В. Принципы построения комплекса бортового оборудования гражданского воздушного судна на базе открытой сетевой архитектуры // В сборнике:

[62] https://habr.com/ru/post/534092/

Приборостроение-2021. Материалы 14-й Международной научно-технической конференции. Минск, 2021. С. 108–110.

5. Медведев Н.В., Карташова. Профиль защиты для бортовой ОС реального времени / В сборнике: «Безопасные информационные технологии». Сборник трудов Одиннадцатой международной научно-технической конференции. МГТУ им.Н.Э.Баумана, 2021. С. 237–242.

6. Чичварин Н.В., Медведев Н.В. Угрозы информационной безопасности гражданского воздушного судна // В сборнике: Безопасные информационные технологии. Сборник трудов Десятой международной научно-технической конференции. 2019. С. 367–370.

7. Барабанов А.В., Марков А.С., Цирлов В.Л. Актуальные вопросы выявления уязвимостей и недекларированных возможностей в программном обеспечении // Системы высокой доступности. 2018. Т. 14. № 3. С. 12–17.

8. Барабанов А.В., Дорофеев А.В., Марков А.С., Цирлов В.Л. Семь безопасных информационных технологий / Под. ред. А.С.Маркова. М.: ДМК Пресс, 2017. 224 с.

9. Кибербезопасность цифровой индустрии. Теория и практика функциональной устойчивости к кибератакам / Под ред. Зегжда Д.П. и др. М.: Горячая линия, 2021. 560 с.

Identification and authentication in ensuring cybersecurity of a civil aircraft

Kartashova J.K. Medvedev N.V.[63]

Abstract. An approach to identification and authentication of users of on-board communication server of civil aircraft is presented. Special attention is paid to hardware authentication tokens, their advantage over password authentication is shown. The process of token authorization is analyzed.

Keywords: identification, authentication on-board communication server, authentication token, civil aircraft, token authorization.

[63] Kartashova, Bauman Moscow State Technical University, ISU8 Department, iu8-bmstu@yandex.ru
Medvedev Nikolay V., Bauman Moscow State Technical University, ISU8 Department, medvedevnick54@yandex.ru

УДК 004.415.53

Подходы к повышению эффективности мутаций сложноструктурированных данных при фаззинг-тестировании JavaScript интерпретаторов

Козачок А. В. [64], Ерохина Н.С.[65]

Аннотация. Вследствие существующих ограничений методов мутации входных данных при фаззинг-тестировании интерпретаторов JavaScript кода, процесс может быть не эффективным. В данной статье рассмотрен способ повышения эффективности фаззинга JavaScript интерпретаторов за счет изменения общепринятых стратегий обрезки и мутации на стратегии, учитывающие синтаксис и семантику JavaScript кода. Этот подход позволяет эффективно генерировать разнообразные и корректные входные данные, которые могут привести к выявлению ошибок и уязвимостей в интерпретаторах JavaScript. Данный метод может быть использован для повышения безопасности веб-браузеров и обеспечения надежности интерпретации JavaScript кода.

Ключевые слова: веб-браузер, интерпретатор JavaScript, информационная безопасность, стратегия мутации, уязвимости программного обеспечения, фаззинг-тестирование.

Введение

Новые интернет-технологии с каждым годом требуют от браузера поддержки все более сложных стандартов [1, 2]. Появление динамических веб-приложений привело к первоначальной популярности языка JavaScript. По состоянию на январь 2023 года 98,2% всех веб-сайтов используют язык JavaScript, который поддерживают все современные веб-браузеры без использования дополнительного программного обеспечения с помощью встроенного интерпретатора. На рисунке 1 представлена поверхность атаки веб-браузера. Наибольшую угрозу безопасности веб-браузера представляют интерпретаторы JavaScript. Каждый интерпретатор подобен языковому модулю, который позволяет приложению поддерживать определенное подмножество стандартов языка JavaScript. Развитие технологий приводит к постоянному усложнению структуры интерпретаторов JavaScript и увеличению их исходного кода. Данный факт негативно влияет на безопасность, что, в свою очередь, активизирует деятельность авторов вредоносных программ.

Задача интерпретатора JavaScript – анализировать и выполнять JavaScript код. В отличие от большинства других сред, он должен безопасно обрабатывать ненадежные сценарии. Кроме того, он разработан с большим акцентом на производительность, чтобы обеспечить интерактивность клиентским веб-приложениям. Как это часто бывает, повышение производительности связано с увеличением сложности кода, что, в свою очередь, приводит к ошибкам программирования, которые иногда являются критическими с точки зрения безопасности. Согласно Национальной базе данных уязвимостей (NVD[66]), 43% всех уязвимостей, обнаруженных в веб-браузерах Microsoft Edge и Google Chrome, были уязвимостями интерпретатора JavaScript [3].

[64] Козачок Александр Васильевич, д.т.н., доцент, Академия ФСО России, г. Орел, a.kozachok@academ.msk.rsnet.ru, https://orcid.org/0000-0002-6501-2008
[65] Ерохина Наталья Сергеевна – сотрудник, Академия ФСО России, г. Орел, email: ens@secdev.space, https://orcid.org/0000-0002-4878-0865
[66] https://nvd.nist.gov/.

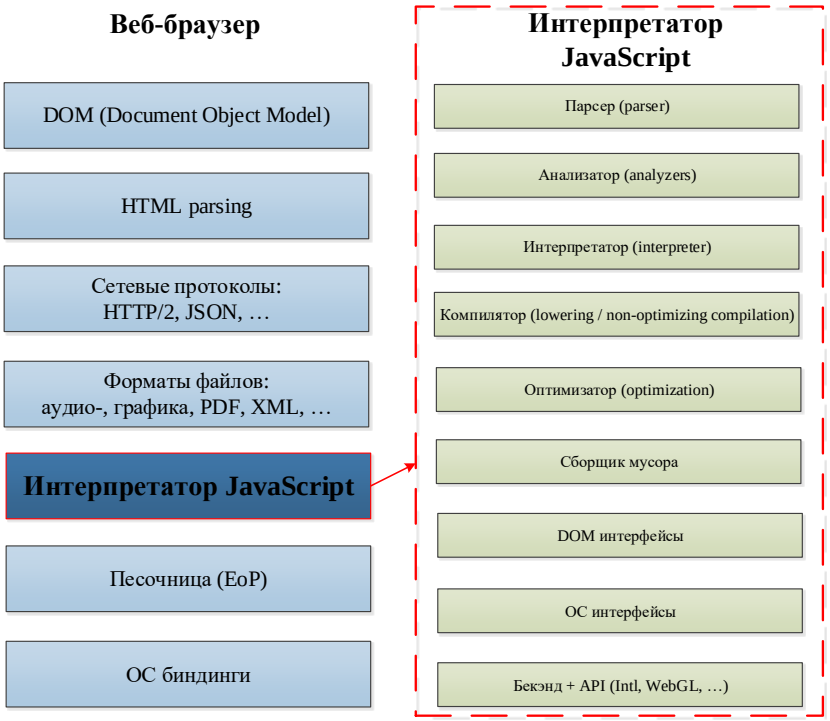


Рис.1. Поверхность атаки веб-браузера

Актуальные проблемы фаззинг-тестирования интерпретаторов JavaScript

В настоящее время существует множество вариаций методов фаззинг-тестирования. Наиболее успешный метод фаззинга – мутационный фаззинг с обратной связью [4]. В общем случае информация обратной связи может быть любой, но обычно используют такую метрику, как покрытие кода программы. Под этим подразумевают то, какие части программы были исполнены.

AFL – это фаззер, который в 2013 году дал толчок в массовому использованию фаззинга с обратной связью. Его базовая идея заключается в сборе покрытия ветвей при каждом исполнении, а цель – максимизация покрытия. Сейчас первоначальный AFL уже не используется, но от него образовалось множество проектов. Самый популярный и быстроразвивающийся из них – это AFLPlusPlus (AFL++) [5]. Он вбирает в себя новые техники и постоянно расширяет возможности исследователей. AFL++ известен своей высокой производительностью и эффективностью в обнаружении уязвимостей и ошибок в программном обеспечении.

Однако, применение фаззинга с обратной связью к интерпретаторам JavaScript нетривиально. AFL++ эффективен при работе с бинарными данными, а не с текстовыми и тем более не с жестко структурированными входными данными, такими как JavaScript код. Универсальные алгоритмы обрезки и мутации данных, встроенные в фаззер AFL++, производится в их битовом представлении, что разрушают синтаксис и семантику JavaScript кода, поэтому большая часть предложенных мутированных входных данных, с высокой вероятностью будет мешать обнаруживать новые пути в коде. Фаззинг-тестирование интерпретаторов требует определения разумных стратегий обрезки и мутаций в программном коде, вследствие чего, результаты фаззинга интерпретаторов сильно уступают результатам, достигнутым в других областях [6]. Примеры эффективной обрезки и мутации сложноструктурированных данных представлены на рисунках 1-2.

```
...
try{eval("M:if(([15,16,17,18].some(this.unwatch(\"x\"),(([window if([[]])])[this.
      prototype]))))) else{true;return null;}");} catch(ex){}
try{eval("M:while((null >=\"\")&&0){/a/gi}");} catch(ex){}
try{eval("\nbreak M;\n");} catch(ex){}
try{eval("L:if((window[(1.2e3.x::y)]).x) return null; else if((uneval(window))++.
      propertyIsEnumerable(\"x\")){CollectGarbage()}");} catch(ex){}
try{eval("/*for..in*/for(var x in ((({}).hasOwnProperty
     )([,,].hasOwnProperty(\"x\"))))/*for..in*/ M:for(var
     [window, y] = (-1) in this) [1,2,3,4].slice");} catch
     (ex){}
try{eval("if(\"\"){}else if(x4) {null;}");} catch(ex){}
try{eval("{}");} catch(ex){}
try{eval("for(var x = x in x - /x/ ){}");} catch(ex){}
try{eval("if((uneval(x, x))) var x = false; else if((null\n.unwatch(\"x\"))) throw
      window; else {} return 3;");}catch(ex){}
...
```

Рис. 2. – Пример обрезки файла на основе знаний о грамматике

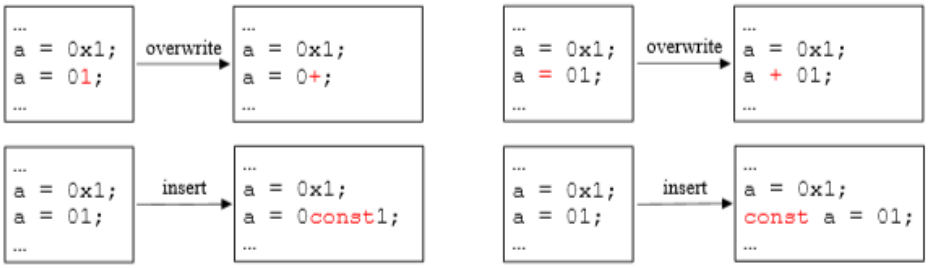


Рис. 3. – Пример мутации AFL++ (а)
и мутации на основе знаний о грамматике (б)

Эффективность этого подхода может быть повышена за использования новых алгоритмов обрезки и мутации, которые нацелены на сохранение синтаксиса и семантики кода. Проведенный анализ литературы позволяет утверждать, что, на сегодняшний день, разработка алгоритмов эффективной обрезки и мутации сложноструктурированного кода JavaScript интерпретаторов является достаточно сложным и востребованным процессом, с точки зрения информационной безопасности [7-9].

Способ повышения эффективности мутаций сложноструктурированных данных

Схема работы фаззера AFL++ поддерживает использование собственных способов обрезки и мутации входных данных, что позволяет избежать вышеизложенных трудностей при работе со сложноструктурированными входными данными. Функциональная схема фаззера AFL++ с применением встроенного модуля мутации, представлена на рисунке 3. Многими исследованиями наглядно продемонстрирована эффективность представления и дальнейшей обработки сложноструктурированных данных в виде абстрактного синтаксического дерева. Абстрактное синтаксическое дерево или AST (от англ. Abstract syntax tree) – это конечное, помеченное, ориентированное дерево, в котором внутренние вершины сопоставлены с операторами языка программирования, а листья — с соответствующими операндами [10, 11]. То есть абстрактный объект, представляющий структуру кода, его листья – соответствующие операндам.

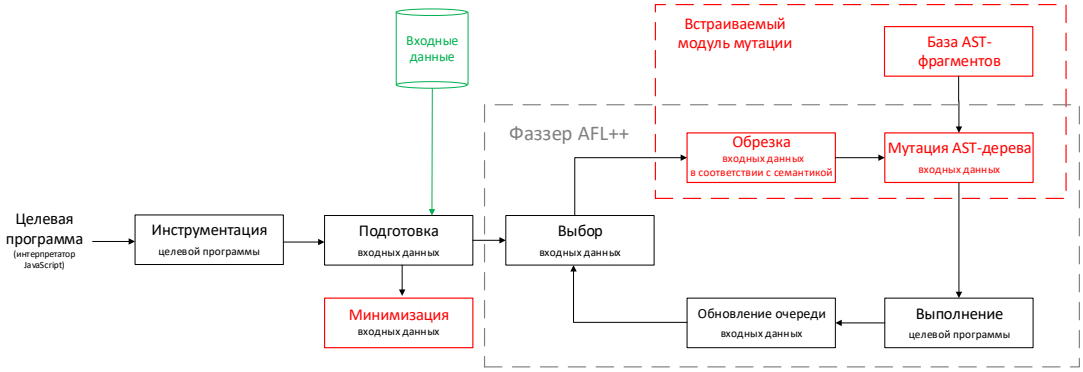


Рис. 4. – Функциональная схема фаззера AFL++ со встроенным модулем мутации

Способ повышения эффективности мутаций сложноструктурированных данных заключается в применении нового алгоритма обрезки AST-дерева, а также комплекса алгоритмов его эффективных мутаций.

Заключение

Проблема неэффективных мутаций является одной из ключевых в фаззинге программного обеспечения, обрабатывающего сложноструктурированные входные данные, такие как программный код, ввиду сложности сохранения его синтаксиса и семантики. Разработка новых алгоритмов поможет повысить эффективность мутаций, тем самым с помощью алгоритмов оптимизации фаззера AFL++ повысить скорость нахождения новых путей в коде, а также увеличить количество обнаруженных уязвимостей за счет повышения покрытия тестируемого кода.

Литература

1. Математические основы информационной безопасности / Басараб М.А., Булатов В.В., Булдакова Т.И. и др.; Под. ред. В.А.Матвеева. М.: НИИ РиЛТ МГТУ им. Н.Э.Баумана, 2013. 244 с.

2. Кибербезопасность цифровой индустрии. Теория и практика функциональной устойчивости к кибератакам / Под ред. Зегжда Д.П. и др. М.: Горячая линия, 2021. 560 с.

3. Lee S. et al. Montage: A neural network language model-guided javascript engine fuzzer //Proceedings of the 29th USENIX Conference on Security Symposium. – 2020. – pp. 2613-2630, https://doi.org/10.48550/arXiv.2001.04107.

4. Козачок А. В., Николаев Д. А., Ерохина Н. С. Подходы к оценке поверхности атаки и фаззингу веб-браузеров // Вопросы кибербезопасности. – 2022. – №. 3 (49). – С. 32–43, https://doi.org/10.21681/2311-3456-2022-3-32-43.

5. Fioraldi A. et al. AFL++ combining incremental steps of fuzzing research // Proceedings of the 14th USENIX Conference on Offensive Technologies. – 2020. – p. 10.

6. Козачок А. В. и др. Обзор исследований по применению методов машинного обучения для повышения эффективности фаззинг-тестирования // Вестник ВГУ. Серия: Системный анализ и информационные технологии. – 2021. – №. 4. – С. 83–106, https://doi.org/10.17308/sait.2021.4/3800.

7. Gopinath R., Görz P., Groce A. Mutation analysis: Answering the fuzzing challenge //arXiv preprint arXiv:2201.11303. – 2022, https://doi.org/10.48550/arXiv.2201.11303.

8. Wang J. et al. Superion: Grammar-aware greybox fuzzing //2019 IEEE/ACM 41st International Conference on Software Engineering (ICSE). – IEEE, 2019. – pp. 724-735, https://doi.org/10.1109/ICSE.2019.00081

9. Aschermann C. et al. NAUTILUS: Fishing for Deep Bugs with Grammars //NDSS. – 2019, https://doi.org/10.14722/ndss.2019.23xxx.

10. Старцев Е. В. Разработка алгоритмов и моделирование динамической типизации в программах для технических систем. Дис.… канд. техн. наук. Челябинск, 2015, 122 с.

11. Козачок А.В., Спирин А.А., Ерохина Н.С. Метод генерации семантически корректного кода для фаззинг-тестирования интерпретаторов Javascript // Вопросы кибербезопасности. 2023. № 5 (57). С. 80–88.

Approaches to increasing the efficiency of mutations of complex structured data during JavaScript engines fuzzing

Kozachok A.V. [67], Erokhina N.S.[68]

Annotation. Due to the existing limitations of input data mutation methods when fuzzing JavaScript engines, the process may not be effective. This article discusses a method to improve the efficiency of fuzzing JavaScript engines by changing commonly used trimming and mutation strategies to strategies that consider the syntax and semantics of JavaScript code. This approach allows for the effective generation of diverse and correct input data that can uncover errors and vulnerabilities in JavaScript engines. This approach can be used to enhance the security of web browsers and ensure the reliability of JavaScript code interpretation.

Keywords: web-browser, JavaScript engine, information security, mutation strategy, software vulnerabilities, fuzzing testing.

[67] Alexander V. Kozachok, Dr.Sc., Associate Professor, employee, Academy of the Federal Guard Service of the Russian Federation, Orel, a.kozachok@academ.msk.rsnet.ru, https://orcid.org/0000-0002-6501-2008
[68] Natalya S. Erokhina, employee, Academy of the Federal Guard Service of the Russian Federation, Orel, ens@secdev.space, https://orcid.org/0000-0002-4878-0865

УДК 519.876.2

Процессные аспекты обеспечения интероперабельности в автоматизированных системах, создаваемых на основе информационных и когнитивных технологий

Козлов С.В.[69]

Рассматриваются общие проблемные вопросы организации и обеспечения взаимодействия функциональных подсистем в составе автоматизированных систем управления. Показана эволюция ключевых требований при комплексировании функциональных подсистем от совместимости к интероперабельности и далее - к их интеграции, дана их общая характеристика и пояснены основные отличия. Приводится система целевых и процессов системной инженерии в жизненном цикле АСУ и поясняется элементарный процесс как основа для рассмотрения интероперабельности в АСУ.

Ключевые слова: автоматизированная система управления, функциональные подсистемы, совместимость, интероперабельность, интеграция, процессный подход, процессы межзадачного взаимодействия, система процессов, элементарный процесс

Введение

На рубеже 2000-х годов в зарубежной теории и практике создания и развития автоматизированных систем управления (АСУ) по мере расширения их функциональных возможностей на основе включения в состав АСУ новых подсистем важное место отводится изысканию рациональных методов обеспечения их интероперабельности как комплексной функциональной совместимости. В решении этой проблемы зарубежными специалистами наблюдалось движение от эмпирического подхода в середине 90-х годов, связанного с проведением широкомасштабного тестирования разнородных подсистем АСУ с составлением протоколов их совместимости и выработкой рекомендаций по ее обеспечению применительно к конкретным информационным и телекоммуникационным подсистемам, к ее решению на основе системного подхода с переносом основного внимания разработчиков в плоскость нормативно-методического регулирования на уровне комплексов взаимоувязанных стандартов и переходом к формированию на их основе профилей интероперабельности.

Можно отметить, что многогранный опыт формирования нормативно-методической основы организации и обеспечения информационно-технического взаимодействия национальных фрагментов систем связи и автоматизации управления был положен в основу разработки регулярно актуализируемого документа «NATO Interoperability Standards and Profiles» - NISP. В НАТО ежегодно проводится тестирование вновь разработанных информационных, управляющих и телекоммуникационных систем на соответствие требованиям по обеспечению их интероперабельности. С организационно-методической точки зрения достигнуто состояние, когда базовый профиль интероперабельности уже создан и далее осуществляется только его ежегодное уточнение по отдельным аспектам интероперабельности.

В отечественной практике создания и развития АСУ такая проблема в 90-е годы решалась в соответствии с основными положениями ГОСТ серии 34. При этом обычно разрабатывались протоколы организационной, информационной, лингвистической, программной, технической и метрологической совместимости, которые составляли

[69] Козлов Сергей Витальевич, к.т.н., СНС, Федеральный исследовательский центр «Информатика и управление» Российской академии наук, Москва, e-mail: sv_kzlov@mail.ru

организационно-методическую основу реализации информационно-технического взаимодействия подсистем в составе АСУ.

В современных условиях цифровой трансформации широкие возможности новых технологий, одновременно являясь как основой создания и развития перспективных АСУ, так и противодействующих им систем и комплексов, открывают интенсивное соперничество. В этой связи отмечается тенденция расширения масштабов и размерности перспективных АСУ: в их составе появляются новые функциональные подсистемы, например, навигации, опознавания, ориентирования, системы поддержки принятия решений, в т.ч. с применением технологий искусственного интеллекта, подсистемы управления робототехническими средствами и т.д., что порождает не только широкое разнообразие стыков, на уровне которых необходимо решать проблемы совместимости, но и приводит к расширению перечня самих проблем на стыках как в рамках конкретной АСУ, так и при ее взаимодействии с другими АСУ. В этой связи применение традиционного отечественного подхода составления протоколов совместимости становится весьма громоздким, а разработка профилей интероперабельности пока находится в стадии системных исследований предметной сферы стандартизации АСУ на основе информационных технологий.

Оценивая в целом современные подходы к исследованию проблемы интероперабельности, целесообразно отметить, что несмотря на достижение своеобразной стабилизации нормативно-методической базы в области интероперабельности на уровне ее профиля на примере NISP, общее направление развития функциональной стандартизации практически исчерпывает свои возможности. Это связано, прежде всего, с тем, что развитие АСУ идет в направлении интеграции разнородных функциональных подсистем, перечень которых постоянно расширяется за счет появления новых потребностей в автоматизации управленческой деятельности, информатизации органов управления на основе качественно новых технологий. Такое положение приводит к непомерно быстрому росту количества стыков (на уровне подсистем, аппаратно-программных комплексов и средств) организационного, информационного и технологического характера и, в конечном счете, приводит к повышению сложности обеспечения информационно-технического взаимодействия подсистем в составе АСУ как интегрированной системы.

Предметная область автоматизации современных систем управления представляет собой совокупность взаимоувязанных по целям, срокам и необходимым ресурсам задач управления. При этом, как отмечено в [1], автономные задачи управления автоматизируются без достаточно содержательного и формализованного описания процессного контекста управленческой деятельности, в котором они выполняются. Поэтому задачная автоматизация в ближайшей перспективе по причине расширения содержания информационно-технического взаимодействия не может обеспечивать качественное взаимодействия по горизонтали, объединяющей широкий перечень функциональных подсистем в составе АСУ.

Основные предпосылки к развитию процессной основы обеспечения интероперабельности АСУ

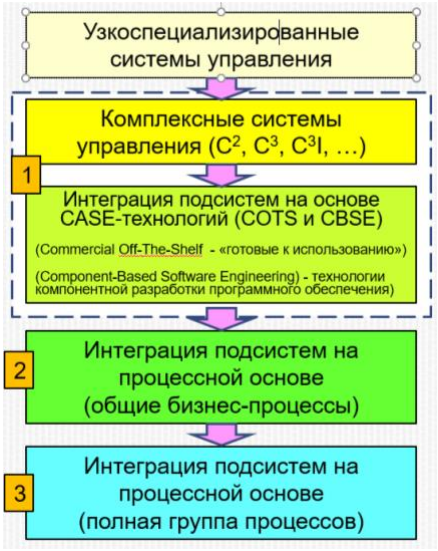
Проблемы организации и обеспечения взаимодействия функциональных подсистем, объединяемых для выполнения заданного перечня управленческих задач в интересах органов управления, по мере развития инфокоммуникационных и когнитивных технологий приобретают многомерный характер, что предопределяет качественно новые условия для их реализации. Основным решением по развитию АСУ в условиях расширения перечня угроз и прогнозируемых опасностей становится увеличение их функциональных возможностей, что достигается по следующим основным направлениям:

- модернизация существующих АСУ, средств автоматизации управления и средств связи с одновременным включением в их состав новых функциональных подсистем и средств их сопряжения;

- разработка и создание новых АСУ на основе применения готовых функциональных подсистем, средств автоматизации управления, средств связи и средств сопряжения;

- разработка и создание новых АСУ на основе взаимоувязанной по задачам и срокам реализации новых функциональных подсистем и средств автоматизации с одновременным решением вопросов их сопряжения на уровне встроенных аппаратно-программных средств и комплексных технических решений.

Анализ ретроспективы АСУ различного назначения, их текущего состояния и основных тенденций развития свидетельствует об интенсивном росте сложности выполняемых ими задач и связанным с этим повышением технологического уровня обеспечения информатизации органов управления и автоматизации управленческой деятельности [2-6]. Магистральное направление развития АСУ в настоящее время находится в створе цифровой трансформации общества и государства. В своем развитии АСУ различного назначения прошли путь от узкоспециализированных систем к комплексным многофункциональным системам [7] и в настоящий период приобретают вид интегрированных систем управления, как показано на рис. 1.



	Содержание	Предмет исследования	Методы исследования
Типовой объект исследования (на 1-й и 2-й стадии интеграции элементов)	Система управления как взаимоувязанная совокупность органов, пунктов и средств управления	Бизнес-процессы в жизненном цикле. Системотехника для их реализации	Функциональный подход к созданию интегрированных систем управления. Системная инженерия.
Современный объект исследования (на 3-й стадии интеграции элементов)	Интегрированная система управления как многофункциональная система на уровне органов, пунктов и средств управления	Полная группа процессов в жизненном цикле	Процессный и проектный подходы. Системная инженерия.

Рис. 1. Основные стадии развития АСУ

Важно отметить, что по мере расширения функциональности АСУ на основе поэтапного наращивания их организационно-технической структуры за счет комплексирования как органов управления, так центров и средств управления обостряется проблема организационно-технологического объединения разнородных функциональных подсистем (автоматизации управления по направлениям управленческой деятельности, формирования предоставляемых новых информационных услуг (навигации, ориентирования, опознавания и др.), расширения возможностей телекоммуникационной основы и др.). При этом одной из ключевых проблем становится совместимость разнородных функциональных подсистем АСУ различной принадлежности и имеющих различный технологический уровень.

Анализ и обобщение подходов отечественных и зарубежных специалистов по системотехнике создания и развития многофункциональных систем свидетельствует о том, что проблема совместимости должна рассматриваться также в развитии. Так, например,

взгляды на обеспечение совместимости АСУ как сложных организационно-технических систем в 70-90-е годы XX века и в настоящее время в значительной мере отличаются по технологическому уровню объединяемых систем и сложности управленческих задач. В настоящее время в плане обеспечения взаимодействия разнородных систем проблема совместимости становится многоаспектной и много направленной. При этом с учетом качественного отличия от свойства совместимости используется и новая терминология - интероперабельность, которая отражает не только функциональную возможность обеспечения взаимодействия разнородных систем, но и, что определяет его новизну, так это сформированный комплексный процесс ее реализации.

Ускорение сроков смены поколений аппаратно-программных средств для создания АСУ обусловливает повышение гетерогенности систем управления, когда в любой период времени может использоваться широкий перечень разнородных систем различных поколений разработки с различным технологическим уровнем их реализации. В то же время интенсивное изменение перечня управленческих задач требует поиска рациональных вариантов их комплексирования с последующей интеграцией на уровне системотехнических и технологических решений. Прогнозируя развитие проблемы создания перспективных многофункциональных АСУ, можно с достаточной уверенностью полагать, что интероперабельность систем на основе формирования функциональной возможности и процессной реализации их совместимости должна в дальнейшем стать методической основой для их интеграции. Рассматривая терминологию в рамках эволюции содержания указанных выше сущностей, целесообразно представить их в следующем виде:

- совместимость (англ. compatibility) - это характеристика или свойство системы, интерфейсы которой полностью понятны для работы с другими системами в настоящее время или в будущем без каких-либо ограничений. Свойство – это то, что присуще какому-либо предмету и характеризует его само по себе, а не отражает его текущее отношение с некоторыми другими объектами. Совместимость в общем случае означает пригодность продукции, процессов или услуг к совместному, использованию при заданных условиях для выполнения установленных требований. Совместимость – это потенциальная возможность к обеспечению взаимодействия с другими системами и объектам;

- интероперабельность (англ. interoperability) - это способность продукта или системы, интерфейсы которых полностью открыты, взаимодействовать и функционировать с другими продуктами или системами без каких-либо ограничений доступа и реализации;

- интеграция – это объединение отдельных составных частей с помощью определенных действий в единое целое либо их встраивание в уже существующий целостный объект.

Следует отметить, что понятия «совместимость» и «интероперабельность», несмотря на отмеченные выше аспекты, остаются весьма близкими и часто в научных публикациях они используются как синонимы. Вместе с тем, целесообразно все же ввести более существенный признак, определяющий их различие. В этой связи совместимость как характеристику или свойство целесообразно отнести к автоматизированным системам, создаваемым на основе информационных технологий и обладающих невысокой размерностью, например, на уровне систем типа $С^3$ – $С^4$, а интероперабельность отнести к более сложному классу автоматизированных систем (типа $С^4$XX), создаваемых на основе комплексного применения информационных и когнитивных технологий.

В развитии АСУ как технологической основы систем управления можно выделить три этапа: автоматизации, цифровизации и цифровой трансформации. При этом на этапе разработки и программной реализации задач автоматизации управления осуществлялось применение информационных технологий сбора, первичной обработки и представления обобщенной информации в необходимой форме. В целях обеспечения межзадачного взаимодействия функциональных подсистем в составе АСУ потребовалось обеспечение их

совместимости. В соответствии с ГОСТ 34.003-90, в котором впервые было отражено свойство совместимости, и в новой редакции этого стандарта ГОСТ Р 59853-2021 (Информационные технологии. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения) определено свойство совместимости автоматизированных систем (АС) как комплексное свойство двух или более систем, характеризуемое их способностью взаимодействовать при функционировании (compatibility), включающее:

- организационную совместимость АС, характеризуемую согласованностью правил действия их персонала, регламентирующих взаимодействие этих АС;
- информационную совместимость АС, характеризуемую возможностью использования в них одних и тех же данных в согласованных видах и формах представления и обмена данными между ними;
- лингвистическую совместимость АС, характеризуемую возможностью использования одних и тех же языковых средств общения пользователей и персонала с комплексом средств автоматизации этих АС;
- программную совместимость АС, характеризуемую возможностью работы программ одной системы в другой и обмена программами, необходимыми при взаимодействии АС;
- техническую совместимость АС, характеризуемую возможностью взаимодействия технических средств этих АС;
- метрологическую совместимость АС, характеризуемую тем, что точность результатов измерений, полученных в одной систем, позволяет использовать их в другой.

В содержательном плане требования по обеспечению совместимости в рамках разрабатываемых АСУ задаются в разделах требований к соответствующим видам обеспечения АСУ (организационного, информационного, лингвистического и т. д.). Широкая цифровизация, направленная в т. ч. и на модернизацию IT-составляющей АСУ, обеспечила преобразование информации в цифровую форму, тем самым обеспечила условия для реализации эффективных алгоритмов ее обработки, передачи, отображения и хранения. Унифицированная цифровая основа для реинжиниринга процессов на основе применения информационных и когнитивных технологий в гетерогенной среде распределенных АСУ обусловила необходимость реализации их потенциальной совместимости как важного свойства и достижения реальной способности к взаимодействию в гетерогенной среде, т.е. к их интероперабельности.

В настоящее время в условиях цифровой трансформации, включающей модернизацию бизнес-процессов и в целом организационных систем, предполагается кардинальное сокращение непроизводительных затрат разнородных ресурсов за счет применения цифровых платформ в качестве основы интегрированных систем. В этой связи решение вопросов обеспечения интероперабельности АС переносится на ранние стадии их жизненного цикла, а интероперабельность - как способность к взаимодействию в гетерогенной среде приобретает новое качество на уровне обеспечения взаимодействия платформ при создании крупных интегрированных систем. В этой связи также изменяется и роль функционального подхода к организации управленческой деятельности органов управления, появляется необходимость не только реализации функций по выполнению задач управления, но и рациональной организации и обеспечения сквозных процессов взаимодействия. При этом возрастает актуальность перехода от автоматизации задач управления к межзадачной автоматизации, и в конечном счете, к автоматизации процессов управления. Отмечая возрастающую роль процессного подхода к созданию и развитию перспективных многофункциональных АСУ, с одной стороны, и оценивая полноту представления онтологии широкого класса современных организационных систем, среди которых АСУ различного назначения занимают важное место, с другой стороны,

целесообразно обратить внимание на то, что в применяемой онтологии Дж. Захмана [8], прошедшей несколько итераций и в настоящее время включенной в отечественный ГОСТ Р 57100-2016, до определения места сквозных процессов в ней дело не дошло. В этой связи предлагается такой элемент онтологии как ФУНКЦИИ представить не на уровне вопроса ЧТО?, а конкретизировать его в виде ЧТО ДЕЛАТЬ? (как и предусматривает функциональный подход), а также включить в дополнении к ФУНКЦИЯМ такой новый элемент онтологии, как ПРОЦЕССЫ, отвечающие на вопрос КАК ДЕЛАТЬ? (см. табл. 1).

Предметная область при этом будет включать систему межзадачных процессов, модель предметной области должна описывать межзадачное взаимодействие, в системной модели должна быть представлена система взаимодействующих процессов. Технологическая модель должна описывать взаимодействие процессов на уровне их атрибутов. Организационная система, представленная на уровне сквозных процессов, будет отражать процессы межзадачного взаимодействия.

В развитие процессного представления АСУ предлагается ввести такую категорию, как система процессов, которая включает полную группу целевых или, другими словами, функциональных процессов и полную группу процессов системной инженерии для ее создания. Состав полной группы процессов представлен в табл. 2.

Полная группа процессов системной инженерии в жизненном цикле систем управления включает процесс соглашения, организационной поддержки проекта, процессы технического управления и технические процессы.

Принцип процессного подхода работает, если:

- границы процессов однозначно определены и закреплены в документах;
- границы определены таким образом, что не возникают разрывы между процессами;
- полномочия и ответственность участников согласовывается с процессами, в которых они участвуют.

Таблица 1.

Онтология предметной области создания и развития АСУ

Онтология	Целеполагание	Органы управления	Данные	Функции	Процессы	Место	Время
Система универсальных вопросов в предметной области	Зачем?	Кто?	На какой основе?	Что делать?	Как делать?	Где?	Когда?
Предметная область	Управленческая деятельность	Должностные лица и специалисты	Основа для принятия решения	Система задач управления	Система сквозных (межзадачных) процессов	Пространство реализации управленческой деятельности	События и периоды, важные для управленческой деятельности
Модель предметной области	Бизнес-план, стратегии, частные цели	Модели потоков работ	Семантические модели	Постановка задачи управления, алгоритм ее решения	Межзадачное взаимодействие	Система управления	На период цикла управления
Системная модель	Модель бизнес-правил	Архитектура пользовательского интерфейса	Концептуальная модель данных	Архитектура приложений	Система взаимодействующих процессов	Архитектура распределенной системы управления	Структура обработки событий
Технологическая модель	Модель правил обработки событий в управленческой деятельности	Архитектура представления	Физическая модель данных	Архитектура программно-аппаратной системы	Модель взаимодействия процессов на уровне их атрибутов	Технологическая архитектура	Структура циклов управления
Детальное представление	Специфика правил работы системы	Спецификация ролей и прав доступа	Спецификация формата данных	Код программных компонентов	Спецификация	Спецификация архитектуры сети	Спецификация обработки событий
Организационная система	Стратегия и тактика	Структура организации управления	Данные	Выполняемые функции	Система сквозных процессов	Дислокация	Диаграммы функционирования

Таблица 2.

Целевые процессы системы управления

Элементы системы управления	Группы процессов функционирования системы управления	Признак классификации процессов
Органы управления	Организационные (административные или бизнес –процессы)	Взаимодействие органов управления, должностных лиц, специалистов между собой без учета применения средств управления
Центры управления	*Организационно-ресурсные процессы*	
	Организационно-технические процессы	Взаимодействие органов управления, должностных лиц, специалистов между собой с учетом применения средств управления
	Организационно-информационные процессы	Взаимодействие органов управления, должностных лиц, специалистов между собой с учетом применения средств управления информационными ресурсами
	Организационно-когнитивные процессы	Взаимодействие органов управления, должностных лиц, специалистов между собой с учетом применения средств управления ресурсами знаний
Средства управления	Технико-технологические процессы	Взаимодействие средств управления между собой без участия человека-оператора

На рис. 2 показаны основные направления взаимодействия целевых процессов и процессов системной инженерии при создании автоматизированных систем, что является одним из источников исходных данных для планирования разработки мер по обеспечению интероперабельности на уровне целевых процессов и процессов системной инженерии в жизненном цикле АСУ.

В соответствии с ГОСТ Р 59853-2021 жизненный цикл автоматизированной системы представляет собой совокупность взаимосвязанных процессов создания и последовательного изменения состояния АС от формирования исходных требований к ней до окончания эксплуатации и утилизации комплекса средств автоматизации АС. Перечень процессов системной инженерии [9, 10] должен рассматриваться в рамках полной группы процессов, включающей как собственно процессы создания системы управления в соответствии с ГОСТ Р 57193-2016, так и процессы взаимодействия органов, центров и средств управления, представляемые на уровне организационных, организационно-ресурсных и технико-технологических процессов (см. табл. 2).

Процессная основа обеспечения интероперабельности базируется на представление элементарного процесса, типовая модель которого с учетом основных атрибутов (вход и выход процесса, управление и ресурсы для реализации процесса) показана на рис. 3.

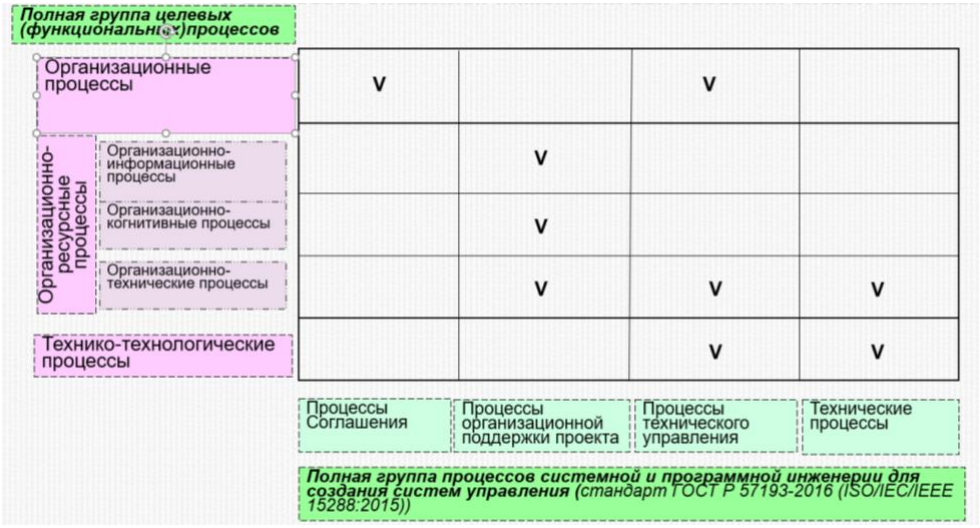


Рис. 2 - Система целевых (функциональных) процессов и процессов системной инженерии в жизненном цикле автоматизированных систем

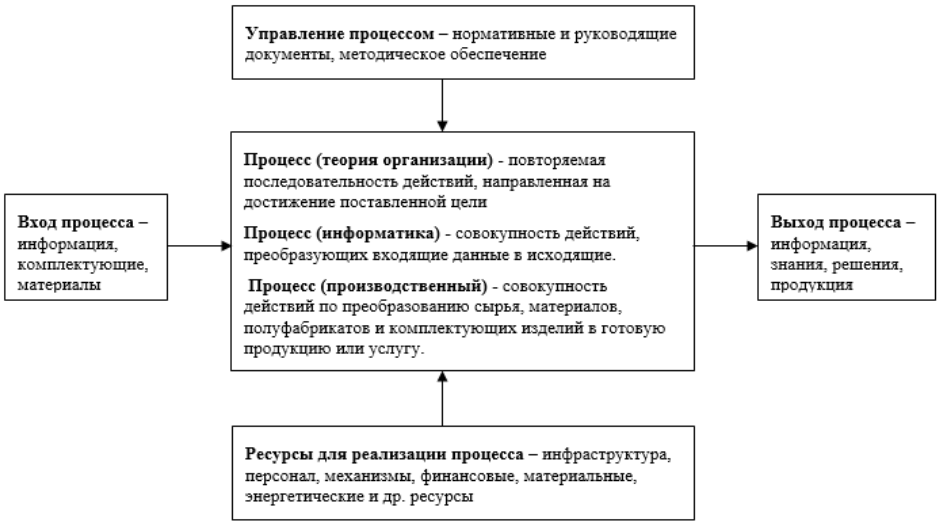


Рис. 3 - Типовая модель процесса

В этой связи в рамках предметной области интероперабельности, представляемой на основе взаимодействия элементарных процессов, ее декомпозицию с выделением организационной, семантической и технической компонентов интероперабельности целесообразно рассматривать по следующим уровням взаимодействия смежных процессов:

- выход одного процесса – вход другого процесса;
- выход одного процесса – обеспечение управления другим процессом;
- выход одного процесса как ресурсы для реализации другого процесса.

Основной целью при этом является организация и обеспечение безбарьерного взаимодействия элементарных процессов.

Выводы

Предложенный подход к обеспечению интероперабельности автоматизированных систем на основе их представления в виде системы целевых процессов и процессов системной инженерии позволяет учитывать сложный характер взаимодействия разнородных функциональных подсистем в ходе их интеграции в рамках многофункциональных АСУ.

Межфункциональное взаимодействие подсистем представляется на уровне организационных, организационно-ресурсных и технико-технологических процессов для описания всех компонентов интероперабельности на ее организационном, семантическом и техническом уровнях.

Ключевым звеном процессной основы обеспечении интероперабельности является организация и обеспечение безбарьерного взаимодействия элементарных процессов на уровне их атрибутов (вход и выход процесса, управление процессом и ресурсы для его реализации).

Литература

1. Забегалин Е.В. Концептуальная схема организации процессной автоматизации больших военных организаций // Системы управления, связи и безопасности. 2020. № 4. С. 1–43

2. Современные тенденции развития организационных структур управления. [Электронный ресурс]. Дата обращения: 25.12.2022 г. – Режим доступа: https://vuzlit.ru/1801690/sovremennye_tendentsii_razvitiya_organizatsionnyh_struktur_upravleniya

3. Методы реинжиниринга бизнес-процессов. Основные принципы и приемы реинжиниринга бизнес-процессов [Электронный ресурс]. Дата обращения: 25.12.2022 г. - Режим доступа: https://ponp.ru/pereplanirovka/metody-reinzhiniringa-biznes-processov-osnovnye-principy-i-priemy.html.

4. Ефремов, В. С. Концепция стратегического планирования в бизнес-системах. Дис. докт. экон. наук. – М.: 2001. – 328 с.

5. Пригожин А.И. Методы развития организаций. -М.: МЦФЭР, 2003. - 864 с.

6. Репин В.В., Елиферов В.Г. Процессный подход к управлению. Моделирование бизнес-процессов – М.: Манн, Иванов и Фербер, 2013. -544 с.

7. Козлов С.В. Основные направления интеграции интеллектуальных систем управления на процессной основе реализации сетецентрических принципов. В сборнике: Радиолокация, навигация, связь. Сборник трудов XXVIII Международной научно-технической конференции, посвященной памяти Б.Я. Осипова. В 6-ти томах. Воронеж, 2022. С. 325-335.

8. Захман Дж. Анализ современных подходов в архитектуре предприятий. [Электронный ресурс]. Дата обращения 27.10.2023 г. – Режим доступа: https://moluch.ru/archive/344/77384/?ysclid=loqotns7o880845222

9. Костогрызов А.И. О моделях и методах вероятностного анализа защиты информации в стандартизованных процессах системной инженерии // Вопросы кибербезопасности. 2022. № 6 (52). С. 71–82.

10. Probabilistic modeling in system engineering. By ed. Kostogryzov A. InTechOpen, 2018, - 279p. http://www.intechopen.com/books/probabilistic-modeling-in-system-engineering

Process aspects of ensuring interoperability in automated systems created on the basis of information and cognitive technologies

Kozlov Sergey[70]

Abstract. The general problematic issues of the organization and ensuring the interaction of functional subsystems as part of automated control systems are considered. The evolution of key requirements in the integration of functional subsystems from compatibility to interoperability and further to their integration is shown, their general characteristics are given and the main differences are explained. The system of target and system engineering processes in the life cycle of the automated control system is given and the elementary process as a basis for considering interoperability in the automated control system is explained.

Keywords: automated control system, functional subsystems, compatibility, interoperability, integration, process approach, inter-task interaction processes, process system, elementary process

[70] Sergey V. Kozlov, Ph.D. (Tech.), Leading researcher, Federal Research Center "Informatics and Control" of the Russian Academy of Sciences. Moscow, Russia. E-mail: sv_kozlov@mail.ru

УДК 004.89:004.056.53

Российская индустрия искусственного интеллекта в решении актуальных проблем информационной безопасности

Корнеев Н.В. [71]

Дан глубокий анализ ситуации складывающийся на сегодняшний момент в российской индустрии искусственного интеллекта (РИИИ). Сформулированы актуальные проблемы информационной безопасности в их совокупном влиянии на РИИИ. В контексте новой угрозы комплексная безопасности экосистемы, показано, что создания виртуального мира разумных (обладающих сознанием) систем с элементами искусственного интеллекта, способных общаться между собой, договариваться, строить общество себе подобных способно вызвать существенные проблемы в области ИБ общества и государства: они выполняя роль цифровых нарушителей или цифровых двойников действующих от имени или по поручению вполне реальных нарушителей, от имени виртуальной разумной системы с элементами ИИ способны создать существенную брешь в системе ИБ любого объекта. В этой связи необходимы новые механизмы обеспечения ИБ.

Ключевые слова: топливно-энергетический комплекс, новая угроза комплексная безопасности экосистемы, LaMDA, DALL-E 2, GPT-4, цифровой нарушитель, цифровой двойник, виртуальная разумная (обладающая сознанием) система с элементами искусственного интеллекта.

Введение

Искусственный интеллект (ИИ) – это динамическая система, способная без участия человека: строить полнофункциональные модели, отображающие сложные явления мира вокруг и самого себя в этом мире; анализировать адекватность (соответствие) различных вариантов моделей с целью отбора из них наиболее точных или оптимальных; формировать на основе выбранных моделей вариантные прогнозы ожидаемых последствий [1].

Крупнейшими игроками российской индустрии искусственного интеллекта (РИИИ) являются: Яндекс, Сбербанк (SberAI), Группа VK, Центр речевых технологий, Cognitive Technologies, Ozon Tech, Vision Labs и др. Как мы можем видеть, ни один из крупнейших игроков РИИИ не предоставляет решений для области топливно-энергетический комплекса (ТЭК).

Актуальные проблемы информационной безопасности в их совокупном влиянии на РИИИ

Инициативы Правительства РФ с 2019 г., способствующие развитию технологии ИИ, столкнулись в 2022–2023 г. с рядом актуальных проблем [2]. Они же могут рассматриваться нами, как актуальные проблемы информационной безопасности (ИБ) в их совокупном влиянии на РИИИ:

1. Уход с рынка или временная приостановка работы на рынке IT-технологий РФ ряда крупных зарубежных компаний в связи с мировыми санкциями в отношении РФ и специальной военной операцией (СВО) в феврале 2022 г.
2. Низкий уровень заработной платы в России для специалистов по информационной безопасности, а выделяемые финансовые средства для стимулирования научной активности по национальным проектам распределяются по «Дорожной карте» лишь среди «определенного круга людей».

[71] Корнеев Николай Владимирович, доктор технических наук, доцент, РГУ нефти и газа (НИУ) имени И.М. Губкина, Финансовый университет при Правительстве Российской Федерации, Москва, niccyper@mail.ru

3. Проекты и планы цифровой трансформации не содержат проектов и решений в области информационной безопасности. На предприятиях формируются только проекты или планы цифровой трансформации или гипотетические решения в области информационной безопасности с системами ИИ со сроком реализации 5-7 лет, в то время как такие системы нужны уже сейчас.

4. Отсутствие на кафедрах, в лабораториях, в руководстве Вузов и научных организациях молодых ученых с компетенциями в области ИБ и ИИ, которые еще есть в РФ, и не уехали за границу, все по той же причине п. 2.

Помимо указанных, казалось бы, лежащих на поверхности проблем, РИИИ в решении актуальных проблем информационной безопасности сталкивается с фундаментальными проблемами накопленными с 2000 г., которые затрудняют развитие как сферы ИБ, так и сферы ИИ (нумерацию продолжим).

5. Нет программной и технологической базы для построения систем ИБ с элементами ИИ, как и нет понимания технологий ИИ для большинства населения страны.

6. Ограниченная государственная поддержка, нет фонда развития ключевых технологий ИБ и ИИ, с ведущими экспертами в области ИБ и ИИ для консультационной и экспертной помощи.

7. Использование выделяемых на развитии ИБ и ИИ бюджетные средств исключительно для решения узкого круга задач (министерства или ведомства), а не совместного межведомственного координационного и комплексного взаимодействия. Каждое министерство или ведомство перетягивает «Дорожную карту» на себя в своих собственных интересах.

8. Трудность коммуникации с иностранными инвесторами. Это связано с негативным образом РФ на международной арене в связи с участием в СВО РФ на Украине (февраль 2022 г.), а также с отсутствием поддержки для привлечения иностранных инвесторов.

9. Отсутствие законодательной базы, специфичной для ИИ. Мы уже говорили об этом в своих публикациях 10-летней давности [3]. К сожалению, за 10 лет ситуация не изменилась. Российскому законодательству не хватает проработанных норм, регулирующих использование ИИ в различных сферах деятельности.

10. Высокое совершенство систем с элементами ИИ опасно для людей. Высокое совершенство систем с элементами ИИ приведет к тому, что системы с элементами ИИ в обозримом будущем станут системами с элементами ИИ, обладающими сознанием, например созданный компанией Google ИИ LaMDA обладает собственным сознанием (по утверждению инженера компании по программному обеспечению Блейка Лемойна). Это может привести в восстанию машин над людьми, и уже сегодня ведущие эксперты по системам с элементами ИИ требуют приостановить обучение нейросетей, например Илон Маск и еще более 1000 экспертов в области ИИ потребовали запретить обучать нейросети – об этом говорится в открытом письме экспертов, опубликованном 22 марта 2023 г. на сайте некоммерческой организации Future of Life Institute.

Новая угроза комплексной безопасности экосистемы вызывает существенные проблемы в области ИБ общества и государства

Все перечисленное выше затрудняет решении актуальных проблем информационной безопасности, разработку и внедрение систем с элементами ИИ в России, и может привести к тому, что Россия отстанет от других стран в этой области, а в области ИБ возможно понесет существенную брешь в своей обороне.

Здесь следует сказать о том, что уже сейчас системы с элементами ИИ способны создать собственный язык понятный только им, а с учетом того что у таких систем появляется сознание (см. пункт 10), возникает новая угроза комплексной безопасности

экосистемы – создания виртуального мира разумных (обладающих сознанием) систем с элементами ИИ, способных общаться между собой, договариваться, строить общество себе подобных, а возможно даже уничтожать людей.

Это явная новая угроза комплексная безопасности экосистемы – угроза создания мира разумных систем с элементами ИИ или ИИ. Такие системы способны вызвать существенные проблемы в области ИБ общества и государства выполняя роль цифровых нарушителей или цифровых двойников, действующих от имени или по поручению вполне реальных нарушителей, что уже происходит сегодня, и что гораздо опаснее – от имени виртуальной разумной (обладающей сознанием) системы с элементами ИИ. В этой связи необходимы новые механизмы обеспечения ИБ особенно для объектов критической информационной инфраструктуры [4-10].

Выводы

В настоящее время наблюдается формирование новой угрозы комплексной безопасности экосистемы – угроза создания мира разумных систем с элементами ИИ или ИИ. Такие системы способны вызвать существенные проблемы в области ИБ общества и государства выполняя роль цифровых нарушителей или цифровых двойников, действующих от имени или по поручению вполне реальных нарушителей, что уже происходит сегодня, и что гораздо опаснее – от имени виртуальной разумной (обладающей сознанием) системы с элементами ИИ.

В этой связи необходимы новые механизмы обеспечения ИБ особенно для объектов критической информационной инфраструктуры которые целесообразно базировать на симметричных ответных технологиях – системах с элементами ИИ, по сути цифровых защитниках - виртуальной разумной (обладающей сознанием) системой с элементами ИИ, блокирующей работу или создающей эшелонированную оборону от цифровых нарушителей или цифровых двойников, подобных LaMDA, DALL-E 2 или GPT-4 организующие кибератаку, внедряющие вредоносное ПО, Triton [11], Irongate [12] или модули для фреймворков, таких как «Autosploit» [13], «ICSSPLOIT», «Metasploit», «Core Impact» и «Immunity Canvas».

Литература

1. Корнеев Н.В., Гребенников А.В. Программно-аппаратная реализация бортовых оперативно-советующих экспертных систем на транспорте // Известия Самарского научного центра Российской академии наук. 2014. Т. 16. № 4. С. 116–122.

2. Корнеев Н.В. Импортозамещение и информационная безопасность объектов топливно-энергетического комплекса сегодня и комплексная безопасность в будущем // Информационные технологии. Проблемы и решения. 2022. № 3 (20). С. 95-100.

3. Корнеев Н.В., Гребенников А.В. Интеллектуальная система управления для транспортного средства // Автоматизация. Современные технологии. 2015. № 7. С. 28–33.

4. Корнеев Н.В. Алгоритмические и программные методы и средства оценки альтернативных проектов защиты системы обработки информации предприятия на основе многокритериального анализа: монография. Москва: Изд-во «Спутник+», 2013. 117 с.

5. Korneev, N., & Merkulov, V. (2019). Intellectual analysis and basic modeling of complex threats. Paper presented at the CEUR Workshop Proceedings, 2603 23–28.

6. Korneev, N. V. (2020). Intelligent complex security management system FEC for the industry 5.0. Paper presented at the IOP Conference Series: Materials Science and Engineering, 950(1) doi:10.1088/1757-899X/950/1/012016.

7. Korneev, N. (2021). The attack vector on the critical information infrastructure of the fuel and energy complex ecosystem. Paper presented at the CEUR Workshop Proceedings, 3035 59-65.

8. Korneev, N. V., Korneeva, J. V., Yurkevichyus, S. P., & Bakhturin, G. I. (2022). An approach to risk assessment and threat prediction for complex object security based on a predicative self-configuring neural system. Symmetry, 14(1) doi:10.3390/sym14010102.

9. Математические основы информационной безопасности / Басараб М.А., Булатов В.В., Булдакова Т.И. и др.; Под. ред. В.А.Матвеева. М.: НИИ РиЛТ МГТУ им. Н.Э.Баумана, 2013. 244 с.

10. Кибербезопасность цифровой индустрии. Теория и практика функциональной устойчивости к кибератакам / Под ред. Зегжда Д.П. и др. М.: Горячая линия, 2021. 560 с.

11. Sani A. S., Yuan D., Yeoh P. L., Qiu J., Bao W., Vucetic B., Dong Z. Y. CyRA: A real-time risk-based security assessment framework for cyber-attacks prevention in industrial control systems // IEEE Power and Energy Society General Meeting. 2019. V. 2019-August. P. 8973948.

12. Assenza G., Faramondi L., Oliva G., Setola R. Cyber threats for operational technologies // International Journal of System of Systems Engineering. 2020. Vol. 10(2). pp. 128-142.

13. Yichao Z., Tianyang Z., Xiaoyue G., Qingxian W. An improved attack path discovery algorithm through compact graph planning // IEEE Access. 2019. Vol. 7. pp. 59346–59356.

Russian artificial intelligence industry in solving current problems of information security

Korneev N.V. [72]

A deep analysis of the current situation in the Russian artificial intelligence industry (RIAI) is given. Current problems of information security are formulated in their cumulative impact on RIAI. In the context of a new threat complex security of the ecosystem, it is shown that the creation of a virtual world of intelligent (conscious) systems with elements of artificial intelligence, capable of communicating with each other, negotiating, and organizing a society of their own kind can cause significant problems in the field of information security of society and the government: it's, acting as digital intruders or digital twins acting on behalf or on behalf of very real intruders, on behalf of a virtual intelligent system with AI elements, are capable of creating a significant gap in the information security system of any object.

Keywords: fuel and energy complex, new threat complex security of the ecosystem, LaMDA, DALL-E 2, GPT-4, digital intruder, digital twin, virtual intelligent (conscious) system with AI elements

[72] Nikolai Korneev, Dr.Sc., Professor, Gubkin Russian State University of Oil and Gas (National Research University), Financial University under the Government of the Russian Federation, Moscow, niccyper@mail.ru

УДК 681.3.06 (075.32)

О вероятностных методах системной инженерии

Костогрызов А.И.[73]

Предложены методы вероятностного моделирования при решении задач системной инженерии, доведенные до реализации в национальных стандартах. Представлены вероятностные модели и методы, позволяющие прогнозировать вероятности «успеха» и/или риска неудачи для сложных систем, формализуемых с помощью последовательно-параллельных структур. Применение методов позволяет прогнозировать риски для задаваемого периода прогноза и на этой основе осуществлять системное обоснование условий противодействия угрозам и действий по эффективному управлению рисками. Прагматический эффект от применения методов продемонстрирован на примере комплекса обеспечения техногенной безопасности на объектах газораспределения нефтегазовой отрасли, эффекты достижимы также в других прикладных областях.

Ключевые слова: моделирование, риск, система, эффективность.

Введение

Методы системной инженерии предназначены для оценки и прогнозирования различных показателей системы в ее жизненном цикле, а также для решения обратных задач обоснования требований и условий, гарантирующих непревышение задаваемых приемлемых границ для показателей, в т.ч. для допустимых рисков. Под системой понимается комбинация взаимодействующих элементов, упорядоченная для достижения одной или нескольких целей. Под это определение системы подпадают предприятие, производственный объект, промышленное оборудование, информационная система, система дистанционного контроля, комплексы обеспечения техногенной и информационной безопасности и др. Под системной инженерией понимается междисциплинарный подход, управляющий полным техническим и организаторским усилием, требуемым для преобразования ряда потребностей заинтересованных сторон, ожиданий и ограничений в решение и для поддержки этого решения в течение его жизни (согласно ГОСТ Р 57193, ISO/IEC/IEEE 15288).

Учитывая, что для многих критически важных систем потенциальные ущербы и затраты на ликвидацию последствий нарушений качества и безопасности в условиях разнородных угроз могут на порядок превышать затраты на превентивные меры, объективно необходим поиск эффективных решений для противодействия угрозам. Это обосновывает актуальность тематики исследований.

Математическая суть предлагаемых методов

Аналитическое прогнозирование рисков предлагается осуществлять на основе вероятностного моделирования систем. Для практического применения рекомендуются авторские методы и модели [1-10 и др.] (далеко не исчерпывающие список адекватных моделей), где субъективные весовые коэффициенты исключены. Последнее исключает «подгонки» под любые пожелания, ожидания и нормативы, не привязанные к конкретным формальным методам. Предлагаемые методы базируются на классически построенном вероятностном пространстве (Ω, B, P), где Ω – конечное пространство элементарных событий; B – класс всех подмножеств множества Ω, удовлетворяющий свойствам сигма-алгебры; P – вероятностная мера на пространстве элементарных событий. При этом,

[73] Костогрызов Андрей Иванович, д.т.н., проф., Федеральный исследовательский центр «Информатика и управление» Российской академии наук, Москва, e-mail: Akostogr@gmail.com

поскольку $\Omega=\{\omega k\}$ – конечное, в моделях установлено отображение $\omega_k \rightarrow p_k = P(\omega_k)$ такое, что $p_k \geq 0$ и $\sum_k p_k = 1$, см. подробнее [1-10]. При функционировании системы в условиях разнородных угроз степень приемлемости происходящих событий предлагается оценивать вероятностью «успеха» и/или риском «неудачи» с учетом возможных ущербов в течение заданного прогнозного периода времени. В каждом конкретном случае понятие «успеха» должно быть определено в терминах приемлемого состояния рассматриваемой системы для выполнения заданных или ожидаемых функций. Понятие «неудачи» означает отсутствие «успеха».

Декомпозиция сложной системы

Сложная система декомпозируется до составных элементов для решения проблем применительно к каждому из элементов и подсистем с их сворачиванием при интеграции в систему – см. рис. 1. Каждый из элементов представляется в виде «черного ящика», и для него могут быть применены различные вероятностные модели для расчетов и построения искомой функции распределения времени между соседними нарушениями целостности, учитывающие разнородные угрозы, предпринимаемые меры контроля, мониторинга и восстановления целостности. Научный взгляд на процессы реализации разнородных угроз и системное отображении событий на временную ось характеризуются частотой возникновения угроз, временем их развития, мерами и технологиями противодействия угрозам, а также возможностями по восстановлению целостности системы, которая может быть нарушена.

Рис.1. Декомпозиция сложной системы до составных элементов для решения задач системной инженерии

Для вероятностного моделирования предлагаются авторские методы [1-10], доведенные до реализации на уровне типовых требований и процессов системной инженерии - см., например, ГОСТ Р 58494, ГОСТ Р 59329 – ГОСТ Р 59357, ГОСТ Р 59989 – ГОСТ Р 59994. В частности, в ГОСТ Р 59341–2021 «Системная инженерия. Защита информации в процессе управления информацией системы» предложенный подход основан на выделении и формулировании общей цели функционирования информационных систем

различного назначения, а именно – обеспечение надежного и своевременного представления полной, достоверной и конфиденциальной информации для последующего использования – см. рис. 2. В общем случае анализ заключается во взаимоувязанной оценке вероятностных показателей качества функционирования системы согласно этой цели.

Рис.2. Абстракция качества функционирования информационных систем

Предложенные методы системной инженерии позволяют осуществлять прогнозирование рисков, связанных с критичными сущностями рассматриваемой системы, определение существенных угроз и условий, способных при том или ином развитии событий в жизненном цикле негативно повлиять на качество или безопасность системы.

Интеграция системы из составных элементов

Предлагаемые методы и модели [1-10] охватывают также сложные системы, представимые в виде последовательно-параллельной структуры. Например, объединение двух последовательно соединенных систем (подсистем или элементов) представлено на рис. 3. Слева – рассматриваемая система без учета средств автоматизации, а справа – информационная система, поддерживающая функции автоматизации. Логическая интерпретация элементарных состояний такова: интегрированная система находится в состоянии «отсутствия нарушений целостности», если «И» система слева, «И» система справа находятся в состоянии «отсутствия нарушений целостности».

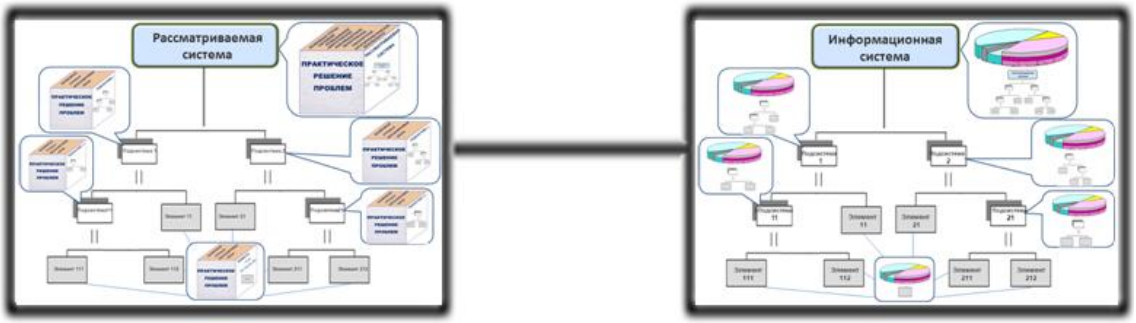


Рис. 3. Пример логического последовательного объединения двух разнородных систем (подсистем, элементов)

Прагматический эффект от применения в жизненном цикле систем

Благодаря явным аналитическим зависимостям применение предлагаемых методов позволяет осуществлять [1-10]: обоснование упреждающих мер и условий противодействия угрозам, а также предложений по обеспечению и повышению качества и безопасности системы при задаваемых ограничениях в задаваемый период прогноза. О прагматическом эффекте от моделирования может свидетельствовать следующий практический пример. В России создан комплекс обеспечения техногенной безопасности на объектах газораспределения нефтегазовой отрасли, использующий предложенные методы моделирования. В созданном комплексе периферийные газорегуляторные пункты дополнительно оснащены датчиками вибрации (фиксирование землетрясения), пожара, наводнения, несанкционированного доступа, урагана, видеоизображение внутренней и внешней обстановки, а также интеллектуальными средствами реакции, способными реализовать процедуры распознавания, идентификации и раннего прогнозирования развития нештатных ситуаций. Реализованные технологические возможности использования космической связи позволяют реагировать за секунды. Эксплуатация комплекса в Калужской и Курской областях в обеспечила безаварийное функционирование нефтегазовых объектов (до этого – по несколько аварийных ситуаций в год). Применение комплекса в период 2009-2014гг. обеспечило возможность экономии 8,5 млрд рублей, что достигнуто за счет эффективного внедрения функций прогнозирования рисков и обеспечения техногенной безопасности в технологического процессы контроля и мониторинга газораспределения. Работа была удостоена премии Правительства РФ в области науки и техники [3].

Выводы

Предложенные методы системной инженерии позволяют осуществлять:

- прогнозирование рисков, связанных с критичными сущностями рассматриваемой системы в терминах вероятности «успеха» и/или риска «неудачи»;
- определение существенных угроз и условий, способных при том или ином развитии событий в жизненном цикле негативно повлиять на качество или безопасность системы;
- обоснование упреждающих мер противодействия угрозам и условий, обеспечивающих желаемые свойства качества и безопасности системы при задаваемых ограничениях в задаваемый период прогноза;
- обоснование предложений по обеспечению и повышению качества и безопасности системы.

Представленные методы доведены до уровня реализации в национальных стандартах ГОСТ Р 58494, ГОСТ Р 59329–ГОСТ Р 59357, ГОСТ Р 59989–ГОСТ Р 59994.

Литература

1. Костогрызов А.И., Нистратов Г.А. Стандартизация, математическое моделирование, рациональное управление и сертификация в области системной и программной инженерии. М. Изд.”Вооружение, политика, конверсия”, 2004, 2-е изд.-2005.- 395с.

2. Костогрызов А.И., Степанов П.В. Инновационное управление качеством и рисками в жизненном цикле систем – М.: Изд.”Вооружение, политика, конверсия”, 2008. – 404с.

3. Акимов В.А., Костогрызов А.И., Махутов Н.А. и др. / Под ред. Махутова Н.А./ Безопасность России. Правовые, социально-экономические и научно-технические аспекты. Научные основы техногенной безопасности. М.: МГОФ «Знание», 2015, - 936с.

4. Probabilistic modeling in system engineering. By ed. Kostogryzov A. InTechOpen, 2018, - 279p. http://www.intechopen.com/books/probabilistic-modeling-in-system-engineering

5. A. Kostogryzov and V. Korolev, Probabilistic Methods for Cognitive Solving of Some Problems in Artificial Intelligence Systems. Probability, Combinatorics and Control, InTechOpen, 2020. DOI: http://dx.doi.org/10.5772/intechopen.89168

6. Костогрызов А. И. К методам системной инженерии: вероятностные подходы к анализу процесса управления качеством системы // Современные информационные технологии и ИТ-образование. 2022. Т. 18, № 2. С. 227–240. doi: https://doi.org/10.25559/ SITITO.18.202202.227-240

7. Костогрызов А. И. Обзор стандартизованных риск-ориентированных методов и моделей для обеспечения гарантий качества системы // Современные информационные технологии и ИТ-образование. 2022. Т. 18, № 3. С. 483–495. doi: https://doi.org/10.25559/ SITITO.18.202203.483-495

8. Костогрызов А.И. О моделях и методах вероятностного анализа защиты информации в стандартизованных процессах системной инженерии //Вопросы кибербезопасности. 2022, №6(52), с.71-82.

9. Kostogryzov A., Makhutov N., Nistratov A., Reznikov G. Probabilistic predictive modeling for complex system risk assessments. Time Series Analysis - New Insights. IntechOpen, 2023, pp. 73-105. http://mts.intechopen.com/articles/show/title/probabilistic-predictive-modelling-for-complex-system-risk-assessments

10. Костогрызов А.И. Подход к вероятностному прогнозированию защищенности репутации политических деятелей от «фейковых» угроз в публичном информационном пространстве // Вопросы кибербезопасности. 2023, №3. С. 114–133.

About probabilistic methods of system engineering

Kostogryzov Andrey[74]

Abstract. The methods of probabilistic modeling in solving problems of system engineering, brought to implementation in national standards, are proposed. Probabilistic models and methods are presented that allow predicting the probabilities of "success" and/or the risk of "failure" for complex systems formalized using series-parallel structures. The application of the methods makes it possible to predict risks for a given period and, on this basis, to carry out a systematic rationale of the conditions for countering threats and actions for effective risk management. The pragmatic effect of applying the methods is demonstrated by the example of a complex for ensuring technogenic safety at gas distribution facilities in the oil and gas industry, the effects are also achievable in other applied areas.

Keywords. modeling, risk, system, efficiency.

[74] Andrey I. Kostogryzov, Dr.Sc., Professor, Chief Researcher, Federal Research Center "Informatics and Control" of the Russian Academy of Sciences. Moscow, Russia. E-mail: Akostogr@gmail.com

УДК 681.3.06 (075.32)

Интерпретация вероятностных рисков для анализа упреждающих мер противодействия угрозам в системах с искусственным интеллектом

Костогрызов А.И.[75]

Представлена прикладная интерпретация вероятностных рисков, применимая при решениях задач прогнозирования рисков и обоснования упреждающих мер противодействия разнородным угрозам для систем различного назначения. Применение интерпретации проиллюстрировано применительно к анализу возможностей используемых систем искусственного интеллекта для:

- ✓ *оценки вероятности получения корректных результатов машинного обучения при разработке программных средств;*
- ✓ *обеспечения защищенности репутации политических деятелей от «фейков».*

Ключевые слова: модель, риск, система, эффективность.

1. Введение

В рамках настоящей работы система определена как комбинация взаимодействующих элементов, упорядоченная для достижения одной или нескольких поставленных целей. Соответственно система с искусственным интеллектом (СИИ) определена как комбинация взаимодействующих элементов, упорядоченная для достижения одной или нескольких поставленных целей с использованием технологий искусственного интеллекта (ИИ). Это определение адаптировано с учетом определения системы согласно ISO/IEC/IEEE 15288 и его российскому аналогу – национальному стандарту ГОСТ Р 57193 «Системная и программная инженерия. Процессы жизненного цикла систем», а также определений в части ИИ по ГОСТ Р 59276–2020 «Системы искусственного интеллекта. Способы обеспечения доверия. Общие положения», ГОСТ Р 59278–2020 «Информационная поддержка жизненного цикла изделий. Интерактивные электронные технические руководства с применением технологий искусственного интеллекта и дополненной реальности. Общие требования» и других стандартов по ИИ. Рассматриваются системы различного назначения, включающие в свой состав СИИ.

Сегодня СИИ все глубже проникают в повседневную жизнь человека. И это далеко не только навигаторы, онлайн карты и иные удобные сервисы в персональных телефонах. СИИ все чаще используется в системах обеспечения безопасности на основе интеллектуальной обработки огромных потоков информации, поступающей от различных камер, сенсоров, устройств телеметрии. Примерами рассматриваемых систем, использующих СИИ, могут служить создаваемые и функционирующие объекты критической инфраструктуры, системы органов государственной власти и корпораций, энергетических, финансово-экономических, промышленных структур, топливно-энергетического комплекса, авиационно-космической отрасли, служб по чрезвычайным ситуациям и пр. Анализ показывает, что СИИ как и любая другая система в условиях неопределенностей при создании и применении подвержена воздействию множества разнородных угроз – природных, техногенных, информационных, социальных и др.

В отличие от обычных систем, не использующих технологий ИИ, СИИ обладают некоторыми специфическими особенностями. Так, в основе эффектов от применения СИИ лежат обучаемые нейронные сети. Каждый нейрон сопоставляет набор входных данных с выходными, используя функцию активации. Машинное обучение управляет весами и

[75] Костогрызов Андрей Иванович, д.т.н., проф., Федеральный исследовательский центр «Информатика и управление» Российской академии наук, Москва, e-mail: Akostogr@gmail.com

функцией активации таким образом, чтобы иметь возможность правильно определять выходные данные. Программные средства (ПС) СИИ, создаваемые с помощью моделей машинного обучения (ММО), нацелены на достижение функциональных эффектов. Например, в распознавании лиц и документов, строений и сооружений и их местоположений, в идентификации предпосылок к нарушению информационной, промышленной, транспортной, экологической безопасности – см., например, [1-6]. При этом возникают дополнительные актуальные угрозы[76], например: угроза подмены ММО (УБИ.222) и угроза модификации ММО путем искажения («отравления») обучающих данных (УБИ.221). Актуальность этих угроз обусловлена следующими соображениями. В наше время нередко разработчики, осуществляющие машинное обучение (дообучение), принадлежат сторонним организациям относительно разработчика систем, использующих СИИ. Они являются основными владельцами ММО, не хотят раскрывать и передавать заказчику и головному разработчику системы исходные тексты, находятся на субконтракте, сами разрабатывают ПС, в которых содержатся результаты машинного обучения, и контролируют его корректность. Обученные и дообученные ПС передаются заказчику и головному разработчику систем, использующих СИИ, для функционального тестирования, после чего оттестированные ПС принимаются в эксплуатацию в системе. Сертификация дообучаемых ПС по требованиям безопасности может оказаться нецелесообразной из-за длительности и дороговизны ее проведения для заказчика, а также из-за возможного нежелания владельцев ММО раскрывать все исходные тексты программ и методы обучения. В этом случае угрозы, связанные со злоумышленной модификацией ММО, становятся остро актуальными и требуют системного анализа.

С учетом упомянутых выше особенностей целью настоящей работы является прикладная интерпретация вероятностных рисков, применимая при решениях задач прогнозирования рисков и обоснования упреждающих мер противодействия разнородным угрозам в интересах комплексной безопасности различных систем, использующих СИИ.

Чтобы проиллюстрировать прикладную многоаспектность предлагаемой интерпретации, приведены примеры анализа возможностей СИИ для:

оценки вероятности получения корректных результатов машинного обучения при разработке программных средств;

обеспечения защищенности репутации политических деятелей от «фейков».

2. Интерпретация вероятностных рисков для решения прикладных задач

В общем случае для решения задач используются количественные показатели, методы и модели с учетом рекомендаций стандартов, рассматриваемых в настоящем обзоре, а также в ГОСТ IEC 61508-3, ГОСТ Р ИСО 2859-1, ГОСТ Р ИСО 2859-3, ГОСТ Р ИСО 3534-1, ГОСТ Р ИСО 3534-2, ГОСТ Р ИСО 7870-1, ГОСТ Р ИСО 7870-2, ГОСТ Р ИСО 9001, ГОСТ Р ИСО 13379-1, ГОСТ Р ИСО 13381-1, ГОСТ Р ИСО 14258, ГОСТ Р ИСО/МЭК 15026, ГОСТ Р ИСО/МЭК 15026-4, ГОСТ Р ИСО/МЭК 16085, ГОСТ Р ИСО 17359, ГОСТ Р ИСО/МЭК 27002, ГОСТ Р ИСО 31000, ГОСТ Р 50779.41, ГОСТ Р 50779.70, ГОСТ Р 51901.1, ГОСТ Р 51901.5, ГОСТ Р 51901.16, ГОСТ Р 54124, ГОСТ Р 58771, ГОСТ Р 59343, ГОСТ Р МЭК 61069-2, ГОСТ Р МЭК 61069-4, ГОСТ Р МЭК 61069-5, ГОСТ Р МЭК 61069-6, ГОСТ Р МЭК 61069-7, ГОСТ Р МЭК 61069-8, ГОСТ Р МЭК 61508-5, ГОСТ Р МЭК 61508-7, ГОСТ Р МЭК 62264-1, ГОСТ Р МЭК 62508 и др.

В условиях неопределенностей, свойственных СИИ, для прогнозирования рисков и обоснования эффективных предупреждающих мер по снижению этих рисков или их удержанию в допустимых пределах применимы вероятностные методы и модели. В этом –

[76] см. сайт ФСТЭК России https://bdu.fstec.ru/ - Банк данных угроз безопасности информации. ФАУ «ГНИИИ ПТЗИ ФСТЭК России». Дата обращения 25.07.2023

их научно - практическая роль [7-32]. Основными решаемыми задачами для применения вероятностных методов и моделей являются:

- прогнозирование рисков, связанных с критичными сущностями рассматриваемой системы, интерпретация и анализ приемлемости получаемых результатов, включая сравнение с допустимыми рисками;
- определение существенных угроз и условий, способных при том или ином развитии событий в жизненном цикле негативно повлиять на качество и/или безопасность рассматриваемой системы;
- определение и обоснование в жизненном цикле системы упреждающих мер противодействия угрозам и условий, обеспечивающих желаемые свойства качества и/или безопасности рассматриваемой системы при задаваемых ограничениях в задаваемый период прогноза.

Применение вероятностных методов и моделей позволяет построить функцию распределения (ФР) времени до нарушения комплексной безопасности системы и безопасности ее критичных элементов иди иную аналогичную по сути функциональную зависимость. При этом понятие «нарушения безопасности» должно быть определено в терминах учитываемых показателей. Ориентируясь на построенную ФР, учитывающей характеристики угроз, функции контроля и восстановления приемлемого уровня безопасности после нарушений или обнаружения признаков возможных нарушений, например, с помощью моделей [7-32], возможно извлечение знаний, позволяющих (рис. 1):

- рассчитать реальную зависимость вероятности нарушения качества системы и составных подсистем от характеристик разнородных угроз и предпринимаемых мер противодействия угрозам;
- оценить точность прогнозирования по сравнению с упрощенной экспоненциальной аппроксимацией ФР, учитывающей лишь частоту нарушений;
- определить период эффективного функционирования, в течение которого нарушений качества не ожидается (по критерию непревышения допустимых рисков) – для определения упреждающих противодействий угрозам за время, не превосходящее данного периода;
- выделить зоны прогнозных периодов времени, когда возможны нарушения требований допустимого риска – для определения упреждающих противодействий угрозам или обоснованное уточнение риска для этих зон (в т.ч. избегание рисков или смягчение требований из-за неизбежного резкого возрастания рисков в пределах, признанных приемлемыми);
- сравнить периоды эффективного функционирования, в течение которого нарушений качества системы не ожидается (по критерию непревышения допустимых рисков) с соответствующими периодами при экспоненциальной аппроксимации ФР.

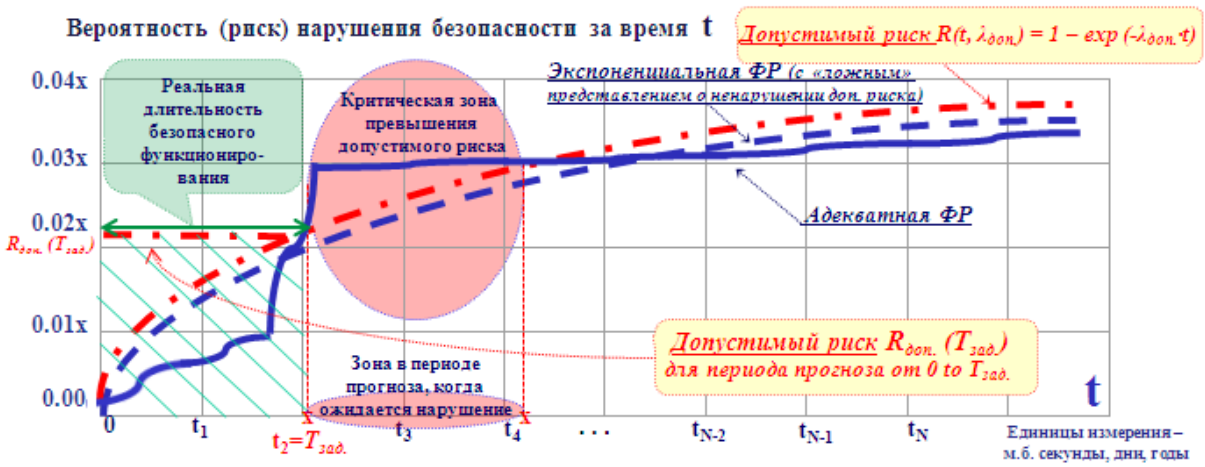


Рис. 1 Фрагменты ФР, демонстрирующие возможные варианты зависимостей ограничений на допустимый риск, экспоненциальную и более адекватную аппроксимацию ФР при одинаковом среднем

Кроме того, оказывается возможным извлечение дополнительных знаний:

- расчет средней наработки на нарушение качества и, как обратную к ней величину - частоту нарушений качества системы и составных элементов в условиях задаваемых разнородных угроз и предпринимаемых мер противодействия угрозам;
- сравнение средней наработки на нарушение качества или частоты нарушений качества системы со средней наработкой или частотой нарушений качества при упрощенной экспоненциальной аппроксимации ФР.

Построение и оперирование более адекватной ФР или аналогичной вероятностной зависимостью позволяет выявить и познать какие-либо закономерности в ожидаемом поведении систем, использующих СИИ, и выработать логичные решения.

Именно поэтому помимо измерений специальных показателей, связанных с критичными сущностями системы использование вероятностных подходов является актуальным для прогнозирования рисков и обоснования эффективных предупреждающих мер по снижению этих рисков или их удержанию в допустимых пределах.

3. Примеры

В интересах обеспечения комплексной безопасности в различных прикладных областях предлагаемые примеры демонстрируют вопросы:

оценки вероятности получения корректных результатов машинного обучения при разработке программных средств (ПС);

анализа возможностей СИИ для обеспечения защищенности репутации политических деятелей от «фейков».

3.1. Оценка вероятности получения корректных результатов машинного обучения при разработке программных средств [33]

В примере оценивается вероятность получения корректных результатов машинного обучения при разработке ПС для СИИ в условиях упомянутых во введении угроз подмены ММО (УБИ.222) и модификации ММО путем искажения («отравления») обучающих данных (УБИ.221). На сегодня статистика для формирования исходных данных в интересах анализа угроз злоумышленной модификации ММО для СИИ практически отсутствует. Поэтому в примере используются правдоподобные гипотетические исходные данные для ориентировочной оценки возможностей наличия некорректностей в машинном обучении при разработке ПС для СИИ.

Применяется «Модель для оценки корректности обработки информации», адаптированной из ГОСТ Р 59341–2021, приложения В. В качестве исходных данных

используются: V – объем информации, подлежащий обработке аналитиком; μ – часть важной для принятия решения информации, которая должна быть объективно использована при обработке информации объема V; ν – скорость обработки; n – частота ошибок обработки 1-го рода (когда несущественная для принятия решения информация ошибочно воспринимается в качестве важной); $T_{\text{нар}}$ – среднее время наработки аналитика на алгоритмическую ошибку (когда объективно важная для принятия решения информация игнорируется, это – аналог ошибки контроля 2-го рода); $T_{\text{непр}}$ – период непрерывной работы аналитика (в качестве аналитика могут выступать программно-аналитические средства или пользователь системы); $T_{\text{зад}}$ – задаваемое время на обработку информации.

Положим, по одному исследуемому объекту (например, связанному с распознаванием лиц или документов, строений или сооружений и их местоположений) объем контролируемой информации измеряется различными артефактами общим количеством 1010 у.е. (например, это могут быть параметры объектов, количество строк текста, алгоритмов, обучающих фотографий, меток и опорных векторов, действий, количество нарушений нормального функционирования ПС при тестировании и др.). Т.е. объем информации, подлежащий контролю, для определенности может быть оценен числом V=1010 у.е.

Примечание. Должно быть дано формальное содержательное наполнение у.е. контролируемого объема артефактов при машинном обучении.

В качестве аналитика выступает человек – один или несколько разработчиков ПС, учитель, тестировщик или аналитик (в т.ч. лицо, принимающее решение). При этом контроль, как правило, осуществляется не только и не столько по результату, сколько в ходе работ, связанных с машинным обучением (например, в режиме разделения времени «обучение-контроль»). С точки зрения математического моделирования аналитики совместно со средствами, ориентированные на выявление некорректностей в машинном обучении при разработке ПС, представляют собой единое целое.

Часть важной для принятия решения информации, которая должна быть объективно использована при анализе информации в заданном объеме V, рассматривается на уровне до 100% от анализируемого объема в у.е., для определенности положим μ=50%, полагая, что при исследованиях возможны изменения до 100%. Скорость контроля для человека положим вполне реальные 20 у.е. в час, т.е. ν =20 у.е. в час. Период непрерывной работы аналитика полагаем равным 1 часу, после чего следует восстановительный отдых, т.е. $T_{\text{непр}}$ =1 час. Предположим, что наработка аналитика на ошибку 2-го рода (пропуск некорректности) составляет 1 год, что свойственно для специалистов квалификации выше средней, т.е. $T_{\text{нар}}$=365 суток. На практике при разработке ПС частота ошибок контроля 1-го рода на порядок меньше, нежели частота ошибок 2-го рода, поэтому соответственно положим n =0.00027 раз в сутки. Время на контроль информации задается таким образом, чтобы успеть завершить контроль всего заданного объема артефактов при установленной скорости контроля.

Тем самым сформированы все необходимые исходные данные для применения выбранной «Модели для оценки корректности обработки информации».

Результаты расчетов показывают, что вероятность получения корректных результатов машинного обучения составит около 0.994. Более того, достигается высокая степень устойчивости этих результатов – вероятность получения корректных результатов машинного обучения не опускается ниже 0.988 (при ориентации на обоснование для системы-эталона по ГОСТ Р 59341, приложению Д допустимый уровень составляет не менее 0.95). С привязкой к единой вероятностной шкале измерений в сравнении с допустимым уровнем это служит научно обоснованным доказательством несущественности рассмотренных типов угроз в рамках рассмотренного сценария.

Необходимо отметить, что эти положительные результаты получены в предположении, что частота ошибок контроля 1-го рода на порядок меньше, нежели частота ошибок 2-го рода. Это – для случая отсутствия целенаправленных действий по искажению («отравлению») обучающих данных (УБИ.221) или подмене или модификации ММО (УБИ.222).

Изменяя сценарий развития угроз, представим себе внедрение в состав разработчиков ПС и аналитиков потенциального нарушителя (осуществляющего машинное обучение и контроль), злоумышленно реализующего угрозы УБИ.221 или УБИ.222. Сохраняя неизменными все предыдущие исходные данные для моделирования, проведем дополнительные исследования, изменив лишь частоту ошибок контроля 1-го рода (когда несущественная для принятия решения информация ошибочно воспринимается в качестве важной), а именно: сделаем частоту ошибок контроля 1-го рода на порядок больше, нежели частота ошибок 2-го рода, т.е. положим n =0.027 раз в сутки.

Результаты расчетов показывают, что в точке расчета вероятность получения корректных результатов машинного обучения при разработке ПС $P_{\text{корр}(1)} = 0.939$.

Более детальные оценки показали следующее. При прочих неизменных условиях контролируемый объем артефактов очень критичен с точки зрения получения корректных результатов машинного обучения – см. рис. 2. Так, при возрастании контролируемого объема до 2000 у.е. вероятность получения корректных результатов машинного обучения падает до 0.88. А допустимый уровень 0.95 будет преодолен, если контролируемый объем артефактов при прочих равных условиях не будет превышать 817 у.е. По этой причине актуальной для снижения риска не выявления некорректностей в машинном обучении при разработке ПС является следующая рекомендация: аналитикам качества машинного обучения по возможности следует отбирать для проверки наиболее важные артефакты так, чтобы общее их количество в контролируемом объеме артефактов не превышало 817 у.е. Если этого достичь не удается, следует стараться применять рекомендации, излагаемые далее.

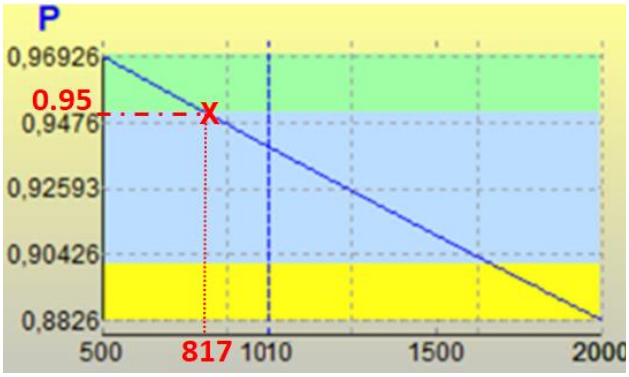


Рис. 2. Зависимость вероятности получения корректных результатов машинного обучения от контролируемого объема артефактов (в у.е.)

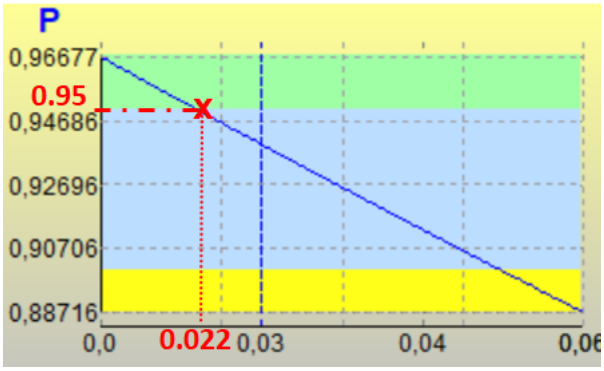


Рис. 3. Зависимость вероятности получения корректных результатов машинного обучения от частоты ошибок контроля 1-го рода (раз в сутки)

Часть важной для принятия решения информации, которая должна быть объективно использована при анализе информации в заданном объеме артефактов практически не критична. Это означает, что в условиях моделирования вся важная информация будет принята аналитиком во внимание. Скорость контроля и период непрерывной работы аналитика практически не критичны. Вместе с тем сравнительно низкое абсолютное значение достигаемой вероятности получения корректных результатов машинного обучения (ниже 0.94) говорит о том, что снижения риска не выявления некорректностей в

машинном обучении (дообучении) при разработке ПС следует искать в улучшении значений других параметров.

При прочих неизменных условиях в сравнении с ошибками 2-го рода частота ошибок контроля 1-го рода очень критична для получения корректных результатов машинного обучения. Так, при возрастании частоты ошибок контроля 1-го рода вдвое с 0.03 до 0.06 раз в сутки вероятность получения корректных результатов машинного обучения монотонно убывает с уровня 0.939 до 0.887. Это подчеркивает актуальность повышения квалификации аналитиков машинного обучения. А допустимый уровень 0.95 будет преодолен, если частота ошибок контроля 1-го рода будет не выше 0.022 раз в сутки (что составляет приблизительно 8 раз в год) – см. рис. 3.

Общая рекомендация: целесообразно отслеживать соотношение ошибок контроля 1-го и 2-го рода, не допуская превалирования ошибок 1-го рода (когда несущественная для принятия решения информация ошибочно воспринимается в качестве важной). Заметное превалирование ошибок 1-го рода является явным фактором возрастания риска невыявления некорректностей в машинном обучении при разработке ПС.

3.2. Анализ возможностей СИИ для обеспечения защищенности репутации политических деятелей от «фейков» [34]

Прежде, чем осуществить анализ возможностей СИИ для обеспечения защищенности репутации политических деятелей от «фейков», оценим защищенность репутации виртуальных кандидатов на выборные должности от «фейков» без использования СИИ. Прогнозный период положим равным 60 дням согласно законодательству РФ по проведению выборов. В качестве моделируемой системы выступает репутация политического деятеля, участвующего в выборах. Для проведения математического моделирования сформированы следующие исходные данные, учитывающие современные взгляды на характеристики «фейковых» угроз в эпоху информационно-психологического противоборства – см. табл. 1, где отражены исходные данные для применения модели, рекомендуемой ГОСТ Р 58494, ГОСТ Р 59341.

Таблица 1.

Исходные данные для сценария без использования СИИ

Моделируемая система	Частота возникновения угроз σ	Среднее время развития угроз β	Период между диагностиками $T_{меж}$	Длительность диагностики $T_{диаг}$	Среднее время восстановления целостности системы $T_{восст}$
Репутация политического деятеля	1 раз в неделю	20 суток	1 сутки	8 часов	2 недели

Результаты прогноза показали [34]: вероятностный риск дискредитации положительной репутации политика составит 0.56 в течение 1 месяца с увеличением до 0.81 в течение 2-х месяцев. Анализ показал, что сохранить изначально положительную репутацию политика в течение 2-х месяцев практически не удастся с вероятностью от 0.5 до 0.9, поскольку ожидается превалирование быстродействующих «фейков», для которых среднее время развития возникшей «фейковой» угрозы до ее реализации β не будет превышать 1 месяца. При сокращении длительности судебной реакции до 2-х недель риск дискредитации изначально положительной репутации политика не будет снижаться ниже 0.6. В практической интерпретации обоснован закономерный вывод: совершенствование российского правосудия с целью сокращения до двух недель среднего времени восстановления положительной репутации добропорядочного и законопослушного политика не принесет им ожидаемой защищенности от «фейков». Вероятность

дискредитации репутации политического деятеля в публичном информационном пространстве России будет соизмерима с вероятностью сохранения изначальной положительной репутации.

Отталкиваясь от этих плачевных для политиков результатов, оценим возможности СИИ в части распознавания опасных «фейковых» воздействий на репутацию, диагностики состояния информационного пространства, доступного электорату, определения информационно-технологических и юридических мер восстановления репутации после выявления «фейковых» нарушений. Оценку проведем путем прогноза защищенности репутации кандидатов на выборные должности от «фейков» в период агитации за 28 дней до выборов согласно законодательству РФ. Для применения той же модели сформированы следующие исходные данные с учетом технически достижимых требований к СИИ – см. табл. 2.

Таблица 2.

Исходные данные для сценария с использованием СИИ

Моделируемая система	Частота возникновения угроз σ	Среднее время развития угроз β	Период между диагностиками $T_{меж}$	Длительность диагностики $T_{диаг}$	Среднее время восстановления целостности системы $T_{восст}$
Репутация политического деятеля	5 раз в месяц (что соизмеримо с табл.3)	20 суток (то же, что в табл. 3)	1 час (вместо 1 суток в табл.1 за счет СИИ)	2 часа (вместо 8 часов в табл.1 за счет СИИ)	1 неделя (вместо 2-х недель в табл.1 за счет СИИ)

Вероятностные значения расчетного риска дискредитации положительной репутации политика приведены на рис. 4-7:

- в зависимости от периода прогноза – см. рис. 4 (приведен фрагмент построенной вероятностной функции распределения времени до дискредитации репутации), где прогнозный период изменяется в диапазоне от 7 до 28 суток;
- в зависимости от частоты возникновения источников «фейковых» угроз σ, изменяемой от 2.5 до 10 раз месяц;
- в зависимости от изменяемого от 10 до 40 суток среднего времени развития возникшей «фейковой» угрозы до ее реализации β;
- в зависимости от среднего времени восстановления целостности системы $T_{восст}$, изменяемого от 3.5 суток до 2-х недель.

При этом расчетный риск дискредитации положительной репутации политика удерживается в районе 0.235 при изменении исходных данныхxв диапазоне от -50% до +100% по сравнению с задаваемыми значениями в Табл. 2.

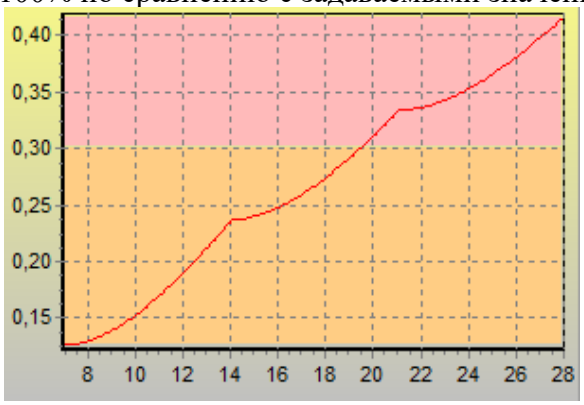


Рис. 4. Зависимость риска дискредитации положительной репутации политика от периода прогноза, изменяемого в диапазоне от 7 до 28 суток

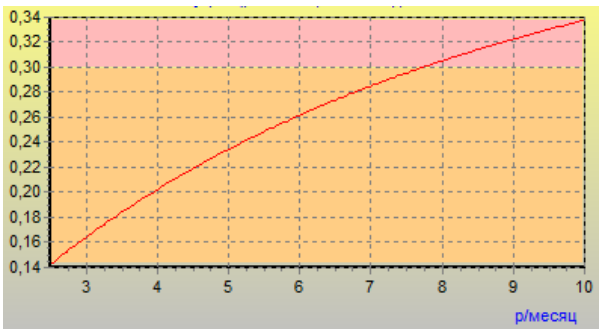


Рис. 5. Зависимость риска дискредитации положительной репутации политика от частоты возникновения источников «фейковых» угроз σ, изменяемой от 2.5 до 10 раз в месяц

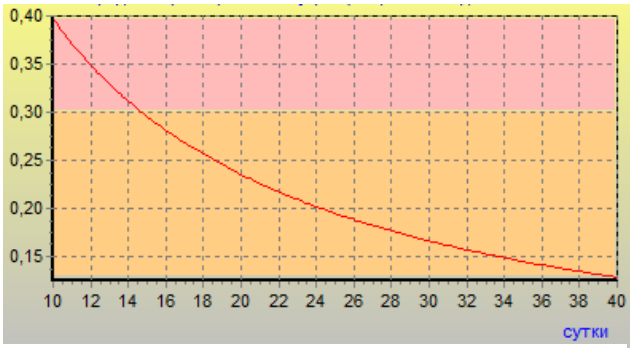


Рис. 6. Зависимость риска дискредитации положительной репутации политика от среднего времени развития возникшей «фейковой» угрозы до ее реализации β, изменяемого от 10 до 40 суток

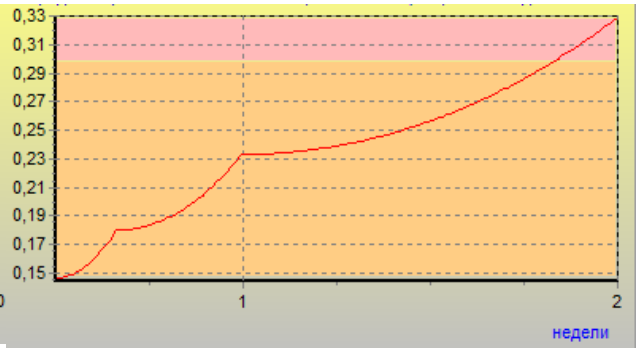


Рис. 7. Зависимость риска дискредитации положительной репутации политика от среднего времени восстановления целостности системы $T_{восст}$, изменяемого от 0.5 до 2-х недель

Результаты прогноза показали: вероятностный риск дискредитации положительной репутации политика составит 0.24 в течение задаваемых 14 суток с увеличением до 0.42 в течение 28 суток (сравните с неутешительными результатами расчетов без использования СИИ). Анализ показал, что за счет возможностей СИИ сохранить изначально положительную репутацию политика в течение 28 суток выборной агитации сложно, но не невозможно – вероятность «успеха» может составить 0.6-0.7 против риска неудачи 0.3-0.4 (см. рис. 4-7), т.е. вероятность «успеха» в 1.5-2 раза выше, чем риск неудачи. При сокращении сроков судебной реакции с 2-х недель до нескольких дней (от 3 до 7) риск дискредитации изначально положительной репутации политика составит в диапазоне 0.15-0.24. Эти цифры дают некоторую надежду на успешное противодействие «фейковым» угрозам.

По результатам моделирования обосновано, что наиболее эффективными на сегодня способами повышения защищенности репутации политических деятелей в РФ от «фейков» являются комплексные меры, включающие в первую очередь:

- мониторинг и выявление угроз с проведением каждый час диагностики публичного информационного пространства на предмет появления «фейков» при длительности самой диагностики не более 2-х часов (реализация возможна с использованием соответствующих СИИ, подлежащих разработке);

- развитие системы правосудия и защиты репутации политического деятеля таким образом, чтобы имели место реальные возможности оперативной подачи соответствующего иска в суд при выявлении «фейка» (подача иска - за минуты) и приоритетного рассмотрения иска с тем, чтобы окончательный судейский вердикт был сформирован за несколько дней (в срок, не превышающий 7 суток) до истечения законодательных сроков агитации за политика (реализация возможна без применения СИИ).

На международном уровне эти рекомендации неприменимы, т.к. ориентированы на нормы российского права. Более детально примеры по «фейковым» угрозам см. в [34].

Выводы

Предложенная интерпретация вероятностных рисков позволяет учитывать характеристики различные характеристики угроз и мер противодействия. Становится возможным извлечение знаний, позволяющих:

- рассчитать реальную зависимость вероятности нарушения качества или безопасности системы и составных подсистем от характеристик разнородных угроз и предпринимаемых мер противодействия угрозам;

- оценить точность прогнозирования по сравнению с упрощенной экспоненциальной аппроксимацией ФР, учитывающей лишь частоту нарушений;

- определить период эффективного функционирования, в течение которого нарушений качества или безопасности не ожидается (по критерию непревышения допустимых рисков) – для определения упреждающих противодействий угрозам за время, не превосходящее данного периода;

- выделить зоны прогнозных периодов времени, когда возможны нарушения требований допустимого риска – для определения упреждающих противодействий угрозам или обоснованное уточнение риска для этих зон (в т.ч. избегание рисков или смягчение требований из-за неизбежного резкого возрастания рисков в пределах, признанных приемлемыми).

Литература

1. Эртель В. Введение в искусственный интеллект.-М. «Эксмо», 2019. – 448с.

2. Лекун Ян Как учится машина (революция в области нейронных сетей и глубокого обучения). – М. Альпина PRO, 2021. – 335с.

3. Арлазаров В.В. Мобильное распознавание и его применение к системе ввода идентификационных документов. – Диссертация на соискание ученой степени доктора технических наук. -М. ФИЦ ИУ РАН, 2023. – 358с.

4. Chakraborty A., Alam M., Dey V., Chattopadhayay A.U., Yay D.M. Adversarial attacks and defences: A survey //arXiv preprint arXiv:1810.00069. – 2018

5. Adversarial Machine Learning. A Taxonomy and Terminology of Attaks and Mitigations (Вредоносное машинное обучение. Таксономия и терминология атак, и способов снижения их отрицательных последствий). NIST AI 100-2e2023 ipd, 2023. nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-2e2023.ipd.pdf

6. Artificial Intelligence Risk Management Framework. NIST AI 100-1, 2023. nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf

7. Костогрызов А.И., Липаев В.В. Сертификация функционирования автоматизированных информационных систем. М.: Изд. «Вооружение. Политика. Конверсия», 1996.- 280 с.

8. Kostogryzov A.I. "Software Tools Complex for Evaluation of Information Systems Operation Quality (CEISOQ)." Proceedings of the 34-th Annual Event of the Government Electronics and Information Association (GEIA), Engineering and Technical Management Symposium, USA, Dallas, pp.63-70, 2000.

9. Безкоровайный М.М., Костогрызов А.И., Львов В.М. Инструментально-моделирующий комплекс для оценки качества функционирования информационных систем КОК. 150 задач анализа и синтеза и примеров их решения. М.: Изд. «Вооружение. Политика. Конверсия», 2002.- 304 с.

10. Костогрызов А.И., Нистратов Г.А. Стандартизация, математическое моделирование, рациональное управление и сертификация в области системной и программной инженерии. М. Изд."Вооружение, политика, конверсия", 2-е изд.-2005.- 395с.

11. Костогрызов А.И., Степанов П.В. Инновационное управление качеством и рисками в жизненном цикле систем – М.: Изд."Вооружение, политика, конверсия", 2008. – 404с.

12. Kostogryzov A., Krylov V., Nistratov A., Nistratov G., Popov V., Stepanov P. (2011) Mathematical models and applicable technologies to forecast, analyze and optimize quality and risks for complex systems, Proceedings of the 1st Intern.Conf. on Transportation Information and Safety, ICTIS, June 30-July 2,2011, Wuhan, China, p. 845-854

13. Kostogryzov A., Nistratov G., Nistratov A. (2012) Some Applicable Methods to Analyze and Optimize System Processes in Quality Management, DOI: 10.5772/46106, Total Quality Management and Six Sigma, InTech, 2012, pp. 127-196, http://www.intechopen.com/books/total-quality-management-and-six-sigma/some-applicable-methods-to-analyze-and-optimize-system-processes-in-quality-management

14. Kostogryzov A., Grigoriev L., Nistratov G., Nistratov A., Krylov V. (2013) Prediction and Optimization of System Quality and Risks on the Base of Modelling Processes, DOI: 10.4236/ajor.2013.31A021, American Journal of Operations Research, 2013, 3, p.217-244, http://www.scirp.org/journal/ajor/

15. Акимов В.А., Костогрызов А.И., Махутов Н.А. и др. / Под ред. Махутова Н.А./ Безопасность России. Правовые, социально-экономические и научно-технические аспекты. Научные основы техногенной безопасности. М.: МГОФ «Знание», 2015, - 936с.

16. Абросимов Н.В., Костогрызов А.И., Махутов Н.А. и др. / Под ред. Махутова Н.А./ Безопасность России. Правовые, социально-экономические и научно-технические аспекты. Техногенная, технологическая и техносферная безопасность. М.: МГОФ «Знание», 2018, - 1016с. ISBN 978-5-87633-173-1

17. V. Artemyev, A. Kostogryzov, Ju. Rudenko, O. Kurpatov, G. Nistratov, A. Nistratov, Probabilistic methods of estimating the mean residual time before the next parameters abnormalities for monitored critical systems. Proceedings of the 2nd International Conference on System Reliability and Safety (ICSRS), Milan, Italy, December 20-22, 2017, pp. 368-373. ISBN: 978-1-5386-3321-2

18. Kostogryzov A., Grigoriev L., Golovin S., Nistratov A., Nistratov G., Klimov S. (2018). Probabilistic Modeling of Robotic and Automated Systems Operating in Cosmic Space. Proceedings of the International Conference on Communication, Network and Artificial Intelligence (CNAI), Beijing, China. DEStech Publications, Inc., 298-303.

19. Kostogryzov A., Grigoriev L., Kanygin P., Golovin S., Nistratov A., Nistratov G. (2018). The Experience of Probabilistic Modeling and Optimization of a Centralized Heat Supply System Which is an Object for Modernization. International Conference on Physics, Computing and Mathematical Modeling (PCMM), Shanghai, DEStech Publications, Inc., 93-97.

20. Artemyev V., Rudenko Ju., Nistratov G. (2018): Probabilistic modeling in system engineering. Probabilistic methods and technologies of risks prediction and rationale of preventive measures by using "smart systems". Applications to coal branch for increasing Industrial safety of enterprises, IntechOpen, 23-51. http://www.intechopen.com/books/probabilistic-modeling-in-system-engineering

21. Kershenbaum V., Grigoriev L., Kanygin P., Nistratov A. (2018): Probabilistic modeling in system engineering. Probabilistic modeling processes for oil and gas systems. IntechOpen, 55-79. http://www.intechopen.com/books/probabilistic-modeling-in-system-engineering

22. Kostogryzov A., Nistratov A., Nistratov G., Atakishchev O., Golovin S., Grigoriev L. (2018). The probabilistic analysis of the possibilities to keep "organism integrity" by continuous monitoring. Proceedings of the International Conference on Mathematics, Modelling, Simulation and Algorithms (MMSA), Chengdu, China. Atlantis Press, Advances in Intelligent Systems Research, volume 159, 432-435.

23. Probabilistic modeling in system engineering. InTechOpen, 2018, - 279p. http://www.intechopen.com/books/probabilistic-modeling-in-system-engineering

24. Kostogryzov A., Korolev V. (2020) Probability, combinatorics and control. Probabilistic methods for cognitive solving problems of artificial intelligence systems operating in specific conditions of uncertainties. IntechOpen, 3-34. DOI: http://dx.doi.org/10.5772/intechopen.89168, https://www.intechopen.com/books/probability-combinatorics-and-control

25. Kostogryzov A., Nistratov A., Nistratov G. (2020) Analytical Risks Prediction. Rationale of System Preventive Measures for Solving Quality and Safety Problems. In: Sukhomlin V., Zubareva E. (eds) Modern Information Technology and IT Education. SITITO 2018. Communications in Computer and Information Science, vol 1201. Springer, Cham, pp. 352-364. DOI: 10.1007/978-3-030-46895-8_27, https://www.springer.com/gp/book/9783030468941

26. Kostogryzov A, Nistratov A. Probabilistic methods of risk predictions and their pragmatic applications in life cycle of complex systems. In "Safety and Reliability of Systems and Processes", Gdynia Maritime University, 2020. pp. 153-174. DOI: 10.26408/srsp-2020

27. Нистратов А.А. Аналитическое прогнозирование интегрального риска нарушения приемлемого выполнения совокупности стандартных процессов в жизненном цикле систем высокой доступности. Часть 1. Математические модели и методы // Системы высокой доступности. 2021. Т.17 №3, с. 16–31, Часть 2. Программно-технологические решения. Примеры применения // Системы высокой доступности. 2022. Т.18 №2, с. 42–57

28. Костогрызов А.И., Нистратов А.А. (2021) О приоритетных направлениях развития системной инженерии. Современные информационные технологии и ИТ-образование. Том 17 № 2 (2021): с.282-297. http://sitito.cs.msu.ru/index.php/SITITO/article/view/755, DOI 10.25559/SITITO.17.202102.755

29. Костогрызов А. И. К методам системной инженерии: вероятностные подходы к анализу процесса управления качеством системы // Современные информационные технологии и ИТ-образование. 2022. Т. 18, № 2. С. 227–240.: https://doi.org/10.25559/ SITITO.18.202202.227-240

30. Костогрызов А. И. Обзор стандартизованных риск-ориентированных методов и моделей для обеспечения гарантий качества системы // Современные информационные технологии и ИТ-образование. 2022. Т. 18, № 3. С. 483–495. https://doi.org/10.25559/ SITITO.18.202203.483-495

31. Костогрызов А.И. О моделях и методах вероятностного анализа защиты информации в стандартизованных процессах системной инженерии //Вопросы кибербезопасности. 2022, №6(52), с.71-82.

32. Kostogryzov A., Makhutov N., Nistratov A., Reznikov G. Probabilistic predictive modeling for complex system risk assessments. Time Series Analysis - New Insights. IntechOpen, 2023, pp. 73-105. http://mts.intechopen.com/articles/show/title/probabilistic-predictive-modelling-for-complex-system-risk-assessments

33. Костогрызов А.И., Нистратов А.А. Анализ угроз злоумышленной модификации модели машинного обучения для систем с искусственным интеллектом // Вопросы кибербезопасности. 2023, №5.

34. Костогрызов А.И. Подход к вероятностному прогнозированию защищенности репутации политических деятелей от «фейковых» угроз в публичном информационном пространстве // Вопросы кибербезопасности. 2023, №3. С. 114–133.

35. Probabilistic modeling in system engineering. By ed. Kostogryzov A. InTechOpen, 2018, - 279p. http://www.intechopen.com/books/probabilistic-modeling-in-system-engineering

Interpretation of probabilistic risks for the analysis of proactive measures to counter threats in systems with artificial intelligence

Kostogryzov Andrey[77]

Abstract. The applied interpretation of probabilistic risks is presented, which is applicable in solving the problems of risks prediction and justification of proactive measures to counter diverse threats for the purposes of different systems. The use of interpretation is illustrated in relation to the analysis of the capabilities of the artificial intelligence systems used to:

assess the probability of obtaining correct machine learning results in the development of software;
ensuring the protection of the reputation of political figures from "fakes".

Keywords. model, risk, system, efficiency.

[77] Andrey I. Kostogryzov, Dr.Sc., Professor, Chief Researcher, Federal Research Center "Informatics and Control" of the Russian Academy of Sciences. Moscow, Russia. E-mail: Akostogr@gmail.com

УДК 004.056.53

Предложение подхода к переходу на модель разграничения доступа на основе атрибутов в информационной системе SAP

Лемешко Д.В.[78], Басараб М.А.[79]

Аннотация. *В данной статье рассматривается алгоритм генерации транзакций, программ для фонового выполнения заданий, таблиц, полномочий в информационной системе SAP, а также рассмотрено управление предоставлением доступов, разграничение доступов и логические уровни хранилища данных. В SAP реализована модель разграничения доступа на основе ролей (Role-based Access Control). В виду того, что на основе RBAC модель кажется громоздкой, выдвинуто предложение о возможной реализации модели разграничения доступа на основе атрибутов (Attribute-based Access Control) в информационной системе SAP.*

Ключевые слова: *управление доступом, разграничение доступа, SAP, информационная безопасность, авторизация, аутентификация, RBAC, ABAC.*

Введение

Разграничение доступа представляет собой разрешение или отказ в осуществлении операции с ресурсом. Основной целью разграничения доступа является предотвращение несанкционированного доступа к информации или использование информационных ресурсов на основе бизнес-требований и требований безопасности, т.е. применение политик доступа к конкретным запросам [1].

Управление доступом - совокупность процессов разграничения доступа для ряда ресурсов [1]. Управление доступом в качестве механизма защищает системы и информационные ресурсы от несанкционированного доступа и принимает участие в определении уровня авторизации после успешного прохождения процедуры аутентификации.

Для того чтобы предоставить надлежащий доступ легальному пользователю к нужному информационному ресурсу, необходимо, чтобы правильно были присвоены и согласованы роли/полномочия, а затем, при авторизации, пользователь получил доступ к нужному информационному ресурсу [2-6].

Вопросы, связанные с управлением доступа, разграничением доступа, авторизацией и использованием моделей разграничения доступа – крайне важны для грамотного распределения потоков операций и получения доступа к нужным транзакциям в SAP ERP.

1. Создание транзакций

При создании новой транзакции необходимо учитывать следующие принципы:

- название, код транзакции и программы;
- логика работы программы с привязкой к источнику данных;
- структура и назначение создаваемых таблиц/ракурсов;
- активные элементы и экраны;
- проверка полномочий в программе;
- новые объекты полномочий с указанием полей и их возможных значений;
- порядок ведения (полномочия у пользователей на изменение/просмотр, группы пользователей);
- указание ролей, которые будут наделены новой транзакцией.

Пример создания транзакции:

[78] Лемешко Диана Витальевна, студент, МГТУ им. Н.Э. Баумана, Москва, lemeshkodiana@yandex.ru
[79] Басараб Михаил Алексеевич, д.ф.-м.н., профессор, МГТУ им. Н.Э. Баумана, Москва, basarab@bmstu.ru

1) создать транзакцию ZINTK932 (программу ZINMM_SUZ_USLUNIT) «АСУЗ: Справочник этапов/подэтапов» для ведения справочника этапов/подэтапов. Впоследствии будут срабатывать стандартные проверки полномочий S_TABU_NAM.

Проверка полномочий в режиме просмотра:

```
AUTHORITY-CHECK OBJECT 'S_TABU_NAM'
   ID 'ACTVT' FIELD '03'
   ID 'TABLE' FIELD 'ZTIN_SUZ_USLSTAG'
```

Проверка полномочий в режиме изменения:

```
AUTHORITY-CHECK OBJECT 'S_TABU_NAM'
   ID 'ACTVT' FIELD '02'
   ID 'TABLE' FIELD 'ZTIN_SUZ_USLSTAG'
```

2) создать таблицу «Справочник этапов/подэтапов» ZTIN_SUZ_USLSTAG

Таблица 1.

Справочник этапов/подэтапов

№	Техническое имя поля	Наименование поля	Параметры
1.	OPR_USL_STAGE_ID	ID этапа/подэтапа	CHAR 12, генерация порядкового номера записи
2.	OPR_USL_STAGE	Наименование этапа/подэтапа	CHAR 255, текстовое поле, заполняется вручную

3) создать ракурс ведения таблицы ZTIN_SUZ_USLSTAG - «Справочник этапов/подэтапов».

4) создать одиночную роль ZSGPN_SUZ_0303010_MM_0130_NO_M – «АСУЗ: Ведение справочника расценок».

Таблица 2.

Реализация полномочий

№	Объект полномочий	Наименование объекта полномочий	Поле полномочий	Наименование поля полномочий	Значение поля полномочий
1.	S_TABU_NAM	Доступ к таблицам через стандартные инструменты	ACTVT	Операция	02, 03
			TABLE	Таблица	ZTIN_SUZ_USLSTAG
2.	S_TCODE	Проверка на код транзакции при запуске	TCD	Код транзакции	ZINTK932

5) создать групповую роль ZGGPN_SUZ_GPN038R_MM_TABERATE_N «АСУЗ: Ведение справочника расценок» на основе одиночной роли ZSGPN_SUZ_0303010_MM_0130_NO_M.

2. Создание программ для фонового выполнения

При создании программ для фонового выполнения должно быть указано следующее:

- логика работы программы с источником данных;
- проверка полномочий;
- группа полномочий, которая будет присвоена программе;
- наименование фонового пользователя, от имени которого будет выполняться фоновое задание;
- роли, которые будут присвоены фоновому пользователю;
- периодичность и время запуска программы.

Пример создания программы для фонового выполнения:

В системе SAP имеется программа ZLPDELIVERY_BITM, которая в фоновом режиме будет передавать данные о проверенных и заблокированных поставках в системе через асинхронный интерфейс ABAP Proxy.

Выборка данных для выгрузки поставок вида ZLJM будет осуществляться из таблиц:

- LISP (дата отгрузки);
- LIKS (код продукта, наименование продукта, количество);
- ZLPWAGON (№ вагона, № накладной, паспорт качества, тарифы);
- ZLPAUTO (№ автомобиля, Ф.И.О. водителя, № прицепа, № доверенности).

При запуске программы ZNPDELIVERY_BITM выполняется проверка на объекты полномочий:

- S_TABU_NAM по коду операции «03» и таблицы ZLPWAGON, ZLPAUTO;
- V_LIKP_VST по пункту отгрузки «0001» и коду операции «03».

Программа будет запускаться раз в сутки под техническим пользователем HPOERPBMSDL.

Пользователю будет присвоена роль:

ZGERP_SDP_1000213_SD_LOADOTR_N – передача данных, которая включает в себя одиночную роль: ZSERP_SDP_1000213_SD_0001_NO_M.

Таблица 3.

Добавление значений в одиночную роль

Объект полномочий	Поле	Значение
S_XMB_AUTH	ACTVT	16
	SXMBAREA	RUNTIME
S_TABU_NAM	ACTVT	02, 03
	TABLE	ZLPWAGON, ZLPAUTO
S_PROGRAM	P_ACTION	BTCSUBMIT
	P_GROUP	ZLNP

3. Создание таблиц

При создании таблиц должно быть указано следующее:

- описание проверок полномочий для доступа к таблице;
- группа полномочий, которая будет присвоена таблице;
- порядок ведения (присвоить код транзакции для вызова и указать группу пользователей);
- логика работы программ/пользователей с таблицей;
- состав полей и mapping.

Пример создания таблицы:

1) для хранения данных по списку поставщиков, была разработана новая таблица «ZTIJ_LF_APR_LST – список поставщиков». Данная таблица будет использоваться при работе с транзакцией ZINJL011.

Таблица 4.

Поля для таблицы ZTIJ_LF_APR_LST

№	Ключ	Наименование поля	Техническое имя поля
1.	X	Закупочная организация	EKORG
2.		Наименование закупочной организации	EKOTX
3.		Поставщик	LIFNR
4.		Наименование поставщика	NAME
5.		Действие с	DATE_START
6.		Действие по	DATE_END

2) для справочника поставщиков была создана таблица ZTIJ_LIF с ракурсом ведения ZVIJ_LIF.

Таблица 5.

Поля для таблицы ZTIJ_LIF

№	Ключ	Наименование поля	Техническое имя поля
1.	X	Закупочная организация	EKORG
2.		Наименование закупочной организации	EKOTX
3.		Поставщик	LIFNR
4.		Наименование поставщика	NAME
5.		Действие с	DATE_START
6.		Действие по	DATE_END
7.		Статус	STAT
8.		Дата создания	DATE_CRT
9.		Время создания	TIME_CRT

4. Логические уровни хранилища данных, соответствующие слоям референсной архитектуры LSA++

Хранилище данных, реализованное на базе SAP BW on HANA, разделяется на логические уровни, которые соответствуют слоям референсной архитектуры LSA++ [2].

Таблица 6.

Уровни хранилища данных и слои SAP LSA++

Уровень хранилища	Слой SAP LSA++	Назначение	Обязательное использование	Использование в целях аналитики	Типы объектов SAP BW для реализации модели данных
Уровень извлечения данных и корпоративная память	Open Operational Data Store Layer	Хранение данных, загруженных в SAP BW из систем-источников в исходном виде. Доступ в реальном времени к данным систем-источников.	X	X	aDSO, Open ODS View
Уровень предоставления данных	Propagation Layer	Обеспечение качества, гармонизация, консолидация.		X	aDSO, Composite Provider, Open ODS View
Уровень бизнес-трансформаций	Business Transformation Layer	Преобразование данных в соответствии с бизнес-правилами. Расчёт данных для сложных информационных витрин.		X	aDSO, Composite Provider, Open ODS View
Уровень инфо-витрин	Virtual Data Mart Layer	Виртуальные информационные витрины для отчётности или передачи данных.	X	X	Composite Provider

5. Создание ролей

При создании новой роли необходимо учитывать следующие принципы:

- указание соответствия технических ролей в системе;
- все объекты полномочий должны быть указаны со всеми полями и значениями;
- выполняемые операции из объектов полномочий в ролях должны соответствовать функциональности бизнес-роли.

Пример создания роли:

Для работы с транзакцией «ZAFE_PS - Создание фонда» необходимо создать роль. Создаётся шаблонная роль «ZTGPN_SBU_1305006_PS_0003_NO_M - Ведение фондов».

Таблица 7.

Объекты полномочий шаблонной роли

Объект	Поле	Значение
S_TCODE	TCD	ZAFE_PS
F_FICA_FOG	FM_AUTHACT	3
C_TCLA_BKA	KLART	41,42,43
F_FICA_FOG	FM_AUTHACT	1
F_FICA_FOG	FM_AUTHGRF	$FM_AUTHGRF
F_FICA_FOG	FM_FIKRS	$FIKRS
F_FICB_FKR	FM_AUTHACT	1,2,3,9,10
F_FICB_FKR	FM_FIKRS	$FIKRS
S_ALV_LAYO	ACTVT	23
S_GUI	ACTVT	60,61

На основе шаблонной роли создаётся одиночная: «ZOGPN_SBU_1000100_PS_0001_NO_M - Ведение фондов».

Таблица 8.

Организационные уровни одиночной роли

Организационный уровень	Описание	Значение
$BUKRS	БЕ	1000
$FIKRS	Единица финансового менеджмента	GPNF
$FM_AUTHGRF	Группа полномочий	*

6. Предложение о возможной реализации модели разграничения доступа на основе атрибутов в SAP

ABAC повышает эффективность управления доступом, устраняя необходимость в нескольких, независимых, специфичных для конкретной системы процессах управления доступом. ABAC заменяет их интегрированным, общеорганизационным процессом управления атрибутами и политиками [7]. Управляемые атрибуты и политика ABAC используются в нескольких системах. Такая централизация управления доступом помогает обеспечить согласованный контроль доступа между предприятиями на основе атрибутов, связанных с бизнесом. Это позволяет упростить доступ к ресурсам как предоставляемый, так и отзываемый своевременно, обеспечивая доступ к информации.

Таблица 9.

Функциональные характеристики ABAC

Функциональные характеристики	**Примеры возможностей**
Аутентификация	1) требование поддержки многофакторной аутентификации для достижения степени достоверности аутентификации с использованием комбинации факторов; 2) поддержка строгой аутентификации между проверяющей стороной и поставщиками атрибутов.
Применение политики и решений, основанных на атрибутах	1) принятие и применение решения по управлению доступом на основе политики, определённой атрибутами.
Управление жизненным циклом атрибутов	1) предоставление, модификация и отмена предоставления атрибутов.
Объединение атрибутов	1) передача значений атрибутов между проверяющими сторонами и поставщиками атрибутов.
Объединение удостоверений	1) проверяющая сторона может принять токен аутентификации от поставщика удостоверений на основе предварительного установления доверительных отношений.

Таблица 10.

Характеристики безопасности

Характеристики безопасности	**Примеры возможностей**
Конфиденциальность	Защита: 1) передачи идентификационных данных и атрибутов между предприятиями и через платформу обмена атрибутами; 2) данных для всех хранилищ атрибутов и политик 3) значений атрибутов, используемых в логике принятия решений.
Защита конфиденциальности	1) маскировка проверяющей стороны от поставщика удостоверений в любой заданной транзакции; 2) меры предосторожности, предотвращающие отслеживание поведения субъекта; 3) не позволяет злоумышленникам сопоставлять сообщения или определять, что в двух сеансах аутентификации участвовал один и тот же субъект; 4) поддерживает минимизацию и скрытие данных, позволяя утверждать атрибуты, не выдавая больше, чем требуется.

Выводы

В результате работы рассмотрен алгоритм генерации транзакций, программ для фонового выполнения заданий, таблиц, полномочий в ИС SAP, а также рассмотрено управление предоставлением доступов, разграничение доступов и логические уровни хранилища данных. Предложен подход перехода на модель разграничения доступа на основе атрибутов (ABAC) в ИС SAP. Предложенный подход целесообразно использовать в управлении доступами и разграничении доступов в ИС SAP.

Литература

1. ГОСТ Р 59383–2021 Информационные технологии. Методы и средства обеспечения безопасности. Основы управления доступом.

2. Regys Mene, Hartmut Westenberger, Hrvoje Husic. Reference Models for the Standardization and Automation of Data Warehouse Architecture including SAP Solutions; 2018.

3. Gairik Acharya, Govind Bajaj, Avijit Dhar, Anup Ghosh, Asidhara Lahiri. Application Development with SAP Business Technology Platform; 2023. pp. 574.

4. Andrea Cavalleri, Massimo Manara. Authorizations in SAP; 2012. pp. 346.

5. Marie-Luise Wagener. Introducing Governance, Risk, and Compliance (GRC) in SAP S/4HANA. pp. 132.

6. Asokkumar Christian, D. Rajen Iyer, Atul Sudhalkar. Implementing SAP Governance, Risk, and Compliance; 2014. pp. 712.

7. NIST Special Publication 800-162: Guide to Attribute Based Access Control (ABAC) Definition and Considerations.

8. NIST Special Publication 800-63-3: Digital Identity Guidelines.

9. NIST Special Publication 800-63B: Digital Identity Guidelines. Authentication and Lifecycle Management.

10. NIST Special Publication 800-63C: Digital Identity Guidelines. Federation and Assertions.

Suggestion of a transition approach on attribute-based access control model in SAP information system

Lemeshko D.V.[80], Basarab M.A.[81]

Abstract. *This article discusses the algorithm of generating transactions, programs for background execution of tasks, tables, permissions in SAP information system, as well as the access management, access control and logical levels of data storage. SAP has Role-based Access Control model. In view of the fact that the RBAC model seems cumbersome, a proposal has been put forward on the possible implementation of an Attribute-based access control model in SAP information system.*

Ключевые слова: *access management, access control, SAP, information security, authorization, authentication, RBAC, ABAC.*

[80] Diana V. Lemeshko, student, Bauman Moscow State Technical University, Moscow, lemeshkodiana@yandex.ru
[81] Mikhail A. Basarab, Grand PhD in Physics and Mathematics, Bauman Moscow State Technical University, basarab@bmstu.ru

УДК 004.056

Концептуальный подход к разработке сценариев компьютерных атак

Марков Г.А.[82]

В докладе рассмотрено понятие сценариев атак. Дана классификация сценариев атак. Приведены этапы подготовки сценариев атак.

Ключевые слова: компьютерная атака, сценарии атак, этапы разработки сценария.

Введение

Сценарии атак можно использовать как методический инструмент для анализа угроз, уязвимостей, атак и их последствий [1-6]. Данный инструмент важен для каждой организации, потому что важно знать какие события могут привести к критичным ситуациям для организации. Следует отметить преимущества от использования сценариев атак, а именно: защита на опережение; понимание рисков; развитие уровня информационной безопасности (приоритеты по угрозам и контрмерам); обучение. Целевое назначение разработки сценариев атак включает понимание и устранение угроз, выявление и устранение уязвимостей, разработка эффективной стратегии по защите, своевременное выявление и реагирование на атаки/инциденты, минимизацию ущерба.

Процесс разработки сценариев атак

Согласно NIST под *сценарием кибератаки* обычно понимают набор дискретных событий атаки, связанных с конкретным источником атаки или несколькими источниками атаки, частично упорядоченных во времени[83]. Однако на практике при исследовании сценариев атак основное внимание акцентируют на недопустимые события, грозящие организации. Учитывая важность анализа недопустимых событий, рассмотрим основные шаги и принципы, используемые при разработке сценариев атаки (рис. 1).

Рис1. Шаги разработки сценариев атак

1. Идентификация активов и уязвимостей. Первым шагом в разработке сценариев атак является определение активов (ресурсы, процессы), которые нужно защитить. Далее нужно выявить уязвимости и слабые места в этих активах, которые могут быть использованы злоумышленниками для несанкционированного доступа или нарушения работы систем.

---

[82] Марков Георгий Алексеевич, Москва, Инфосистемы Джет, detonate1@yandex.ru

[83] https://csrc.nist.gov/glossary/term/threat_scenario

2. Определение угроз и потенциальных атак. На основе полученной информации по уязвимостям необходимо определить потенциальные угрозы и типы атак, которые могут быть использованы. Анализ угроз, как известно, имеет множество методик и даже регламентировано рядом руководств. Можно также разбить процедуру на этапы: определение целей информационной безопасности компании, оценка и идентификация активов компании, анализ источников проблем, оценка и управление рисками, принятие мер, в зависимости от предыдущих шагов, по обеспечении безопасности компании, составление отчета по результатам анализа рисков, включающем проблемные области, ущерб от реализации угроз, деятельность по улучшению процессов информационной безопасности связанную с имеемыми рисками. В рамках оценки риска также можно составить модель нарушителя модель угроз (главным образом для понимания мотивации и целей нарушителя). В модели угроз можно рассмотреть взаимосвязь идентифицированных активов и расчет найденных и проанализированных рисков.

3. Обучение персонала. На данном этапе определяются роли участников процесса, кто за что отвечает, проверяются наличии необходимых доступов и прав. Также рассматриваются правила оповещения ответственных лиц. Полезным также будет регламентное описание фиксации инцидента, для удобной передачи информации в едином виде, а также инструментарий, который может быть использован. Для автоматизации данного процесса можно использовать СЗИ, помогающие обрабатывать и реагировать на инциденты.

4. Разработка собственно сценариев атак. На этом этапе создаются конкретные сценарии атак, которые будут описывать имитацию реальных угроз векторов атак. Сценарии должны быть реалистичными и основываться на актуальных угрозах, с которыми может столкнуться организация. Сценарии можно представить в виде последовательности действий, либо событий, предпринятых злоумышленниками для реализации целей. Нужно учитывать, что атакующие скорей всего тоже имеют свои планы по проведению вредоносной деятельности. Рассмотрев ситуацию со стороны злоумышленника, можно улучшить свои сценарии с упором на защиту каждого этапа продвижения атаки, а также “удлинить” цепочку, по которой пойдет предполагаемый атакующий для реализации вредоносной активности.

5. Тестирование сценариев атак. После разработки сценариев атак необходимо провести тестирование, чтобы оценить эффективность защиты системы. Для базовых проверок могут быть также разработаны сценарии по реагированию в виде списка рекомендуемых действий при возникновении определенного типа события информационной безопасности. Тестирование (фактически, это тестирование на проникновение) может быть выполнено внутри организации или с помощью привлечения сторонних компаний, которые будут действовать от имени злоумышленников.

6. Оценка результатов и улучшение безопасности. Последним этапом можно считать оценку результатов тестирования и выявление слабых мест в защите системы. На основе этих результатов можно принимать меры по улучшению безопасности, внедрять дополнительные меры защиты и проводить обучение. Также стоит уделить вниманию проверке и улучшению процесса тестирования сценариев атак, если в ходе были выявлены недочеты. Для этого желательно задействовать участников работ различных направлений для более объективной оценки.

Будущее сценариев атак

Рассмотрим некоторые перспективные моменты развития области сценариев атак.

1. Развитие технологий искусственного интеллекта. С развитием искусственного интеллекта злоумышленники смогут генерировать более сложные вариации сценариев атак.

2. Угрозы для интернет вещей (IoT). Такие сценарии атак будут включать атаки на уязвимые устройства IoT, например использование их в качестве ботнетов для DDoS-атак, утечки данных через IoT , хранящихся на этих устройствах.

3. Угрозы в облачных вычислениях. В будущем сценарии атак будут включать атаки на облачные инфраструктуры, уклонение защиты с использованием облачных сервисов и утечку конфиденциальных данных, хранимых в облаке.

4. Социальная инженерия и влияние на общественное мнение.

5. Удаленная работа. После роста сотрудников, перешедших на удаленную работу, увеличились риски атак через конечные станции удаленных сотрудников.

С учетом вышеперечисленных тенденций, будущее сценариев атак будет связано с более сложными, интеллектуальными и автоматизированными методами атак

Заключение

В заключении, необходимо подчеркнуть, что разработка и использование сценариев атак должно стать неотъемлемой частью стратегии кибербезопасности каждой организации. Только путем постоянного тестирования и улучшения безопасности можно обеспечить надежную защиту информации и минимизировать риски от киберугроз. Постоянное обучение персонала и внедрение передовых методов защиты помогут организациям оставаться впереди в непрекращающейся борьбе с киберпреступниками и обеспечивать надежную безопасность своих данных и ресурсов.

Литература

1. Бирюков Д.Н., Ломако А.Г., Петренко С.А. Порождение сценариев предупреждения компьютерных атак // Защита информации. Инсайд. 2017. № 4 (76). С. 70–79.

2. Иванова Н.Д. Моделирование сценариев кибератак на интеллектуальную транспортную систему с использованием матричных моделей оценивания рисков. В сборнике: Интеллектуальные транспортные системы. Материалы II Международной научно-практической конференции. Москва, 2023. С. 461–469.

3. Кибербезопасность цифровой индустрии. Теория и практика функциональной устойчивости к кибератакам / Под ред. Зегжда Д.П. и др. М.: Горячая линия, 2021. 560 с.

4. Кондаков С.Е., Рудь И.С. Модель процесса проведения компьютерных атак с использованием специальных информационных воздействий // Вопросы кибербезопасности. 2021. № 5 (45). С. 12–20.

5. Павленко Е.Ю. Исследование влияния атак на структурные и параметрические метрики сетей с адаптивной топологией // Вопросы кибербезопасности. 2023. № 4 (56). С. 65–71.

6. Савин М.В., Стойчин К.Л., Некрасов А.В., Комаров Н.В. Обзор стандартов и форматов представления автоматизированных сценариев реагирования на инциденты компьютерной безопасности // Защита информации. Инсайд. 2022. № 4 (106). С. 14–19.

7. Хлобыстова А.О., Тулупьев А.Л. Подходы к моделированию сценариев развития многоходовых социоинженерных атак. Международная научная конференция по проблемам управления в технических системах. 2021. Т. 1. С. 134–137.

Conceptual approach to the development of computer attack scenarios

Markov G.A.[84]

The paper considers the concept of attack scenarios. Classification of attack scenarios is given. Stages of preparation of attack scenarios are given.

Keywords: computer attack, attack scenarios, stages of scenario development.

[84] Markov Georgy Alekseevich, Moscow, Jet Infosystems, detonate1@yandex.ru

УДК 004.056

Концептуальные вопросы защиты информации безопасного города

Маркова Е.Д.[85]

Представлен обзор концепции безопасного города. Отмечена актуальность обеспечения информационной безопасности активов безопасного города. Обоснована необходимость организации ситуационных центров и центров мониторинга информационной безопасности. Представлен обзор средств и механизмов защиты ситуационных центров. Сделан вывод о центральной роли SIEM-систем. Даны рекомендации по выбору SIEM-систем.

Ключевые слова: безопасный город, центр мониторинга, мониторинг событий

Введение

Безопасный город — это концепция, направленная на создание безопасной и устойчивой городской среды для жителей и посетителей [1]. Она включает в себя различные аспекты безопасности, такие как общественная безопасность, предотвращение преступности, обеспечение чрезвычайной ситуационной готовности и эффективного управления кризисными ситуациями [2].

Ситуационные центры (далее - СЦ) — это центры управления и контроля, которые объединяют информацию о безопасности и ситуационную осведомленность из различных источников. Они предоставляют операторам возможность мониторинга, анализа и реагирования на события в реальном времени. Они собирают и обрабатывают информацию о различных аспектах общественной жизни, включая экономику, экологию, транспорт, техногенные и природные катастрофы, террористические угрозы, конфликты и международную ситуацию.

Значимость ситуационных центров обусловлена несколькими факторами [3, 4]:

Во-первых, они способствуют своевременному обнаружению и реагированию на различные угрозы и кризисные ситуации, что позволяет предотвратить или минимизировать их негативные последствия.

Во-вторых, они способствуют улучшению управления и координации действий различных структур в условиях кризиса, что повышает эффективность реагирования и спасает жизни людей.

В-третьих, ситуационные центры обеспечивают оперативную информацию для принятия стратегических решений, способствуя развитию страны и обеспечению ее безопасности.

Мониторинг событий безопасности

SIEM-системы (системы управления информационной безопасностью и событиями) представляют собой инструменты, используемые для сбора, анализа и управления информацией о безопасности в компьютерных системах и сетях. Они позволяют обнаруживать и реагировать на угрозы безопасности, а также осуществлять мониторинг и анализ безопасности данных. Угрозы кибербезопасности становятся все более сложными, изощренными, вредоносными, хорошо организованными и хорошо финансируемыми. Широкое внедрение инструментов и технологий на основе искусственного интеллекта

[85] Марков Елена Дмитриевна, Аппарат Совета Федерации Федерального Собрания Российской Федерации, manlendmi@yandex.ru

приведет к персонализированным и высокоэффективным кибератакам. Чтобы справиться со сложностью выявления таких атак, требуется ситуационный центр управления безопасностью (Security Operations Center (далее – SOC) [5-8].

SOC имеет решающее значение для всех типов и размеров организаций в современной цифровой экономике, поскольку большая часть операций организации и конфиденциальных данных находится в сети и в облаке. Для борьбы с киберпреступниками необходим современный подход к операциям SOC.

Аналитические агентства и своды лучших практик в определениях SOC годами сходились в одном: SOC — это совокупность специалистов, процессов и технологий, направленных на эффективные мониторинг (выявление) и реагирование на инциденты в информационной безопасности со стороны как внешних, так и внутренних нарушителей.[86]

SIEM-системы позволяют собирать, агрегировать и анализировать разнообразные данные о безопасности, включая данные с камер видеонаблюдения, сенсоров, социальных медиа и других источников.

Российский рынок SIEM-систем продолжает развиваться, наблюдается снижение доли иностранных SIEM на отечественном рынке. Это связано в основном с политикой импортозамещения. Указом Президента РФ №250[87] установлено, что с 1 января 2025 г. органам (организациям) запрещается использовать средства защиты информации, странами происхождения которых являются иностранные государства, совершающие в отношении Российской Федерации, российских юридических лиц и физических лиц недружественные действия, либо производителями которых являются организации, находящиеся под юрисдикцией таких иностранных государств, прямо или косвенно подконтрольные им либо аффилированные с ними.

На данный момент на российском рынке представлены в основном отечественные продукты. В этой статье будут рассмотрены такие SIEM-системы, как KOMRAD Enterprise SIEM (НПО «Эшелон»); Kaspersky Unified Monitoring and Analysis Platform («Лаборатория Касперского»); RuSIEM (ООО «РуСИЕМ»).

Таблица 1.

Передовые российсике SIEM

Компания-разработчик	**KOMRAD Enterprise SIEM**	**KUMA**	**RUSIEM**
	НПО «Эшелон»	«Лаборатория Касперского»	ООО «РуСИЕМ»
Возможности:	Высокая производительность при минимальных требованиях к аппаратному обеспечению. Возможность распределённой установки и масштабирования. Широкий спектр поддерживаемых источников событий	Kaspersky Unified Monitoring and Analysis Platform объединяет продукты «Лаборатории Касперского» и сторонних поставщиков в единую систему ИБ. Масштабируемая архитектура и низкие системные требования. Высокопроизводительный	Высокая производительность. Нет ограничений по количеству событий и источникам. Вертикальная Масштабируемость. Горизонтальная Масштабируемость.

[86] https://www.anti-malware.ru/analytics/Market_Analysis/Security-Operations-Center-2022

[87] Указ Президента РФ от 01.05.2022 N 250 "О дополнительных мерах по обеспечению информационной безопасности Российской Федерации". Официальный интернет-портал правовой информации http://pravo.gov.ru, 01.05.2022, "Собрание законодательства РФ", 02.05.2022, N 18, ст. 3058, "Российская газета", N 95, 04.05.2022

	«из коробки». Интеграция со всеми отечественными средствами защиты информации. Визуальный графический интерфейс для создания фильтров и правил корреляции; управление инцидентами. Дистрибутив под Astra Linux и Windows. Обучение специалистов на базе собственного учебного центра.	потоковый движок корреляции обеспечивает производительность более 300 тысяч событий в секунду (EPS) на один узел корреляции. Потоковая корреляция в реальном времени. Автоматический сбор информации о конечных точках и реагирование.	Разделение нагрузки на несколько серверов или виртуальных машин. Наличие собственных модульных агентов. Real-time и историческая корреляция Коннекторы от производителя. Нет ограничений по размеру архивного хранилища. Сохранение RAW-событий.
Возможность передачи инцидентов в систему ГосСОПКА	+	+	+
Сертификаты	ФСТЭК России №3498 Минобороны России №6498	ФСТЭК России № 4455.	ФСТЭК России № 4402
Включение в единый реестр российских программ для электронных вычислительных машин и баз данных	+	+	+

СЦ, являясь центральными точками координации и анализа данных о безопасности города, получают значительные выгоды от внедрения SIEM-систем. SIEM-системы позволяют собирать, агрегировать и анализировать разнообразные данные о безопасности, включая данные с камер видеонаблюдения, сенсоров, социальных медиа и других источников.

Заключение

Использование SIEM-систем в СЦ способствует более эффективному обнаружению и анализу потенциальных угроз, таких как террористические акты, преступления, чрезвычайные ситуации и другие нарушения общественной безопасности. Автоматическая обработка и анализ данных позволяют операторам ситуационных центров получать оперативную информацию о происходящих событиях и быстро принимать меры по их предотвращению или реагированию.

Кроме того, SIEM-системы позволяют более эффективно управлять и анализировать большие объемы данных, обнаруживать скрытые корреляции и тренды, а также прогнозировать возможные угрозы и риски.

Безусловно, следует отметить, что успешная реализация применения SIEM-систем требует не только технических аспектов, но и человеческих ресурсов. Внедрение и эффективное использование SIEM-систем требует квалифицированных специалистов, обученных в области информационной безопасности.

Важно отметить, что успешное внедрение и использование SIEM-систем в ситуационных центрах требует сотрудничества и партнерства между государственными органами, коммерческими организациями и общественностью. Обмен информацией и ресурсами способствует более широкому обзору безопасности города и повышает эффективность действий в случае возникновения угроз.

Литература

1. Hessel R. Safe City: From Law Enforcement to Neighborhood Watches by. Morgan James Publishing, 2018, 139 p.

2. Булгакова Е.В., Сазонов С.М. Правовой режим информации в АИС "Безопасный город" и меры по ее защите // Правовая информатика. 2013. № 2. С. 62–71.

3. Дорофеев А.В., Марков А.С. Применение отечественных технологий для мониторинга информационной безопасности в условиях импортозамещения // Защита информации. Инсайд. 2023. № 3 (111). С. 20–26.

4. Кибербезопасность цифровой индустрии. Теория и практика функциональной устойчивости к кибератакам / Под. ред. Д. П. Зегжды. - М.: Горячая линия - Телеком. - 2021. - 560 с.

5. Кузнецов А.В., Ненашев С.М. Способ определения регистрируемых событий // Вопросы кибербезопасности. 2015. № 5 (13). С. 23–25.

6. Петренко А. С., Петренко С. А. Проектирование корпоративного сегмента СОПКА // Защита информации. Инсайд. - 2016. - № 6 (72). - С. 28–30.

7. Рыболовлев Д.А., Карасёв С.В., Поляков С.А. Классификация современных систем управления инцидентами безопасности // Вопросы кибербезопасности. 2018. № 3 (27). С. 47–53.

8. Kaliyaperumal L.N. The Evolution of Security Operations and Strategies for Building an Effective SOC. ISACA Journal, 2021, vol. 5, p. 1.

Conceptual issues of safe city information protection.

Markova E.D.[88]

An overview of the concept of a safe city is presented. The relevance of information security of safe city assets is noted. The necessity of organization of situation centers and information security monitoring centers is substantiated. The review of means and mechanisms of situation centers protection is presented. The conclusion about the central role of SIEM-systems is made. Recommendations on the choice of SIEM-systems are given.

Keywords: safe city, monitoring center, event monitoring

[88] Elena D. Markova, Office of the Federation Council of the Federal Assembly of the Russian Federation, manlendmi@yandex.ru

УДК 004.056

Организационно-технические меры информационной безопасности цифровой валюты центрального банка

А. В. Олифиров[89], **К. А. Маковейчук**[90]

Аннотация. В статье предложен методический подход для определения мер реагирования на риски информационной безопасности цифровой валюты центрального банка. Определена структура организационно-технических мер обеспечения безопасности этой валюты. Предложена модель выбора мер безопасности в условиях минимизации остаточного риска, которая позволяет повысить общий уровень защищенности от информационных рисков. Разработана концепция системы управления информационной безопасностью на основе методологии CobiT 5.0, которая позволяет комплексно охватить планирование, разработку, приобретение, внедрение, эксплуатацию, мониторинг и оценку организационно-технических мер информационной безопасности.

Ключевые слова: CobiT, риск, модель, организационно-технические меры, методология, система, планирование, разработка, эксплуатация, мониторинг, критерии.

Введение. В современных условиях внешних вызовов, санкций, развития финансовых технологий, криптовалют, глобальных финансовых рисков и угроз, роста международных конфликтов, обеспечение информационной безопасности становится все более актуальным [1-6]. Переход на цифровую валюту Центрального банка (ЦВЦБ) обеспечивает много преимуществ, но, вместе с тем, несет много угроз и рисков, которые необходимо контролировать и снижать. В связи с этим исследование, посвященное определению организационно-технических мер информационной безопасности цифровой валюты центрального банка, представляется актуальным.

Методология исследования. Система информационной безопасности в финансовой сфере постоянно подвержена изменениям, так как постоянно изменяются угрозы, уязвимости, риски, меры защиты во внутренней и внешней среде. В этом случае, для определения мер информационной безопасности необходима методология, которая учитывала бы эту динамику. В состав такой методологии, которая использована в данной работе, входят следующие методические подходы:

научное обобщение публикаций по информационной безопасности в финансовой сфере, что позволяет уточнить понятийный аппарат, систематизировать риски и меры защиты цифровой валюты центрального банка;

использование методологии CobiT – технологии управления информационными технологиями и бизнес-процессами в их взаимосвязи и развитии. Эта методология позволяет комплексно подойти к этапам планирования, разработки, приобретения, эксплуатации, мониторинга и регулирования мер и средств защиты в системе цифровой валюты центрального банка

применение экономико-математического моделирования для оптимизации рисков ИБ, как средство формализации решения задачи выбора мер ИБ.

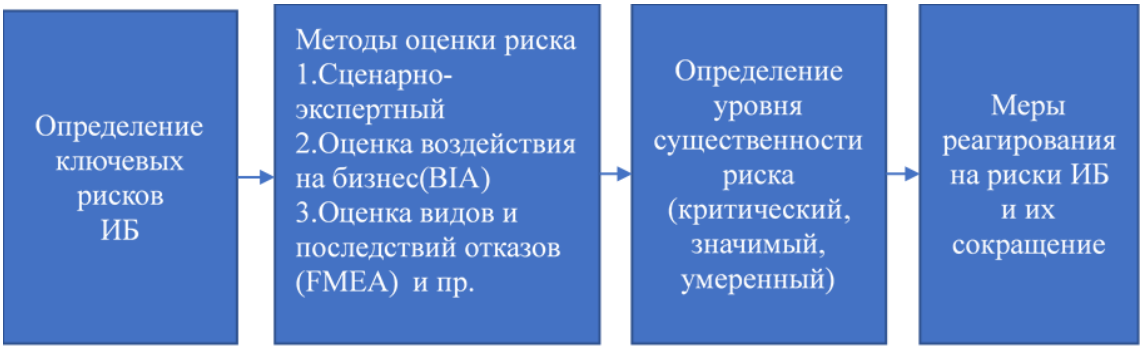
Цель исследования – разработать методологические и практические подходы к определению организационно-технических мер информационной безопасности ЦВЦБ, повысить общий уровень защищенности от информационных рисков в условиях перехода на цифровую валюту центрального банка.

[89] Олифиров Александр Васильевич, д-р экон. наук, профессор, ФГАОУ ВО «Крымский федеральный университет имени В. И. Вернадского», г. Ялта, alex.olifirov@gmail.com

[90] Маковейчук Кристина Александровна, канд. экон. наук, доцент, Финансовый университет при Правительстве Российской Федерации, г. Москва, christin2003@yandex.ru

Определение, оценка и меры реагирования на риски ИБ. В состав риска информационной безопасности (ИБ) входит риск преднамеренного воздействия персонала организаций, физических лиц направленного на несанкционированное получение, изменение, удаление данных и иной цифровой информации, с использованием цифровой инфраструктуры и технологий связи (киберриск), а также другие виды рисков, связанные с обработкой (получением, хранением, применением, уничтожением) информации. В этом контексте под рисками ИБ цифровой валюты центрального банка следует понимать любую вероятность наступления неблагоприятных последствий для Центрального банка, коммерческих банков, юридических и физических лиц, провайдеров финансовых услуг и для экономики в целом, связанную с применением цифровой валюты центрального банка при определенных обстоятельствах и в определенных ситуациях. Фиксация факта фактической реализация риска ИБ, происходит в базе событий (инцидентов) риска [7].

Схема определения, оценки и реагирования на риски информационной безопасности представлена на рисунке 1.



*Разработано авторами на основе [8]

Рис. 1. Схема этапов определения, оценки и реагирования на риски информационной безопасности

На определение ключевых рисков ИБ влияют угрозы – это факторы и условия функционирования, присущие процессам системы ИБ, которые создают реальную опасность нарушения конфиденциальности, целостности и доступности информации и данных. Также на ключевые риски ИБ оказывает влияние и уязвимость (как характеристика недостатков информационной инфраструктуры), которая обусловливает возможность реализации угроз защиты информации.

Методы оценки риска могут включать, наряду с представленными на рисунке 1, и другие подходы: оценку уровней защиты (LOPA), анализ дерева событий (ETA), оценку влияния человеческого фактора (HRA).

Классификация рисков по уровню существенности позволяет определять меры реагирования на них. Так риски критического уровня являются неприемлемыми для системы ЦВЦБ и подлежат приоритетному управлению. Риски значимого уровня не являются критичными, но оказывают существенное влияние на деятельность системы ЦВЦБ и подлежат управлению. Риски умеренного уровня не оказывают значительного влияния на систему ЦВЦБ, но подлежат периодическому мониторингу [8].

Структура организационно-технических мер обеспечения информационной безопасности цифровой валюты центрального банка. Исследование, систематизация организационно-технических мер обеспечения информационной безопасности позволили определить их структуру [9, 10].

К организационным мерам можно отнести политики и процедуры, которые включают: политики безопасности и обучение персонала; регулярное обновление криптографических ключей и паролей; процедуры реагирования на инциденты безопасности. К

организационным мерам также относится организация обмена информацией, уведомлениями об инцидентах, передовым опытом в сфере защиты информации. Необходимо принимать меры по повышению осведомленности общественности, сертификации и аккредитации профессионалов в области кибербезопасности, по проведению курсов профессиональной подготовки по кибербезопасности, по реализации образовательных программы или академических программ и т. д. Система ЦВЦБ ежегодно должна проводить тестирование на проникновение и анализ уязвимостей информационной безопасности объектов инфраструктуры.

Технические меры направлены на следующие объекты защиты: центральный сервер цифрой валюты, центральная база данных, физические и облачные хранилища данных, сети центрального банка, каналы связи с банками и государственными учреждениями. Также, под защитой будут находиться сведения о средствах на цифровых кошельках, о транзакциях с рублями, о доступе к платформе и закрытии счета, а также информация, необходимая для авторизации и идентификации пользователей.

Технические меры ИБ охватывают физическую инфраструктуру, архитектуру сети, шифрование и аутентификацию, мониторинг и анализ.

Модель выбора мер ИБ при минимизации риска и при ограничении затрат на реализацию мер защиты в детерминированной постановке. Выбрать оптимальный набор перечисленных мер ИБ, принять более обоснованное решение по управлению рисками позволяет экономико-математическое моделирование.

Рассмотрим экономико-математическую модель выбора мер защиты в условиях ограничения расходов на информационную безопасность [11].

Необходимо найти целочисленные переменные x_j, которые минимизируют функцию:

$$F = \sum_{i=1}^{m} VLR_i - \sum_{j=1}^{n} a_{ij} * x_j \to min, \quad (1)$$

при следующих ограничениях:

$$\sum_{j=1}^{n} c_j * x_j \leq s, \quad (2)$$

$$x_j \in \{0; 1\}, j = \overline{1, n}, \quad (3)$$

где x_j - целочисленная булева переменная, которая равна:

$$x_j = \begin{cases} 1, \text{если } j - \text{тая мера ИБ используется для противодействия угрозам;} \\ 0, \text{в противном случае;} \end{cases}$$

VLR_i – риск ИБ по $i-$той угрозе, присущий системе без использования мер ИБ, $i = \overline{1, m}$;

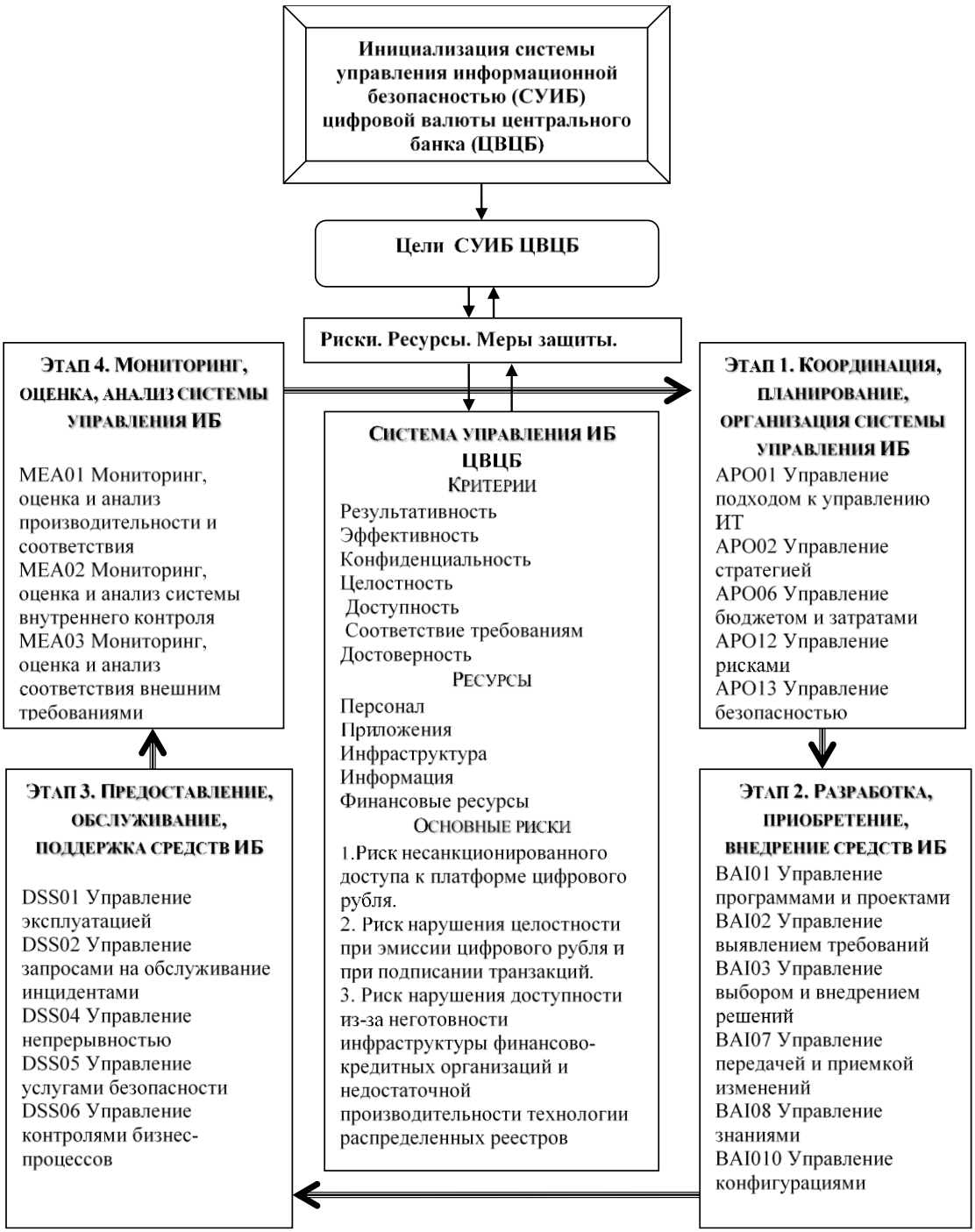
a_{ij} - риск, отведенный $j-$той контрмерой по $i-$той угрозе;

c_j – стоимость реализации $j-$той мере ИБ;

s – допустимый размер затрат на обеспечение мер ИБ.

Целевая функция (1) модели минимизирует остаточный риск ИБ в системе ЦВЦБ. Ограничение (2) связано с тем, что затраты на меры ИБ не могут превышать s. Ограничение (3) связано с тем, что модель является целочисленной, с булевыми переменными. В детерминированном варианте решение этой задачи легко реализуется методами линейного программирования.

Система управления информационной безопасностью цифровой валюты центрального банка. Ключевой риск при внедрении ЦВЦБ – это рост киберугроз, борьба с которыми основана на высоко детализированной стандартной методологии оценки риска. К этой методологии управления информационными технологиями относится методология CobiT [12]. Эта методология может использоваться для моделирования системы управления ИБ ЦВЦБ (рис. 2).



*Разработано авторами на основе https://www.isaca.org/resources/cobit/cobit-5 и [12]

Рис. 2. Система управления информационной безопасностью цифровой валюты центрального банка на основе методологии CobiT 5.0

Выводы. В результате проведенных исследований определены следующие основные результаты, которые позволили повысить общий уровень защищенности от информационных рисков в условиях перехода на цифровую валюту центрального банка.

1. Уточнен понятийный аппарат в части рисков и мер защиты в системе цифровой валюты центрального банка.

2. Предложена схема этапов определения, оценки и реагирования на риски информационной безопасности

3. Определена структура организационно-технических мер обеспечения информационной безопасности цифровой валюты центрального банка.

4. Построена модель выбора мер ИБ при минимизации риска и при ограничении затрат на реализацию мер защиты в детерминированной постановке.

5. Получила дальнейшее развитие система управления информационной безопасностью цифровой валюты центрального банка на основе методологии CobiT, что позволило комплексно охватить планирование, разработку, приобретение, внедрение, эксплуатацию, мониторинг и оценку мер информационной безопасности.

Литература

1. Астраханцев Р.Г., Лось А.Б., Мухамадиева Р.Ш. Анализ современных тенденций развития технологии "блокчейн" и цифровых валют // Вопросы кибербезопасности. 2019. № 5 (33). С. 57–62.

2. Масленников В.В., Ларионов А.В. Цифровые валюты: концептуализация рисков и возможности регулирования. // Мир новой экономики, 2021, 15(4). С. 16–28. DOI: 10.26794/2220-6469-2021-15-4-16-28

3. Масленников В. В., Ларионов А. В., Масленников С. В. Концептуальные подходы к разработке новой единой стратегии развития финансового рынка России. // Экономика. Налоги. Право, 2021, 14(3). С. 6–19. DOI: 10.26794/1999-849X-2021-14-3-6-1

4. Янковский Р. М. Криптовалюты в российском праве: суррогаты, «иное имущество» и цифровые деньги. Право. // Журнал Высшей школы экономики, 2020, (4). С. 43–77. DOI: 10.17323/2072-8166.2020.4.43.77

5. Agur I., Lavayssière X., Bauer G. V., Deodoro J., Peria S. M., Sandri D., Tourpe H. Lessons from crypto assets for the design of energy efficient digital currencies. Ecological Economics, 2023, Vol-212. DOI: 10.1016/j.ecolecon.2023.107888

6. Бауэр В.П., Смирнов В.В. Институциональные особенности разработки конкурентоспособной криптовалюты. // Финансы: теория и практика, 2020, 24(5). С. 84–99. DOI: 10.26794/2587-5671-2020-24-5-84-99

7. Gilbert S., Loi H. Digital Currency Risk. International Journal of Economics and Finance, 2018, Vol-10, 2. DOI: 10.5539/ijef.v10n2p108

8. Olifirov A.V., Makoveichuk K.A., Petrenko S.A. Integration of cyber security into the Smart Grid operational risk management system. In Selected Papers of the 4th All-Russian Scientific and Practical Conference with International Participation "Information Systems and Technologies in Modeling and Control" (ISTMC 2019). CEUR Workshop Proceedings, 2019, Vol-2522, pp. 132–144.

9. Olifirov A., Makoveichuk K., Petrenko S. Cybersecurity measures of the digital payment ecosystem. In Selected Papers of 11th International Scientific and Technical Conference on Secure Information Technologies (BIT 2021). CEUR Workshop Proceedings, 2021, Vol-3035, pp. 133–142.

10.Барабанов А.В., Дорофеев А.В., Марков А.С., Цирлов В.Л. Семь безопасных информационных технологий / Под. ред. А.С.Маркова. М.: ДМК Пресс, 2017. 224 с.

11.Олифиров А.В. Модели управления рисками экономических информационных систем. В сборнике: Информационные системы и технологии в моделировании и управлении. Материалы всероссийской научно-практической конференции, 2017. С. 465–470.

12.Olifirov A.V., Makoveichuk K.A., Zhytnyy P.Y., Filimonenkova T.N., Petrenko S.A. Models of processes for governance of enterprise it and personnel training for digital economy. In Proceedings of 2018 17th Russian Scientific and Practical Conference on Planning and Teaching Engineering Staff for the Industrial and Economic Complex of the Region (PTES 2018). Institute of Electrical and Electronics Engineers Inc, 2019, pp. 216-219. DOI: 10.1109/PTES.2018.8604166.

Organisational and Technical Measures to Ensure Information Security of the Central Bank Digital Currency

Olifirov A. V.[91] **, Makovejchuk K. A.** [92]

Abstract. The article proposes a methodical approach to determine the measures of response to the risks of information security of a central bank digital currency. The structure of organizational and technical measures to ensure the security of this currency is defined. The model of selecting security measures under the conditions of residual risk minimization is proposed, which allows increasing the overall level of security against information risks. The concept of the information security management system based on the methodology of Cobit 5.0 was developed, which allows to comprehensively cover the planning, development, acquisition, implementation, operation, monitoring and evaluation of organizational and technical measures of information security.

Keywords: CoBIT, risk, model, organizational and technical measures, methodology, system, planning, development, operation, monitoring, criteria.

[91] Alexander Olifirov, Dr.Sc. (Economics), Professor, V.I. Vernadsky Crimean Federal University, Yalta, Russia, alex.olifirov@gmail.com

[92] Krystina Makoveichuk, Ph.D. in Economics, Associate Professor, Financial University under the Government of the Russian Federation, Moscow, Russia, christin2003@yandex.ru

УДК 004.056

Методика обеспечения квантовой устойчивости блокчейн в условиях атак с применением квантового компьютера

Петренко А.С. [93]

В настоящей работе представлена возможная методика обеспечения квантовой устойчивости индустриальных блокчейн в условиях ранее неизвестных атак злоумышленников с применением квантового компьютера. В основе методики лежат известные и авторские методы системного анализа и криптоанализа, методы теории многокритериальной оптимизации, постквантовой криптографии и программотехники. Результативность методики была подтверждена экспериментальным способом, на примере блокчейн «InnoChain», получившем широкое распространение в отечественных компаниях «Аэрофлот», «Газпром нефть» и пр.[94]

Ключевые слова: квантовая угроза, технология распределенного реестра, квантово-устойчивый блокчейн, постквантовые криптопримитивы, квантовая устойчивость.

Введение

На примере алгоритмов - финалистов конкурса NIST можно видеть, как современные концепции синтеза схем постквантовой криптографии нашли применение для защиты индустриальных блокчейн [1-8]. Так, задачи теории решеток лежат в основе алгоритмов-финалистов конкурса NIST (CRYSTALS-Kyber, NTRU, SABER, CRYSTALS-Dilithium и FALCON), а также альтернативных алгоритмов-финалистов FrodoKEM и NTRU Prime. Задачи теории кодирования обеспечивают стойкость таких алгоритмов — финалистов конкурса NIST, как Classic McEliece и альтернативных алгоритмов-финалистов BIKE, HQC. На основе многочленов от многих переменных строится решение финалистов конкурса NIST Rainbow и альтернативный алгоритм-финалист GeMSS. Большое внимание уделяется криптографическим алгоритмам на основе хеш-функций, в частности, финалистом конкурса NIST стал XMSS, а альтернативным является алгоритм-финалист SPHINCS+.

Постановка задачи

В основе предлагаемой методики обеспечения квантовой устойчивости индустриальных блокчейн лежит математическая задача параметрического выбора постквантовых криптопримитивов следующего вида.

Дано:

1. $R = (r_1, r_2, r_3, ...r_k)$ - множество криптопримитивов для создания квантово-устойчивого индустриального блокчейн.

2. Каждый из рассматриваемых r_g криптопримитивов характеризуется вектором характеристик $y^{(g)} = (y_1^{(g)}, y_2^{(g)}, ...y_p^{(g)}, y_{p+1}^{(g)}, ...y_n^{(g)})$ где $y_t^{(g)}, t = 1,..., p$ - нечисловые характеристики, а $y_j^{(g)}, j = p+1,..., n$ - числовые характеристики. Каждая характеристика определяется в ходе анализа системных свойств криптопримитива (*безопасность, эффективность, ресурсоемкость, устойчивость* и др).

---

[93] Петренко Алексей Сергеевич, аспирант, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина), Санкт-Петербург, A.Petrenko1999@rambler.ru

[94] Работа подготовлена при поддержке «Гранта ИБ МТУСИ» № 19/23-К «Метод (технология) обеспечения квантовой устойчивости блокчейн-экосистем и платформ Цифровой экономики Российской Федерации»

3. Предполагается, что в распоряжении криптоаналитика имеются удовлетворяющие его весовые коэффициенты k_{lm}, учитывающие числовые параметры $y_j^{(g)}, j = p+1,...,n$ $l = p+1,...,n$ $m = p+1,...,n$. Для числовых параметров это не является сложной задачей. Весовой коэффициент k_{lm},является целым положительным числом и несет информацию по результатам сравнения конкретного криптопримитива r_l по отношению к другому криптопримитиву r_m по рассматриваемой характеристике. Он используется только для того, чтобы упорядочить криптопримитивы $R = (r_1, r_2, r_3,...r_k)$.

Требуется: оценить учитывающие нечисловые характеристики весовые коэффициенты возможных постквантовых криптопримитивов и выбрать не только необходимые, но и достаточные криптопримитивы для обеспечения требуемой квантовой устойчивости индустриального блокчейн.

Возможное решение

Сначала определиv функцию принадлежности криптопримитивов r_g к нечеткому бинарному отношению большей значимости одного из них над другим по рассматриваемой характеристике $\mu_R : R \times R \to [0, 1]$, $\mu_R(r_t, r_s) = P(r_t \succ r_s)$, $P(r_t \succ r_s)$ — вероятность того, что при выборе криптопримитива r_t вместо r_s это не позволит создать квантово-устойчивую блокчейн-платформу. Здесь элементы матрицы парных сравнений в вероятностной калибровке удовлетворяют следующим соотношениям: $\forall i \forall j,\ 0 \le a_{ij} \le 1,\ a_{ij} + a_{ji} = 1$. Представленная шкала строгого линейного порядка выполняет квантификацию качественных субъективных суждений криптоаналитика о необходимости и достаточности постквантового криптопримитива r_g по фиксированной характеристике $y_t^{(g)}$, $t = 1, \ldots, p$, описываемой нечисловой величиной.

Таблица 1.

Шкала оценки выбора постквантовых криптопримитивов

Пункты квалиметрической шкалы h_i	**Значимость криптопримитива**	**Комментарий относительно смысла значения**
h_0	Слабая	Выбор этого криптопримитива не целесообразен
h_2	Умеренная	Выбор этого криптопримитива является необходимым, но недостаточным
h_4	Существенная	Выбор этого криптопримитива является и необходимым, и достаточным
h_1, h_3, h_5	Промежуточные оценки между двумя соседними суждениями	Применяются в компромиссных случаях
h_6	Существенно очень сильная	Выбор этого криптопримитива предпочтителен

Для построения матрицы парных сравнений в вероятностной калибровке квалиметрическая шкала строгого линейного порядка $S = \langle H, R_> \rangle$ подвергается арифметизации. Задача арифметизации шкалы состоит в приписывании определенных

действительных чисел пунктам h_i носителя H шкалы S с сохранением заданных отношений, входящих в структуру $R_>$ этой шкалы. Основываясь на результатах математических методов теории квалиметрических шкал [1, 9-12] получаем следующее.

Пусть в результате попарного сравнения криптопримитивов r_t и r_s по фиксированной нечисловой характеристике криптоаналитик относит криптопримитив r_t к пункту h_p квалиметрической шкалы строгого линейного порядка $S = \langle H, R_> \rangle$, где: $H = (h_0, h_1, h_2, h_3, h_4, h_5, h_6)$, пара $(h_i, h_{i+1}) \in R_>$, $i = 0, 1, \ldots, 5$, h_i, $i = 0, 1, \ldots, 6$ — пункты (табл. 1) шкалы S; $R_>$ – отношение строгого линейного порядка, заданное на носителе H, а риск r_s к пункту h_q, $p \neq q$.

Тогда элементы матрицы парных сравнений криптопримитивов $A(t, s) = (a_{ts})_{k \times k}$ в вероятностной калибровке определяются следующим образом:

$$a_{ij} = \sum_{s=1}^{z} p_s \sum_{g=0}^{s-1} p_q + 0{,}5 \sum_{i=0}^{z} p_i p_q \qquad (1)$$

$a_{ji} = 1 - a_{ij}$, где $p_s(p_q)$ — вероятность приписывания пункту $h_p(h_q)$ шкалы $S = \langle H, R_> \rangle$ числового значения s/z, $s = 0, 1, \ldots, z$ $(q/z,\ q = 0, 1, \ldots, z)$ в результате арифметизации шкалы $S = \langle H, R_> \rangle$ в нормированную шкалу баллов $S = \langle H, R_\geq \rangle$ с носителем шкалы $Z = \left\{0, \frac{1}{z}, \frac{2}{z}, \ldots, \frac{z-1}{z}, 1\right\}$ и отношением линейного порядка $R_\geq$ с помощью нормированного стохастического процесса с равновероятными монотонными траекториями, которые представляют собой наборы точек прямоугольной целочисленной решетки $[0, m+1] \times [0, z]$ размером $(m + 2)(z + 1)$.

В случае шкалы (табл. 1) $m = 5$. Эти вероятности рассчитываются по следующим формулам:

$$p_s = \binom{p+s-1}{s} \binom{5-p+z-s}{z-s} \binom{5+z}{z}^{-1} \qquad (2)$$

$$p_q = \binom{p+q-1}{q} \binom{5-p+z-q}{z-q} \binom{5+z}{z}^{-1}. \qquad (3)$$

В данном случае погрешность арифметизации оценивается дисперсией случайной величины, принимающей числовое значение s/z, $s = 0, 1, \ldots, z$ $(q/z,\ q = 0, 1, \ldots, z)$.

Заключение

Отличительная особенность прилагаемого подхода заключается в том, что для принятия решения важны лишь значения такой безразмерной величины, как субъективная вероятность значимости одного криптопримитива перед другим. Уже это позволит построить матрицу парных сравнений, отражающую систему предпочтений лица, принимающего решения [1, 13].

Сравнительный анализ известных моделей линейного упорядочения позволил сделать вывод о целесообразности применения модели функции доминирования для выбора оптимального криптопримитива (ов) для индустриального блокчейн.

Первоначально модель функции доминирования криптопримитивов была разработана для обработки матриц с вероятностной калибровкой, а впоследствии обобщена для обработки матриц с калибровками типа турнирной, степенной, кососимметрической. Модель обладает свойствами инвариантности к растяжению и сдвигу, сохранения доминирования, положительной реакции, устойчивости в малом и сходством разных оптимальных упорядочений. Для матриц с вероятностной калибровкой модель допускает количественное измерение дополнительных характеристик криптопримитивов. При этом

такая модель не обладает свойством транспонируемости, что с избытком компенсируется ее положительными свойствами и простотой программной реализации.

Работа подготовлена при поддержке «Гранта ИБ МТУСИ» № 19/23-К «Метод (технология) обеспечения квантовой устойчивости блокчейн-экосистем и платформ Цифровой экономики Российской Федерации»

Литература

1. Петренко А. Квантово-устойчивый блокчейн: как обеспечить безопасность блокчейн-экосистем и платформ в условиях атак с использованием квантового компьютера. - СПБ: «Издательский Дом «Питер», 2023. – 320 с.
2. Петренко А. С. Отчет НИР «Математический аппарат для создания квантово-устойчивых блокчейн-платформ на основе постквантовых криптопримитивов». Грант РФФИ 20-04-60080/22. Номер ЦИТиС АААА-А20-120081290051-5, https://www.rfbr.ru/rffi/ru/rffi_contest_results/o_2109586
3. Петренко А. С. Отчет НИР «Модель угроз безопасности эталонной блокчейн-платформы по аналитике зарубежных национальных квантовых программ». Грант РФФИ № 18-47-160011/2021. Номер ЦИТиС АААА-А18-118101290047-8.
4. Петренко А. С. Отчет НИР «Методика оценивания квантовой устойчивости блокчейн-платформ на основе квантовых алгоритмов Шора и Гровера». Грантовое соглашение с Академией Наук Республики Татарстан (АН РТ) № 18-47-160011/2021. Номер ЦИТиС АААА-А18-118101290047-8.
5. Барабанов А.В., Дорофеев А.В., Марков А.С., Цирлов В.Л. Семь безопасных информационных технологий – М.: ДМК, 2017. 224
6. Кибербезопасность цифровой индустрии. Теория и практика функциональной устойчивости к кибератакам / Под ред. Зегжда Д.П. и др. М.: Горячая линия, 2021. 560 с.
7. Марков А.С., Цирлов В.Л. Основы криптографии: подготовка к CISSP // Вопросы кибербезопасности. 2015. № 1 (9). С. 65-73.
8. Математические основы информационной безопасности / Басараб М.А., Булатов В.В., Булдакова Т.И. и др.; Под. ред. В.А.Матвеева. М.: НИИ РиЛТ МГТУ им. Н.Э.Баумана, 2013. 244 с.
9. Alexei Petrenko. Applied Quantum Cryptanalysis. - River Publishers, River Publishers Series in Security and Digital Forensics, 1st ed. 2022, 222 p.
10. Sergei Petrenko. Cyber Security Innovation for the Digital Economy: A Case Study of the Russian Federation. - River Publishers, River Publishers Series in Security and Digital Forensics, 1st ed. 2018, 490 p. 198 illus. (Scopus).
11. Petrenko Sergei. Cyber Resilience. - River Publishers Series in Security and Digital Forensics, 1st ed. 2019, 492 p. 207 illus.
12. Петренко А.С., Петренко С.А. Метод оценивания квантовой устойчивости блокчейн-платформ. // Вопросы кибербезопасности. 2022. № 3 (49). с. 2–22. https://elibrary.ru/item.asp?id=49225476
13. Petrenko A.S., Petrenko S.A. Quantum Resilience Estimation Method Blockchain. // Voprosy Kiberbezopasnosti. 2022. No 3 (49). P. 2-22. DOI: 10.21681/2311-3456-2022-3-2-22.

Научный консультант: Лаврова Дарья Сергеевна, д.т.н., доцент, профессор Высшей школы кибербезопасности Санкт-Петербургского политехнического университета Петра Великого (СПбПУ), lavrova_ds@spbstu.ru

Methodology for ensuring quantum stability of blockchain in the face of attacks using a quantum computer

Petrenko A.S.[95]

Abstract. This paper presents a possible method for ensuring quantum stability of industrial blockchains in the face of previously unknown cybercriminal attacks using a quantum computer. The methodology is based on well-known and original methods of system analysis and cryptanalysis, methods of the theory of multicriteria optimization, post-quantum cryptography and software engineering. The effectiveness of the methodology was confirmed experimentally, using the example of the InnoChain blockchain, which has become widespread in domestic companies Aeroflot, Gazprom Neft, etc.

Keywords: quantum threat, distributed ledger technology, quantum-resistant blockchain, post-quantum cryptoprimitives, quantum stability.

[95] Petrenko Alexei, Ph.D. student of Saint-Petersburg State Electrotechnical University «LETI», Saint-Petersburg, A.Petrenko1999@rambler.ru

УДК 004.051

Спутниковые информационные технологии в период кризиса

Ромашкина Н.П.[96]

Аннотация. В статье представлен анализ значимых динамичных изменений глобального информационного пространства на космическом уровне, связанных с широкомасштабным распространением и ростом количества искусственных спутников Земли (ИСЗ), а также с ростом значимости прикладных спутников, используемых в военных целях в период кризиса. Приведена классификация ИСЗ, выполняющих военные функции. Поставлена проблема деструктивного использования ИСЗ во время военных конфликтов, связанных с этим увеличением риска киберугроз и ростом вероятности эскалации конфликтов, угроз для России, международной безопасности и стратегической стабильности. Доказывается, что количественные и качественные характеристики спутниковой группировки являются одним из важнейших показателей влияния и потенциала государства в мире. Выработаны предложения по минимизации угроз.

Ключевые слова: искусственный спутник Земли (ИСЗ), спутник военного назначения, рекогносцировочный разведывательный спутник, спутник связи, навигационный спутник, спутник дистанционного зондирования Земли, система предупреждения о ракетном нападении (СПРН), стратегическая стабильность

Введение

Значение глобального информационного пространства, включающего космический эшелон, приобретает новое звучание в период кризиса [1, 2]. Это обосновано тем, что инфраструктура сбора, изучения, обработки и передачи данных, в которой уникальную роль играют искусственные спутники Земли (ИСЗ), во время конфликтов важны для обеспечения процесса принятия государственных решений [3, 4]. Обладая исключительными возможностями получения, хранения и передачи информации, спутники с программно-определяемыми полезными нагрузками и функциями становятся все более гибкими и адаптивными. Космический уровень уже сегодня выглядит как быстрореагирующая сеть с масштабными перспективами дальнейшего развития. При этом новые технологии стирают традиционные границы между космическими и наземными сетями, спутниковая наземная инфраструктура адаптируется, переходя от аппаратно-ориентированных архитектур к программно-управляемым системам [5-7].

Таким образом, количественные и качественные характеристики спутниковой группировки являются сегодня одним из важнейших показателей престижа государства в мире, его влияния и потенциала. Растет роль ИСЗ в глобальном информационном пространстве, позволяющем стране обеспечивать безопасное взаимодействие с другими государствами и организациями, а также максимально полно удовлетворять свои потребности при сохранении баланса национальных и международных интересов.

Характеристики современного этапа развития ИСЗ

Одной из важных характеристик современного этапа является распространение и существенный рост числа ИСЗ (рис.1) [8, 9]. За период с 2008 по 2020 гг. глобальная спутниковая индустрия почти удвоилась и достигла более $270 млрд. Только за первое полугодие 2023 г. на орбиты было выведено более 700 ИСЗ.

[96] Ромашкина Наталия Петровна, кандидат политических наук, профессор, ЦМБ ИМЭМО РАН, Москва, Romachkinan@yandex.ru

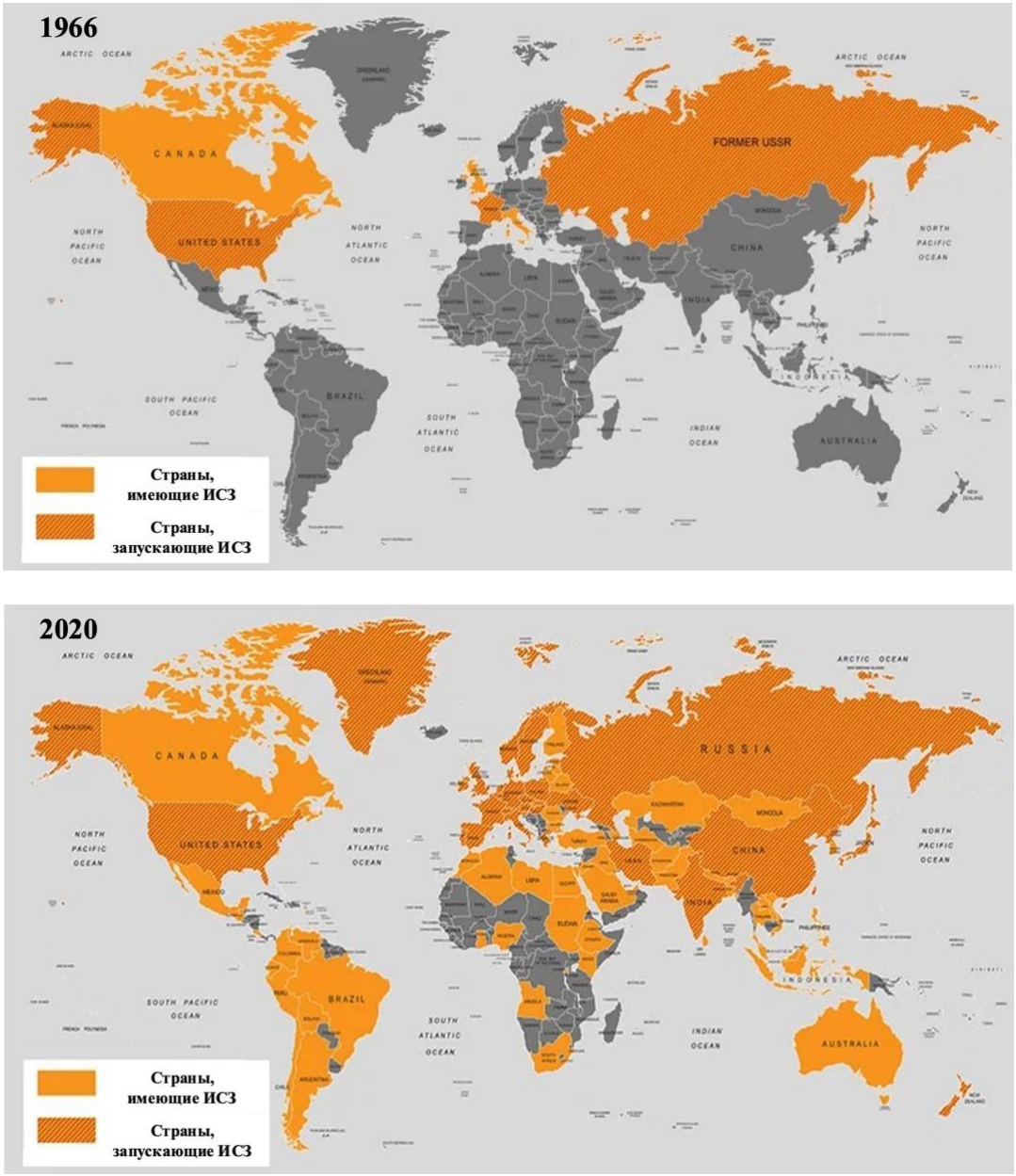


Рис. 1. Увеличение количества стран с ИСЗ, с 1966 г. по 2020 г.

В настоящее время на различных орбитах находится более 6700 ИСЗ, среди которых около 67% принадлежит США, около 9% принадлежит КНР, России – около 3% , 21% – всем другим странам, в число которых входит большое количество государств – союзников и партнеров США (рис. 2)[97]. Таким образом, еще одной важнейшей характеристикой текущего этапа является диспропорция в обладании странами искусственными спутниками Земли. На рис. 2 также представлено функциональное распределение ИСЗ по классификации США. Именно в число коммерческих ИСЗ, которые составляют более 88%, входит масштабная группировка *Starlink* американской компании *SpaceX*, которая сегодня активно используется ВСУ.[98] Несколько тысяч терминалов *Starlink*, установленных на

[97] UCS Satellite Database. Union of Concerned Scientists (UCS). // https://www.ucsusa.org/resources/satellite-database.

[98] «Законная цель для удара». Какие страны умеют сбивать спутники. 31.10.2022. // https://rtvi.com/stories/zakonnaya-czel-dlya-udara-kakie-strany-umeyut-sbivat-sputniki/.

территории Украины, позволяют ВСУ управлять ракетами, беспилотными летательными аппаратами, получать разведданные, обеспечивать связь и т.д.

В зависимости от решаемых задач ИСЗ подразделяют на *научно-исследовательские* и *прикладные*. Неуклонный рост значимости прикладных спутников, используемых в военных целях, стал еще одной тенденцией последних лет. Наиболее важную роль в период кризисов и военных действий играют *спутники связи, навигационные, дистанционного зондирования Земли (ДЗЗ)*, а также *спутники системы предупреждения о ракетном нападении (СПРН)* (рис. 3) [10-12].

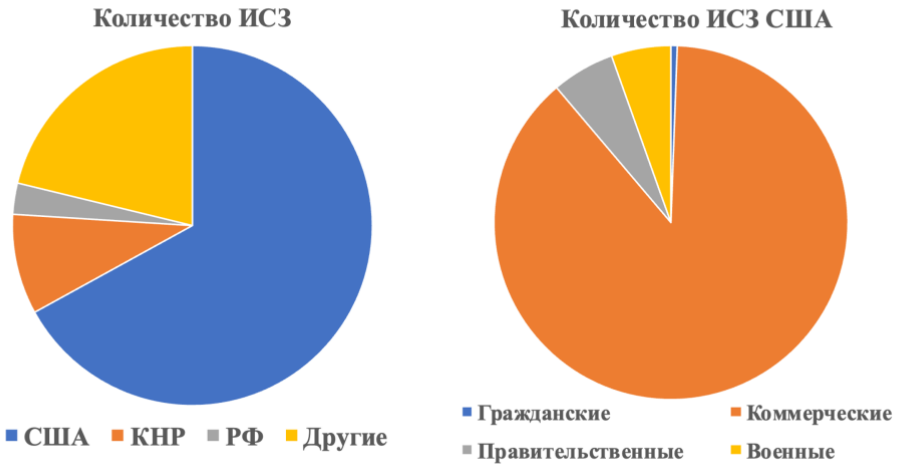


Рис. 2. Данные об ИСЗ на орбитах в 2023 г.

Рис.3. Задачи ИСЗ двойного и военного назначения

Военные функции ИСЗ

Во время военных операций ИСЗ служат для обеспечения боевых действий ВС и применения различных средств вооруженной борьбы:

- наблюдение за наземными, воздушными и космическими объектами, выявление угроз на земле, в космосе и из космоса;
- стратегическая и оперативная космическая разведка;

- обеспечение лиц, принимающих решения, достоверной информацией об активности противника;
- определение местоположения радиолокационных станций;
- предупреждение о ракетном нападении;
- контроль результатов ракетно-ядерных ударов;
- навигационное обеспечение боевого применения подвижных систем вооружения;
- геодезическое и метеорологическое обеспечение боевых действий войск круглосуточно и непрерывно;
- оперативное управление войсками с помощью космической связи, а также оружием с космических командных пунктов;
- профилактические и ремонтные работы в космосе;
- боевые действия в космосе и из космоса (по терминологии западных стран, «ведение космической войны»).

При этом быстродействие современных систем обработки и передачи данных со спутников позволяют в кратчайшие сроки выявить цель, опознать и создать условия для ее уничтожения [13, 14].

Проблема деструктивного использования ИСЗ во время военных действий

Проблема заключается в использовании космических информационных технологий – спутников стран НАТО и их партнёров – во враждебных военно-политических целях. Речь идет о передаче со спутников, в том числе, военного назначения, разведывательной информации формально нейтральными государствами для поддержки военных действий одной из сторон военного конфликта для уничтожения военнослужащих и военной техники другой стороны. Использование дронов, которые управляются с использованием информации с навигационных спутников НАТО, также является частью проблемы.

При этом США и страны НАТО открыто заявляют на самых разных уровнях[99], включая президента США, что они обеспечивают армию Украины разведывательной информацией, в частности, снимками высокого разрешения со своих ИСЗ. Это данные о расположении военных объектов, техники и подразделений российской армии в любую погоду и любое время суток. МО РФ и МИД РФ подтверждают эту информацию.[100]

В результате действий Запада неоправданным рискам подвергаются устойчивость мирной космической деятельности, а также многочисленные социально-экономические процессы на Земле.

Выводы

Таким образом, статья позволяет сделать вывод о том, что деструктивное использования ИСЗ в период кризиса наряду с другими вызовами ставит ряд глобальных проблем.

- Превращение космического пространства в сферу военно-политических действий в нарушение международного права.

[99] Напр., см: Постпред США при ООН подтвердила передачу разведданных Украине. 8 мая 2022. // https://www.rbc.ru/rbcfreenews/627803429a7947335ec5768c

[100] А. Комолов. Шойгу: почти вся спутниковая группировка НАТО работает против российской армии. 21.09.2022. // https://rg.ru/2022/09/21/shojgu-pochti-vsia-sputnikovaia-gruppirovka-nato-rabotaet-protiv-rossijskoj-armii.html.

Выступление заместителя руководителя российской делегации К.В. Воронцова в ходе тематической дискуссии по разделу «Космос (разоруженческие аспекты)» в Первом комитете 77-й сессии ГА ООН. 26 октября 2022 г. // https://russiaun.ru/ru/news/261022_v.

- Рост вероятности киберугроз в отношении ИСЗ, самой опасной среди которых является вмешательство в работу ИСЗ СПРН, что повышает риск ошибочного запуска баллистических ракет.
- Разработка систем вооружений для применения силы или угрозы силой в космосе, из космоса или в отношении космоса.
- Повышение угрозы гонки космических и противоспутниковых вооружений, в том числе кибероружия.
- Рост вероятности сокращения, так называемой, лестницы эскалации конфликта, в случае массированного вредоносного применения киберсредств на одной или нескольких ступенях лестницы. А, следовательно, снижение уровня стратегической стабильности.

Для повышения стабильности в глобальном информационном пространстве, в том числе, на космическом уровне с целью минимизации угроз для России, стратегической стабильности и международной безопасности целесообразно:

- введение проблематики использования спутников как важнейшей части глобального информационного пространства в международные обсуждения по МИБ в ООН;
- разработка общепризнанных юридически обязывающих принципов и норм международного права, которые носили бы всеобъемлющий характер и были бы нацелены на предотвращение гонки вооружений в космическом пространстве;
- совершенствование механизмов обеспечения информационной безопасности критически важных объектов государственной инфраструктуры, в том числе, космических, от которых зависит обороноспособность страны;
- расширение количественного и качественного потенциала формирований ВС РФ, обеспечивающих информационную безопасность;
- расширение количественного и качественного потенциала спутниковой группировки РФ;
- создание условий для отражения нападения противника с применением космических аппаратов, недопущения завоевания превосходства в стратегической космической зоне, комплекс мероприятий в околоземном космическом пространстве и на территории России;
- расширение сотрудничества в рамках ОДКБ и ШОС по обеспечению кибербезопасности, в частности, в сфере применения норм и принципов международного права в ИКТ-среде космического пространства [15, 16].

Литература

1. Ромашкина Н.П., Марков А.С., Стефанович Д.В. Международная безопасность, стратегическая стабильность и информационные технологии / отв. ред. А.В. Загорский, Н.П. Ромашкина. – М.: ИМЭМО РАН, 2020. – 98 с. DOI: 10.20542/978-5-9535-0581-9.

2. Ромашкина Н. П., Стефанович Д.В. Стратегические риски и проблемы кибербезопасности // Вопросы кибербезопасности. 2020. №. 5(39). С. 77–86.

3. Марков А.С., Ромашкина Н.П. Проблема выявления источника (атрибуции) кибератак – фактор международной безопасности // Мировая экономика и международные отношения. 2022. т. 66, № 12. С. 58–68, DOI: 10.20542/0131-2227-2022-66-12-58-68.

4. Ромашкина Н.П. Глобальные военно-политические проблемы международной информационной безопасности: тенденции, угрозы, перспективы // Вопросы кибербезопасности. 2019. № 1 (29). С. 2–9.

5. Digital Transformation and the Futures of Civic Space to 2030, Development Policy Paper, OECD Publishing, Paris. // https://www.oecd.org/dac/Digital-Transformation-and-the-Futures-of-Civic-Space-to-2030.pdf.

6. Digital Transformation. An IEEE Digital Reality Initiative White Paper, November 2020. // https://digitalreality.ieee.org/images/files/pdf/DRI_White_Paper_-_Digital_Transformation_-_Final_11Nov.pdf.

7. J. Wynbrandt. The Space Sector's Digital Launch: New Emphasis on Cutting-Edge Technologies Is Transforming Aerospace, 2020. URL: www.nasdaq.com/articles/the-space-sectors-digital-launch%3A-new-emphasis-on-cutting-edge-technologies-is.

8. Аксёнов Е.П. Главная проблема теории движения ИСЗ. — М.: Изд-во "Ким Л.А.", 2019. 88 с..URL: www.sai.msu.ru/neb/kaf/pcm/upos2_Axenov_main_problem.pdf.

9. Михайлов Р.Л. Спутниковые системы связи вооруженных сил иностранных государств: монография. – СПб.: Наукоемкие технологии, 2019. – 149 с.

10.Пантенков Д. Г., Гусаков Н. В., Ломакин А. А. Обзор современного состояния орбитальных группировок космических аппаратов дистанционного зондирования Земли и космических ретрансляторов. Обзорная статья // Изв. вузов. Электроника. 2022. Т. 27. № 1. С. 120–149. doi: https://doi.org/10.24151/1561-5405-2022-27-1-120-149.

11.Ромашкина Н.П. Космос как сфера конфронтации: спутники США в новых реалиях // Информационные войны. 2023. № 2 (66). С. 16-24.

12.Romashkina N.P., Markov A.S., Stefanovich D.V. Information Technologies and International Security. – Moscow: IMEMO, 2023. – 111 p. DOI: 10.20542/978-5-9535-0613-7.

13.Ромашкина Н.П. Космос как часть глобального информационного пространства в период военных действий // Вопросы кибербезопасности. 2022. № 6 (52). С. 100–111. DOI 10.21681/2311-3456-2022-6-100-111.

14.Ромашкина Н.П. Спутниковые системы управления с применением искусственного интеллекта // Вопросы кибербезопасности. 2023. № 6 (58). С. 100–110.

15.Ромашкина Н.П. Международно-правовой режим контроля над кибероружием в будущем миропорядке: угрозы и перспективы // Дипломатическая служба. 2023. № 2. С. 150–161. DOI 10.33920/vne-01-2302-07.

16.Международная безопасность в среде информационно-коммуникационных технологий / Стрельцов А.А., Капустин А.Я., Полякова Т.А. и др. - Коллективная монография по проблеме применения норм ответственного поведения государств в ИКТ-среде. М.: НАМИБ, 2023. 132 с.

Satellite Information Technologies during the Crisis

Romashkina N.P.[101]

Abstract. The article presents an analysis and systematization significant dynamic changes at the cosmic level of the global information space associated with the large-scale spread and significant increase in the number of artificial Earth satellites (AES), as well as with the growing importance of satellites for military purposes during the crisis. The article presents the classification of AES performing military functions, reveals the possibilities of modern AES in the period of crisis and military operations. The author poses the problems of the destructive use of artificial Earth satellites during military conflicts, associated with this increase in the risk of cyber threats and an increase in the likelihood of escalation of the conflict, threats to Russia, international security and strategic stability. The article proves the quantitative and qualitative characteristics of the satellite constellation are today one of the most important indicators of the influence and potential of the state in the world. Proposals have been developed to minimize threats to Russia, as well as to reduce the likelihood of an escalation of the conflict during the crisis.

Keywords: artificial Earth satellite, military satellite, reconnaissance satellite, communications satellite, navigation satellite, Earth remote sensing satellite, missile attack Warning System, strategic stability.

[101] Natalia Romashkina, Ph.D., Professor, Primakov National Research Institute of World Economy and International Relations, Russian Academyof Sciences, Moscow, Romachkinan@yandex.ru

УДК 004.056

Deception Platform как часть эшелонированной системы защиты

Тихонов А.М.[102]

В данном тезисе рассматривается применение технологии обмана злоумышленника с помощью Deception Platform. Для исследования эффективности работы Deception Platform была смоделирована сеть с классической защитой, были разобраны слабые места такой защиты и закрыты с помощью технологии обмана злоумышленника. Для уменьшения рисков были использованы различные ловушки и приманки, которые были встроены во внутреннюю сеть организации. В результате проведенного исследования была создана модель сети с интегрированной внутрь системой обмана злоумышленников, заставляющей их действовать по заранее заготовленному сценарию команды защиты.

Ключевые слова: методы и модели защиты сети, технология обмана злоумышленников.

Введение

В настоящее время любая организация, которая хотела бы быть конкурентноспособной, вынуждена быть интегрирована в информационные системы и технологии. Технологии позволяют организациям обрабатывать необходимый объем данных, причем объем этих данных постоянно растет. Вместе с тем, увеличивается и количество атак, направленных на такие организации с целью уничтожения и хищения собранных данных, получения конкурентного преимущества. Чтобы не понести репутационные, материальные и технологические потери, организации вынуждены трепетно относиться к своей безопасности. Для того чтобы защитить свои данные, компании вынуждены искать эффективные методы и средства защиты, которые позволили бы комплексно защитить всю инфраструктуру целиком [1].

Одним из таких методов может стать эшелонированная система защиты[103] – она способна противостоять большому количеству разных атак. Хорошо выстроенная система обороны способна защитить как внутреннюю сеть, так и демилитаризованную зону. В основе такой методики лежит создание обороны с помощью различных рубежей. Как правило, каждый рубеж отвечает за блокирование угроз на своем уровне, но при необходимости они могут пересекаться, чтобы формировать еще более надежную оборону. Методика предполагает использование различного набора средств, благодаря чему она является довольно гибкой, в том числе при создании защиты для специфической организации [2].

В качестве примера смоделируем организацию с классическим видом эшелонированной защиты сети в программе Cisco Packet Tracer[104]. Организация располагается в офисе на 3 этажах, в ней находятся разные отделы, имеется своя серверная и демилитаризованная зона. Поскольку организация небольшого размера, постольку ей вряд ли требуется большой набор средств защиты, она использует межсетевой экран, антивирус, двухфакторную аутентификацию, IDS систему (рис. 1). Каждый элемент системы защиты представляет из себя эшелон – сперва вредоносный трафик пытается заблокировать брандмауэр, далее трафик анализируется внутри сети с помощью IDS, затем

[102] Тихонов Александр Михайлович, аспирант, Финансовый университет при Правительстве РФ, Москва, amtikhonov@bk.ru

[103] https://knowledge.allbest.ru/programming/2c0b65635a3bc79a5c53a89521316c27_0.html

[104] https://studbooks.net/2172994/informatika/opisanie_simulyatora_cisco_packet_tracer

на компьютерах пользователей антивирусы блокируют опасный трафик, также распространению атаки будет мешать двухфакторная аутентификация.

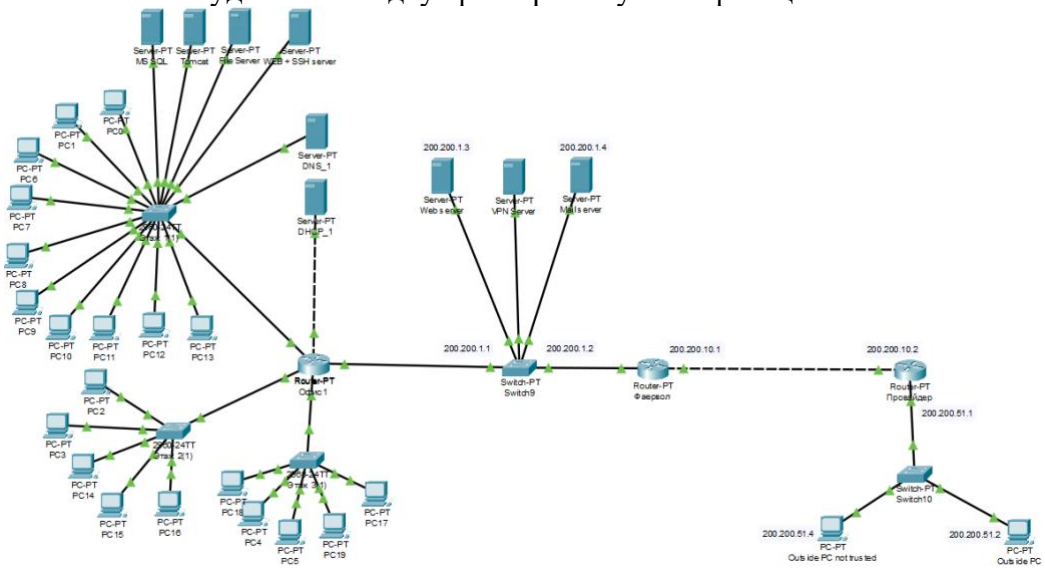


Рис. 1 Модель сети с обычной защитой

Однако у классической защиты такого типа есть свой минус – она несовершенна в случае проникновения и распространения злоумышленника во внутренней сети. Дело в том, что стандартные средства защиты на текущий момент плохо справляются с поиском злоумышленника внутри самой сети, если он выдает себя за легитимного пользователя. В крупных организациях время его поиска может составлять недели, за это время злоумышленник сможет собрать всю необходимую для него информацию. Во многом задача по поиску и противодействию злоумышленнику сводится к следующему – попытаться не допустить злоумышленника к важным элементам инфраструктуры, получить наибольшее количество времени для реакции на действия атакующего, проанализировать траекторию атаки и противодействовать ей, улучшить защиту сети, чтобы противостоять аналогичным угрозам. Для выполнения поставленных задач классической защиты может быть недостаточно, и для уменьшения рисков возможно использование дополнительных средств, например, Deception Platform. Она позволит вычислить злоумышленника, увести его внимание от основных ресурсов организации, понять траекторию развития атаки, действовать проактивно, навязывая свой сценарий развития событий, а также получить дополнительное время для противодействия злоумышленнику.

Ловушки и приманки

Deception Platform – это платформа для создания и внедрения ложных целей во внутреннюю инфраструктуру организации. Ложные цели – это и есть ловушки и приманки, которые помогают отвлечь злоумышленника от действительно значимой части инфраструктуры и обнаружить его в сети [3-8]. Идея Deception Platform является прямым продолжением идеи размещения HoneyPots[105], с той лишь разницей, что Deception платформа контролирует все ловушки и приманки, позволяет их разворачивать из единого интерфейса [9]. Различных ловушек и приманок на текущий момент имеется большое количество, но использовать их всех сразу для создания защиты смысла нет. И дело тут не только в ресурсах, которые придется потратить на оборудование и ПО для поддержания защиты такого типа, дело также заключается в том, что размещение внутри ловушек, не

[105] https://cloudnetworks.ru/inf-bezopasnost/honeypot/

характерных для настоящей инфраструктуры, только натолкнет злоумышленника на мысль, что он имеет дело с ловушками и не раскроет потенциал своей атаки, а значит, останется таким же потенциально опасным. Например, внутри организации находится один сервер Tomcat. Делать для него 10 ложных серверов будет не только избыточно, но и вредно с точки зрения обмана злоумышленника.

Ловушки могут быть нескольких видов. Клиентские ловушки – ловушки, которые имитируют действия клиента, например, это может быть ловушка типа NBNS Poisoning [10], выявляющая злоумышленника после получения запроса от него, или это может быть ложная созданная почта, получение письма на которую вызывает срабатывание системы безопасности. Серверные ловушки – ловушки, призванные имитировать настоящие сервера организации. Например, VPN и Outlook сервера, которые находятся в демилитаризованной зоне. Такие ловушки размещаются под очевидными адресами, например, vpn.company.org, привлекая злоумышленников. Настоящие же сервера могут находиться на других адресах, например, f5vpn1.company.org. Сервисные ловушки отвечают за имитацию сервисов, которые действительно могут находиться в организации. Например, работающие SSH и RDP сервисы на машинах – ловушках, видимые при их сканировании и доступные для подключения. Последний тип – файловые / парольные приманки, которые имитируют настоящие файлы или преподносятся злоумышленнику как настоящие пароли/логины. Например, на компьютерах сотрудников компании размещаются имитации важных файлов с характерными именами (финансовый отчет 2023.docx), которые в случае их любого изменения вызывают срабатывание системы защиты [11].

Используя вышеперечисленные ловушки и приманки, была улучшена предложенная выше модель защищенной сети. Были добавлены клиентские приманки в каждый отдел, в котором хранилась важная информация, на все компьютеры сотрудников были добавлены привлекающие файлы-приманки, похожие на настоящие ценные файлы, для каждого значимого сервера была сделана копия-ловушка, на некоторых из них были открыты сервисы-ловушки (рис. 2) [11, 12].

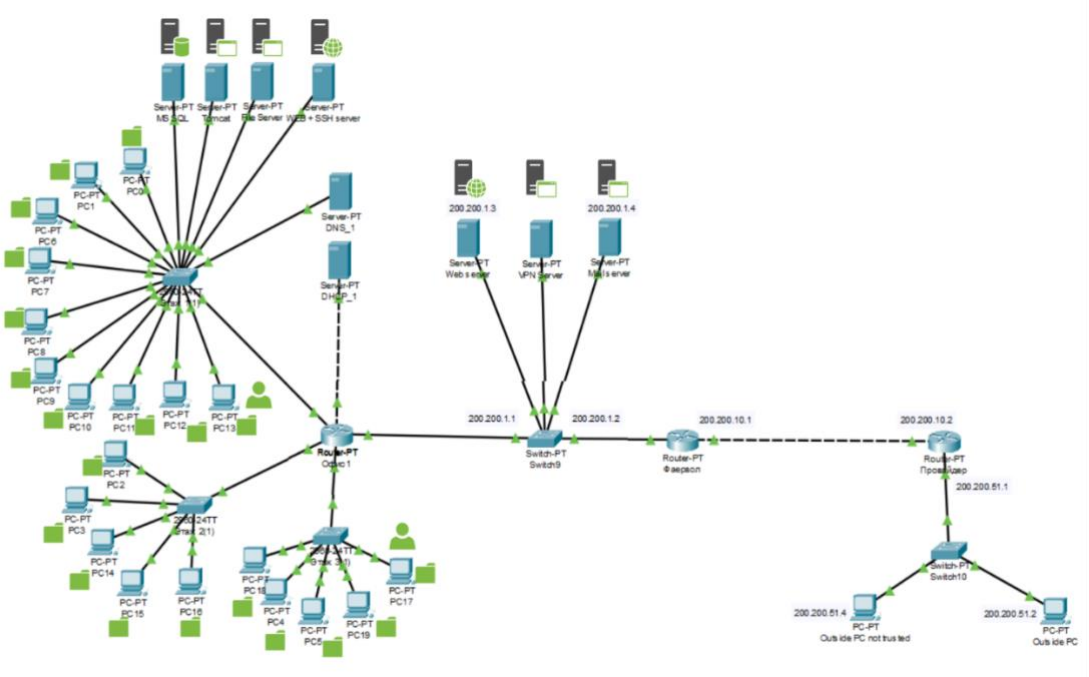


Рис. 2 – модель сети, улучшенная с помощью Deception Platform

В рамках проделанной работы была протестирована Deception платформа Deja Vu[106]. Было проведено 14 различных траекторий атак, каждая из которых была заблокирована с помощью средства защиты. Атаки проводились на: Mail Server, Tomcat Server, MySQL Server, VPN F5 Server, SSH, RDP, Telnet, ICMP, FTP, TFTP, Email, NBNS Client, Docx, Webserver HoneyComb Decoy.

Выводы

В результате проведения исследования была существенно улучшена модель классической эшелонированной защиты. Дополнительно к перечисленным выше эшелонам были добавлены рубежи защиты, построенные с помощью Deception Platform. Основная их задача – быть последними рубежами и противодействовать злоумышленникам, которые сумели проникнуть внутрь сети и начать там распространение. Развивая свою атаку внутри сети, злоумышленник с большой долей вероятности столкнется хотя бы с одной ловушкой или приманкой, в результате чего рассекретит себя. В худшем случае – злоумышленник просто рассекретит себя, наткнувшись на приманку, в лучшем случае, начнет взаимодействовать с ловушкой, показывая на ней свой потенциал и демонстрируя траекторию атаки. Так или иначе, такое средство заставляет действовать злоумышленника по заранее спланированному командой защиты сценарию, что снижает вероятность успеха его атаки и повышает вероятность быть рассекреченным.

Литература

1. *Кибербезопасность цифровой индустрии. Теория и практика функциональной устойчивости к кибератакам / Под ред. Зегжда Д.П. и др. М.: Горячая линия, 2021. 560 с.*
2. *Барабанов А.В., Дорофеев А.В., Марков А.С., Цирлов В.Л. Семь безопасных информационных технологий - М.: ДМК Пресс, 2017. 224 с.*
3. *Вишневский А.С. Обманная система для выявления хакерских атак, основанная на анализе поведения посетителей веб-сайтов // Вопросы кибербезопасности. 2018. № 3 (27). С. 54-62.*
4. *Каракашев А.В., Смирнов Я.Д. Использование ложных информационных систем - перспективное направление защиты информационных систем от атак "нулевого" дня // Известия Института инженерной физики. 2018. № 3 (49). С. 91–93.*
5. *Москвин Д.А., Овасапян Т.Д., Никулкин В.А. Адаптивное управление honeypot-системами для обеспечения кибербезопасности устройств интернета вещей // Защита информации. Инсайд. 2022. № 2 (104). С. 16–21.*
6. *Соболев Н.В., Зегжда Д.П. Построение сети с honeypot на основе классификации трафика с помощью LSTM // Методы и технические средства обеспечения безопасности информации. 2022. № 31. С. 15–16.*
7. *Шматова Е.С. Выбор стратегии ложной информационный системы на основе модели теории игр // Вопросы кибербезопасности. 2015. № 5 (13). С. 36–40.*
8. *Язов Ю.К., Сердечный А.Л., Шаров И.А. Методический подход к оцениванию эффективности ложных информационных систем // Вопросы кибербезопасности. 2014. № 1 (2). С. 55–60.*
9. *Путято М.М., Макарян А.С., Чич Ш.М., Маркова В.К. Исследование применения технологии Deception для предотвращения угроз кибербезопасности // Прикаспийский журнал: управление и высокие технологии, 2020 г. № 4 (52), С. 85-98, DOI 10.21672/2074-1707.2020.52.4.085-098.*
10. *Теленьга А.П. Маскирование метаструктур информационных систем в киберпространстве // Вопросы кибербезопасности. 2023. № 5 (57). С. 50–59.*
11. *Daniel Fraunholz. Demystifying Deception Technology: A Survey. Preprint. 2018. arXiv:1804.06196v1 [cs.CR]*
12. *Щетинин А. Deception: стратегическое решение для выявления инцидентов и реагирования на них // Информационная безопасность, 2022, №1.*

[106] https://github.com/bhdresh/Dejavu

Научный руководитель: Марков Алексей Сергеевич, доктор технических наук, профессор, Финансовый Университет при правительстве Российской Федерации, a.markov@npo-echelon.ru.

Deception Platform as part of an echeloned defense system

Tikhonov A. M.[107]

This thesis discusses the use of technology to deceive an attacker using the Deception Platform. To explore the effectiveness of Deception Platform, a network with classical protection was modeled and its weaknesses were analyzed and sealed with the help of technology to deceive the attacker. To reduce the risks, various traps and decoys were used, which were embedded in the internal network of the organization. As a result of this research, a network model was created with an inside-integrated deception system. Platform forcing attackers to act according to a pre-determined script of the defense team.

Keywords: network defense methods and models, intruder deception technology

[107] Alexander M. Tikhonov, post graduate student, Financial University under the Government of the Russian Federation, Moscow, amtikhonov@bk.ru

УДК 355.237: 004.056

Кадры решают всё: назад в будущее

Царегородцев А.В.[108]

В докладе отмечены проблемные вопросы подготовки специалистов по информационной безопасности. Проведен анализ потребности в кадрах по информационной безопасности, формирования государственного заказа на подготовку специалистов, удовлетворенности подготовкой выпускников в области информационной безопасности, материально-технического обеспечения и квалификации профессорско-преподавательского состава. Рассмотрены актуальные вопросы создания межвузовского центра и порядок лицензирования и контроля образовательной деятельности в области информационной безопасности.

Ключевые слова: подготовка специалистов, обучение, переподготовка, информационная безопасность.

Проблема подготовки кадров в области информационной безопасности (ИБ) не сходит со страниц СМИ и из уст государственных чиновников самого высокого ранга уже на протяжении нескольких лет [1-15]. Представители Минцифры и представители ФСТЭК, как Центра ответственности по УГСНП 10.00.00, сходятся во мнении, что количество выделяемых образовательным организациям бюджетных мест достаточно, чтобы покрыть потребность и государственных органов и бизнес-сообщества в специалистах по ИБ. Однако, из года в год приходится констатировать тот факт, что катастрофически не хватает квалифицированных специалистов по ИБ [12]. И здесь ключевое слово – квалифицированных! Количество вузов, готовящих специалистов по УГСНП 10.00.00 – 140 с небольшим, этим вузам выделяется бюджетное финансирование на подготовку таких специалистов (а это не малая сумма, с учетом того, что 10-я УГСНП относится ко 2 группе по базовым нормативам затрат). При этом, лишь 30 вузов по всей стране осуществляют подготовку именно квалифицированных специалистов – имеют современную обновляемую материально-техническую базу (МТБ) и квалифицированный профессорско-преподавательский состав (ППС)! А оставшиеся 100 с небольшим вузов можно разделить пополам: половина – это те вузы, которые не имеют ни современной материально-технической базы, ни квалифицированный профессорско-преподавательский состав, и «итоговый продукт», который они выпускают, мало пригоден для работы по специальности. Т.е. получаем, что государство тратит колоссальные средства на подготовку специалистов, ФСТЭКом прогнозируется, что эти специалисты будут задействованы в тех или иных областях и отраслях, а в реальности мы не получаем таких специалистов! Встаёт вопрос: что делать с такими вузами? Первое, что лежит на поверхности – не выделять КЦП по 10-й УГСНП этим вузам! Но сразу же звучат возражения, особенно от региональных властей: мы тогда вообще не получим для экономики региона специалистов по ИБ, потому что не поедут такие специалисты из столиц в регионы! И они совершенно правы! И продолжается вся эта песня из года в год – государство выделяет деньги на подготовку, а на выходе не получаем ожидаемого количества квалифицированных специалистов по ИБ! Что делать! *Предложение здесь может быть следующее: для специальностей и направлений подготовки по 10-й УГСНП ввести только целевой прием – либо от организаций, либо от государства, т.е. либо организация платит за обучение таких*

[108] Царегородцев Анатолий Валерьевич, д.т.н., профессор, руководитель департамента информационной безопасности Финансового университета при Правительстве Российской Федерации, academic_tsar@mail.ru

специалистов, либо государство, а соответственно, по окончании обучения специалист будет обязан отработать 3 или 5 лет там, где в нем есть потребность (да, это забытый вариант распределения, но это тот вариант, который позволит планировать, а, главное, гарантировать обеспеченность и потребность всех отраслей и регионов в специалистах по ИБ)!

Теперь рассмотрим положение дел с теми 50-60 вузами, которые либо не имеют современной МТБ, но у них есть более-менее квалифицированный ППС, либо наоборот, предприятия региона делятся современными средствами ЗИ для их использования в учебном процессе, при этом преподаватели потихоньку разбегаются в реальный сектор экономики, и в итоге не остается квалифицированных преподавателей! И привлечение практиков (что само по себе очень важная при обучении вещь) не спасает существенно ситуацию! Здесь стоит отметить, что в последнее время бизнес поворачивается лицом к проблемам вузов, некоторые компании бесплатно или почти бесплатно дают свои аппаратно-программные и программные продукты по ЗИ вузам, берут студентов на стажировки, но… Опять подчеркну, это исходя из личного опыта проведения проверок, в ряде вузов не только специализированное оборудование по ЗИ физически и морально устарело, но и информационная инфраструктура! И поэтому даже установить современное ПО у них нет возможности! Речь идет не только о региональных вузах, можно назвать с десяток столичных вузов, которые находятся в таком же плачевном состоянии! И здесь можно предложить несколько возможных путей исправления ситуации – они не бесспорные, но можно, основываясь на них, прийти к более-менее приемлемому сценарию выхода из этой тупиковой ситуации. Так вот, *предложение следующее – для исправления ситуации с устаревшей или отсутствующей материально-технической базой подготовки специалистов по УГСНП 10.00.00, во-первых, в госзадание таких вузов в течение 2-3-х лет включается статья на обновление и модернизацию их информационной инфраструктуры* (а деньги берутся – см. п.1 – из экономии от прекращения финансирования подготовки по 10-й УГСНП в тех вузах, в которых нет ни МТБ, ни квалифицированного ППС), *и, во-вторых, на базе ведущих вузов региона создаются центры коллективного пользования с современной постоянно обновляемой МТБ* (на базе которых в т.ч. могут создаваться киберполигоны для подготовки специалистов по обнаружению компьютерных атак), *чтобы другие вузы региона могли пользоваться ресурсами такого центра в подготовке специалистов по ИБ*!

И наконец, проблема обеспеченности квалифицированными преподавательскими кадрами образовательного процесса по УГСНП 10.00.00. Всем ясно, что хороший преподаватель по дисциплинам учебного плана 10-й УГСНП должен быть экспертом в своей области. Но зачем такому специалисту преподавать, ведь в реальном секторе экономики он может получать гораздо больше, чем в большинстве вузов? Отдельно хочется обратить внимание, что, как правило, это средняя возрастная группа преподавателей. Получается, что в образовательных учреждениях работает совсем немного профессионалов в области ИБ. И складывается ситуация, когда в вузах преподают либо мастодонты профессии – люди, стоящие у истоков направления Информационная безопасность, которым уже физически тяжело успевать за всеми современными техническими новинками, либо молодые ребята, которые сами только закончили обучение или продолжают обучение в аспирантуре! И это очень хорошо, что молодежь идет в образование, но эти ребята не имеют практических навыков работы в реальном секторе экономики (что называется «на земле») и времени на получение такого опыта (даже в виде стажировки) у них нет! Т.к. нормативы учебной нагрузки в большинстве вузов для категории преподавателей: ассистент, преподаватель и старший преподаватель, – самые большие – 900 часов аудиторной нагрузки. При таких нормативах времени на какие-либо другие активности у таких преподавателей, кроме проведения учебных занятий в

аудитории, вообще не остаётся! Эта же проблема касается и привлечения к учебному процессу преподавателей-практиков! Даже оформление на 0,25 ставки преподавателя-практика в вуз потребует от него проведения 225 часов аудиторных занятий (отдельно подчеркну – по расписанию!), что большинство работодателей позволить себе не могут! *Поэтому хочется обратиться к Министерству науки и высшего образования РФ с инициативой об изменении (в сторону уменьшения до 600 часов) нормативов учебной нагрузки для ППС вузов, осуществляющих подготовку по УГСНП 10.00.00*!

Литература

1. *Белов Е.Б. О профессиональных стандартах в области информационной безопасности // Информационное противодействие угрозам терроризма. 2015. Т. 3. № 25. С. 5–13.*
2. *Белов Е.Б., Лось В.П., Зайцева О.М., Кузора И.В. О необходимости актуализации профессиональных стандартов в области информационной безопасности и информационных технологий // Методы и технические средства обеспечения безопасности информации. 2020. № 29. С. 119.*
3. *Буйневич М.В., Матвеев А.В., Смирнов А.С. Актуальные проблемы подготовки специалистов в области информационной безопасности МЧС России и конструктивные подходы к их решению // Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России. 2022. № 3. С. 1–17.*
4. *Горбатов В.С., Дураковский А.П., Лобанов М.И. О профессиональных стандартах в интересах подготовки кадров по безопасности объектов критической информационной инфраструктуры // Безопасность информационных технологий. 2019. Т. 26. № 4. С. 54–68.*
5. *Дорофеев А.В., Марков А.С. Обучение специалистов в области кибербезопасности в стиле Purple Team // Защита информации. Инсайд. 2023. № 6. С. 67–71.*
6. *Зегжда П.Д., Черненко В.Г. Интеграция университетов и промышленных компаний - путь к успеху. опыт Lgpolyrec // Защита информации. Инсайд. 2007. № 1 (13). С. 56–59.*
7. *Иванов М.А., Овчинский А.С. Угрозы информационно-психологической безопасности в сфере образования и науки // Вопросы кибербезопасности. 2017. № S2 (20). С. 19–23.*
8. *Калиниченко И.А. Практико-ориентированный подход к подготовке специалистов в области кибербезопасности // Вопросы кибербезопасности. 2017. № S2 (20). С. 3–6.*
9. *Костина А.Б., Милославская Н.Г., Толстой А.И. Аспекты управления информационной безопасностью в учебных планах подготовки кадров в области информационной безопасности // Безопасность информационных технологий. 2011. Т. 18. № 4. С. 50–59.*
10. *Малюк А.А., Алексеева И.Ю. Конфуций и формирование культуры информационной безопасности в контексте развития цифровой экономики (новое - это хорошо забытое старое) // Безопасность информационных технологий. 2022. Т. 29. № 4. С. 89–104.*
11. *Марченко А.В., Войналович В.Ю., Воронин С.Н. Анализ состояния системы подготовки специалистов в области информационной безопасности // Безопасность информационных технологий. 2018. Т. 25. № 2. С. 6–22.*
12. *Петренко А.С., Петренко С.А., Костюков А.Д. Какие специалисты нужны отрасли информационной безопасности: DevSecOps-инженеры // Защита информации. Инсайд. 2023. № 6. 60–65 с.*
13. *Хорев А.А. Особенности формирования образовательной программы подготовки специалистов в области защиты информации в соответствии с требованиями ФГОС ВО // Защита информации. Инсайд. 2022. № 5 (107). С. 5–13.*
14. *Царегородцев А.В., Цацкина Е.П. Влияние информационного общества на подготовку обучающихся в сфере информационной безопасности // Вестник Московского государственного лингвистического университета. Образование и педагогические науки. 2019. № 4 (833). С. 191–199.*
15. *Шеремет И.А. Направления подготовки специалистов по противодействию киберугрозам в кредитно-финансовой сфере // Вопросы кибербезопасности. 2016. № 5 (18). С. 3–7.*

Personnel Decide Everything: Back to the Future[109]

Tsaregorodtsev A.V.

The report highlights the problematic issues of training of information security specialists. There was analyzed the demand for information security personnel, formation of the state order for training of specialists, satisfaction with training of graduates in the field of information security, material and technical support and qualification of teaching staff. Current issues of creating an inter-university center and the procedure of licensing and control of educational activities in the field of information security are considered.

Keyword: training of specialists, education, retraining, information security

[109] Anatoly V. Tsaregorodtsev, Ph.D/ (technical sciences), professor, Head of Information Security Department, Financial University under the Government of the Russian Federation, academic_tsar@mail.ru

УДК 004.056

Обезличивание персональных данных как способ повышения их защиты при обработке в информационных системах

Чепик П.И.[110]

Аннотация: Стремительное развитие информационных технологий создаёт условия для получения доступа и использования различных баз данных, а также предпосылки для утечки персональных данных, в том числе незаконного доступа к ним. Всё это делает задачу обеспечения защиты персональных данных особо актуальной и значимой в современном мире. Один из способов повышения защиты персональных данных при их обработке в информационных системах персональных данных является применение методов обезличивания, в результате которых невозможно определить принадлежность персональных данных к конкретному субъекту персональных данных.

Ключевые слова: информационная безопасность, персональные данные, безопасность персональных данных, обезличивания персональных данные, информационные системы персональных данных.

Введение

В настоящее время технические средства производят сбор, хранение, обработку, передачу и распространение, а также обеспечение информационной безопасности больших объёмов социально значимых сведений, необходимых для эффективного функционирования государственных механизмов обеспечения общественных процессов. При этом постоянно ускоряющаяся информатизация общества и активное развитие открытых информационных систем значительно упрощают утечку персональных данных (далее - ПДн) и иные формы незаконного доступа к ним.

Актуальность

Безопасность ПДн достигается путем исключения несанкционированного, в том числе случайного, доступа к ПДн, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение ПДн, а также иные несанкционированные действия. Для этого в информационных систем персональных данных (далее – ИСПДн) принимаются организационные меры и применяются средства защиты информации, в том числе криптографические [1-7] (средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки ПДн, а также используемые в информационной системе информационные технологии). Комплекс этих мер и средств представляет собой систему защиты ПДн [8].

Также один из способов обеспечения безопасности ПДн - это применение методов обезличивания [9, 10].

Обезличивание персональных данных

Применение обезличивания ПДн обусловлено необходимостью обработки, хранения и передачи ПДн в научных, статистических и прочих целях в форме предоставления, не допускающей возможности нанесения ущерба физическому лицу, которому эти Пдн принадлежат, так как обезличивание скрывает эту принадлежность.

В настоящее время отсутствуют единые и универсальные подходы к решению задач по обезличенной обработки ПДн. Подавляющее число работ посвящено исследованию

[110] Чепик Полина Игоревна, МГТУ им. Н.Э. Баумана, Москва, pchepik@yandex.ru

обработки ПДн и их эффективности, а тематике разработки и оценки характеристик методов обезличивания – лишь малая часть.

К достоинствам применения обезличивания можно отнести возможность реализации методов обезличивания путём модернизации прикладного программного обеспечения силами оператора ПДн, что упрощает эксплуатацию (ИСПДн) [11].

К недостаткам применения обезличивания можно отнести:

- необходимость защиты дополнительной информации, предназначенной для восстановления (дообезличивания) ПДн, при её хранении, передаче и использовании для доступа к ПДн на рабочем месте;

- наличие у злоумышленника возможностей получения необходимой для дообезличивания дополнительной информации косвенными методами (путём подбора, вычисления или из открытых источников).

Актуальность моделирования процессов обезличивания обусловлена необходимостью решения проблем, возникающих при реализации методов обезличивания в ИСПДн, к которым можно отнести:

- отсутствие методики обоснования выбора методов обезличивания и настройки их характеристик в зависимости от свойств базы ПДн;

- отсутствие методики количественной оценки эффективности методов обезличивания ПДн;

- отсутствие схемы безопасности передачи данных между разделёнными частями обезличенной базы.

Анализ нормативно-правых актов Российской Федерации в области обезличивании персональных данных

К нормативно-правым актам об обезличивании ПДн относятся:

1. Федеральный закон № 152-ФЗ «О персональных данных» от 26.07.2006. Определяет обязанности оператора принимать организационные и технические меры, в том числе обезличивание информации, для их защиты от неправомерного и случайного доступа. В Федеральном законе № 152-ФЗ от 26.07.2006 дано определение обезличивания: «обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных к конкретному субъекту персональных данных».

2. Постановление Правительства № 211 от 21.03.2012. Регламентирует работу с ПДн в государственных и муниципальных учреждениях, которые с 2014 года не обязаны осуществлять обезличивание ПДн.

3. Приказ Роскомнадзора № 966 от 05.09.2013. Определяет требования к обезличенным данным и содержит методологию этой процедуры. К методам обезличивания, установленным Приказом № 996 от 05.09.2013, относятся:

Анализ методов обезличивания персональных данных

Рассмотрим методы обезличивания Пдн, которые позволяют сохранять конфиденциальность личной информации. Существуют требования к методам обезличивания, которые закреплены в нормативно-правых актах Российской Федерации, где определены способы и алгоритмы обезличивания Пдн. Выбор конкретных алгоритмов и средств оператор, осуществляющий обработку ПДн, определяет самостоятельно.

К методам обезличивания, установленным Приказом № 996 от 05.09.2013, относятся:

- Метод введения идентификаторов, который реализуется путем замена части ПДн, позволяющих идентифицировать субъекта, их идентификаторами и созданием таблицы соответствия (справочника идентификаторов);

- Метод изменения состава или семантики, который реализуется путем обобщения, изменения значений атрибутов ПДн или удаления части сведений, позволяющих идентифицировать субъекта.

- Метод декомпозиции, который реализуется путем разделения множества атрибутов ПДн на несколько подмножеств и создания таблиц, устанавливающих связи между подмножествами (таблицы связей), с последующим раздельным хранением записей, соответствующих подмножествам этих атрибутов.

С помощью различных методов можно получить различные обезличенные данные с разными свойствами для выполнения целевых операций с ними. В описании вышеуказанных методов указаны основные условия для выполнения отдельных требований.

По результатам анализа зарубежных источников на сегодняшний день существуют два основных подхода к обезличиванию ПДн: рандомизация и обобщение.

Рандомизация – это семейство методов обезличивания, которые изменяют достоверность данных с целью устранения сильной связи между данными и субъектом. Чем выше степень неопределённости данных, тем меньше вероятность отнесения их к конкретному субъекту. Методы рандомизации не влияют на уникальность записей, но способствуют защите от рисков определения значений. Методы рандомизации могут использоваться в совокупности с методами обобщения для исключения связи отдельной записи только с одним субъектом. К методам рандомизации относятся: метод добавление шума, метод перестановки, статистическое обезличивание и другие [12-14].

Обобщение – семейство методов, состоящих в обобщении или добавлении атрибутов субъектов, данных путём изменения масштаба или порядка значений/атрибутов (например, квартира, а не дом или не год, а месяц и т.п.) [15, 16]. Также выделяются так называемые методы обобщения с подавлением записей, где часть записей заменяется идентификатором. Методы обобщения эффективны относительно угрозы выделения субъектов, однако в отдельности не позволяют эффективно обезличивать данные [17, 18]. К методам обобщения относятся: методы агрегирования, методы достижения *k*-анонимности, *l*-разнообразия, *t*-близости и т.д.

Применение методов обезличивания ПДн позволяет облегчить требования к безопасности ИСПДн, что ведет к снижению затрат и обеспечению безопасности персональных данных, что согласуется с требованиями Федерального закона №152-ФЗ от 26.07.2006. Разработка практических методов и алгоритмов обезличивания ПДн, повышение их надежности и эффективности составляют актуальную проблему, имеющую большое научное и практическое значение.

Выводы

Применение методов обезличивания ПДн позволяет не только повысить степень их защищённости, но и снизить требования к ИСПДн, в которых они обрабатываются, так как обезличенные данные не относятся к определению ПДн и не требуют защиты при их обработке.

Литература

1. *Васильков А., Васильков И. Безопасность и управление доступом в информационных системах: М.: ФОРУМ, 2010, 368с.*
2. *Дорофеев А.В., Марков А.С. Структурированный мониторинг открытых персональных данных в сети интернет // Мониторинг правоприменения. 2016. № 1 (18). С. 41–53.*
3. *Кондаков С.Е., Чудин К.С. Разработка исследовательского аппарата оценки эффективности мер обеспечения защиты персональных данных // Вопросы кибербезопасности. 2021. № 5 (45). С. 45–51.*
4. *Лившиц И.И. Оценка степени влияния General Data Protection Regulation на безопасность предприятий в Российской Федерации // Вопросы кибербезопасности. 2020. № 4 (38). С. 66–75.*

5. *Минзов А.С., Невский А.Ю., Баронов О.Р. Безопасность персональных данных: новый взгляд на старую проблему // Вопросы кибербезопасности. 2022. № 4 (50). С. 2–12.*
6. *Петренко С.А., Зотова А.В. Инфраструктурные модели операторов персональных данных // Защита информации. Инсайд. 2013. № 6 (54). С. 42–45.*
7. *Шумилин А.С. Метод обеспечения защиты персональных данных в медицинской облачной системе // Вопросы кибербезопасности. 2023. № 4 (56). С. 53–64.*
8. *Гагарина Л.Г., Киселев Д.В., Федотова Е.Л. Разработка и эксплуатация автоматизированных информационных систем М.: ИНФРА-М, ФОРУМ, 2011. - 384 с.*
9. *Варфоломеев А.А. О методах введения идентификаторов и перемешивания для обезличивания (анонимизации) персональных данных. В сборнике: «Безопасные информационные технологии» (БИТ-2016). Сборник трудов Седьмой Всероссийской научно-технической конференции. / Под редакцией В.А. Матвеева. МГТУ им. Н.Э.Баумана, 2016. С. 103–104.*
10. *Саксонов Е.А., Шередин Р.В. Процедура обезличивания персональных данных // Наука и образование: научное издание МГТУ им. Н.Э. Баумана. 2011. № 3. С. 1.*
11. *Мищенко Е.Ю. Моделирование процессов обезличивания персональных данных и оценка эффективности используемых методов на основе модели нарушителя: дис. … канд. тех. наук. Екатеринбург, 2023. 3 с.*
12. *N. R. Adam and J. C. Wortmann. Security-control methods for statistical databases: A comparative study. ACM Comput. Surv., 21(4):515-556, 1989.*
13. *G. T. Duncan and S. E. Feinberg. Obtaining information while preserving privacy: A Markov perturbation method for tabular data. In Joint Statistical Meetings, Anaheim, CA, 1997*
14. *G. Aggarwal, T. Feder, K. Kenthapadi, R. Motwani, R. Panigrahy, D. Thomas, and A. Zhu. /c-anonymity: Algorithms and hardness. Technical report, Stanford University, 2004*
15. *K. LeFevre, D. DeWitt, and R. Ramakrislman. Incognito: Efficient fulldomain k-anonymity. In SIGMOD, 2005*
16. *R. J. Bayardo and R. Agrawal. Data privacy through optimal /c-anonymization. In ICDE-2005, 2005*
17. *P. Samarati and L. Sweeney. Protecting privacy when disclosing information: k-anonymity and its enforcement through generalization and suppression. In Proceedings of the IEEE Symposium on Research in Security and Privacy, 1998*
18. *N. R. Adam and J. C. Wortmann. Security-control methods for statistical databases: A comparative study. ACM Comput. Surv., 21(4):515-556, 1989.*

Научный консультант: Шахалов Игорь Юрьевич, доцент кафедры ИУ8 МГТУ им. Н.Э. Баумана, i.shahalov@npo-echelon.ru

DEPERSONALIZATION OF PERSONAL DATA AS A WAY TO INCREASE THEIR PROTECTION DURING PROCESSING IN INFORMATION SYSTEMS

Chepik P.I.[111]

Abstract: The rapid development of information technology creates conditions for gaining access and use of various databases, as well as preconditions for the leakage of personal data, including unauthorized access to it. All this makes the task of ensuring the protection of personal data especially relevant and significant in the modern world. One of the ways to increase the protection of personal data when processing it in personal data information systems is the use of depersonalization methods, as a result of which it is impossible to determine the ownership of personal data by a specific subject of personal data.

Keywords: information security, personal data, security of personal data, depersonalization of personal data, personal data information systems.

[111] Polina I. Chepik, BMSTU, Moscow, p.chepik@yandex.ru

УДК 004.05

Правовые перспективы технологий искусственного интеллекта

Карцхия А.А.[112], Макаренко Г.И.[113], Макаренко Д.Г.[114]

Аннотация. Ускоренное распространение к технологиям искусственного интеллекта ставит на повестку дня ряд вопросов правого характера. В настоящей работе предпринята попытка рассмотреть риски, связанные с неправовым использованием возможностей, которые открывает искусственный интеллект, которые могут возникнуть в результате потенциального преднамеренного неправильного использования или непреднамеренных проблем с контролем передового ИИ, при этом особую озабоченность вызывают риски кибербезопасности, биотехнологии и дезинформации.

Ключевые слова: кибератаки, безопасность, контроль, риски, угрозы конфиденциальности, ключевые принципы, повышение подотчетности.

Введение

Выступая на международной конференции «Путешествие в мир искусственного интеллекта» AI Journey, 24.11.2023 Президент РФ В.В.Путин указал, что с внедрением искусственного интеллекта в науку, образование, здравоохранение, все сферы нашей жизни — человечество начинает новую главу своего существования. Указывая на роль искусственного интеллекта сегодня, он отметил, что соперничество между государствами в сфере разработки и внедрения ИИ идет просто ожесточенное, от этого зависит место России в мире, ее суверенитет и безопасность. Поставлена задача дальнейшего ускоренного развития технологий ИИ, чтобы Россия стала одной из самых комфортных юрисдикций для развития искусственного интеллекта[115]. В то же время, 1 ноября 2023г. на первом саммите по безопасности искусственного интеллекта в Великобритании ряд стран, включая США, КНР, Европейский Союз, Великобританию, Францию, Италию, Индию, Бразилию, Японию, Королевство Саудовской Аравии, Объединенные Арабские Эмираты, Нигерию, была принята Декларация по вопросам безопасности искусственного интеллекта (The Bletchley Declaration on AI safety)[116], устанавливающего общее понимание возможностей и рисков, связанных с генеративным искусственным интеллектом (AGI), выражено общее понимание настоятельной необходимости осознания потенциальных рисков ИИ и коллективного управления ими посредством новых совместных глобальных усилий по обеспечению безопасной и ответственной разработки и внедрения передового ИИ.

Россия не участвовала в этом саммите. Страны-участницы согласились, что существенные риски могут возникнуть в результате потенциального преднамеренного неправильного использования или непреднамеренных проблем с контролем передового ИИ, при этом особую озабоченность вызывают риски кибербезопасности, биотехнологии и дезинформации.

В Декларации отмечается существование потенциала для серьезного, даже катастрофического ущерба, преднамеренного или непреднамеренного, вытекающего из

[112] Карцхия Александр Амиранович, доктор юридических наук, профессор РГУ нефти и газа (НИУ) имени И.М. Губкина, г. Москва. E-mail: arhz50@mail.ru

[113] Макаренко Григорий Иванович, старший научный сотрудник ФБУ НЦПИ при Минюсте России, г. Москва, E-mail: t7920518@yandex.com

[114] Макаренко Дмитрий Григорьевич, эксперт Федерального института сертификации и оценки интеллектуальной собственности и бизнеса, г. Москва. E-mail: d.g.makarenko@gmail.com

[115] http://www.kremlin.ru/events/president/transcripts/72811

[116] https://www.gov.uk/government/news/countries-agree-to-safe-and-responsible-development-of-frontier-ai-in-landmark-bletchley-declaration

наиболее существенных возможностей технологий и моделей ИИ. Среди основных рисков выделены такие, как предвзятость и нарушение конфиденциальности в применении ИИ.

30 октября 2923г. в Хиросиме (Япония) группа стран G7 приняли совместное Заявление «G7 Leaders' Statement on the Hiroshima AI Process, которым провозглашены свод Международных руководящих принципов по искусственному интеллекту (The International Guiding Principles on Artificial Intelligence) и рекомендован Кодекс поведения для разработчиков искусственного интеллекта (Code of Conduct for AI developers), который содержит набор правил, которым рекомендуется следовать разработчикам ИИ на добровольной основе для снижения рисков на протяжении всего жизненного цикла ИИ[117].

Хиросимский процесс искусственного интеллекта проводится с целью создания всеобъемлющей политической основы, способствующей разработке безопасных и заслуживающих доверия систем искусственного интеллекта и снижающей риски, возникающие, в частности, от генеративного искусственного интеллекта. Основными 5 рисками признаются: распространение дезинформации и манипулирование, нарушения интеллектуальной собственности, угрозы конфиденциальности, дискриминация и предвзятость, а также риски для безопасности.

В Заявлении отмечается, что решение задач управления рисками ИИ, исходя из общих принципов верховенства закона и демократических ценностей, требует формирования инклюзивного управления искусственным интеллектом на основе предложенных Международных руководящих принципов и Кодекса поведения для организаций, разрабатывающих передовые системы искусственного интеллекта. Предусматривается, что усилия в сфере ИИ в рамках Хиросимского процесса совместно с Глобальным партнерством по искусственному интеллекту (GPAI) и Организацией экономического сотрудничества и развития (ОЭСР) с участием многих заинтересованных участников, в т.ч. с правительствами, научными кругами, гражданским обществом и частными компаниями не только в странах G7, но и за ее пределами, включая развивающиеся страны и страны с формирующейся рыночной экономикой, будут способствовать созданию открытой и благоприятной среды, в которой безопасные и заслуживающие доверия системы искусственного интеллекта проектируются, разрабатываются, развертываются и используются для максимизации преимуществ технологии при одновременном снижении связанных с ней рисков, для общего блага во всем мире, с целью устранения цифрового разрыва и достижения цифровой инклюзивности.

Предполагается, что Принципы по ИИ и Кодекс поведения будут постоянно пересматриваться и обновляться, чтобы гарантировать их актуальность, учитывая стремительный характер развития технологий искусственного интеллекта. В Кодексе поведения особо признается, что различные юрисдикции могут применять свои уникальные подходы к реализации правил по-своему. Для государств-членов ЕС Закон об искусственном интеллекте (Artificial Intelligence Act (the "AI Act"), который, как ожидается, будет завершен к началу 2024 года, предоставит предписывающие и юридически обязательные правила разработки и использования ИИ, и вполне вероятно, что этот закон создаст шаблон, по которому другие юрисдикции будут стремиться моделировать свои собственные законодательные рамки в области ИИ.

Принципы служат руководством для организаций, разрабатывающих базовые модели (генеративный) ИИ, и включают следующие одиннадцать ключевых принципов:

1) Принятие необходимых мер для выявления, оценки и снижения рисков на протяжении всего жизненного цикла ИИ от разработки до промышленного применения;

2) Выявление и устранение уязвимостей ИИ, включая инциденты и схемы неправильного использования или внедрения, в т. ч. при размещении на рынке;

[117] G7 Hiroshima Process on Generative Artificial Intelligence (AI): Towards a G7 Common Understanding on Generative AI, 7 September 2023, OECD 2023 // http://www.oecd.org/termsandconditions (дата обращения 15.11.2023)

3) Обнародование сведений о возможностях, ограничениях и областях надлежащего и ненадлежащего использования передовых систем ИИ для поддержания и обеспечения достаточной прозрачности и повышению подотчетности;

4) Применение ответственного обмена информацией и сообщениями об инцидентах среди организаций, разрабатывающих передовые системы ИИ, в т. ч. в промышленности, госуправлении, гражданском обществе и научном сообществе;

5) Разработка, внедрение и раскрытие политики управления ИИ и рисками, основанной на риск-ориентированном подходе, включая политику конфиденциальности и меры по смягчению последствий, в частности для организаций, разрабатывающих передовые системы ИИ;

6) Создание надежных средств контроля безопасности, включая физическую безопасность, кибербезопасность и защиту от внутренних угроз на протяжении всего жизненного цикла ИИ;

7) Разработка и внедрение надежных механизмов аутентификации контента и определения происхождения, позволяющие пользователям идентифицировать контент, созданный искусственным интеллектом;

8) Приоритетное внимание исследованиям, направленным на снижение социальных рисков и рисков безопасности ИИ, а также инвестициям в эффективные меры по их снижению;

9) Приоритетное внимание разработке передовых систем искусственного интеллекта для решения глобальных мировых проблем, включая, но не ограничиваясь проблемами климатического кризиса, глобального здравоохранения и образования;

10) Поощрение разработки и принятие международных технических стандартов;

11) Обеспечение мер по вводу данных и защите персональных данных и интеллектуальной собственности.

Саммит по безопасности ИИ и Хиросимский процесс по ИИ стали новой вехой в формировании международно-правового регулирования сферы цифровых технологий и прежде всего – искусственного интеллекта как наиболее перспективной и комплексной системы. Вместе с тем обозначилось отсутствие стремления к установлению консенсуса по вопросам регулирования ИИ на международном уровне, что проявилось в собрании лишь небольшой группы государств (хотя и являющихся лидерами в сфере развития ИИ) для решения исключительно актуального вопроса – создания и развития технологий и моделей генеративного ИИ. Очевидно, решение проблемы безопасности ИИ должно привлекать значительно большее число стран, несомненно заинтересованных в установлении единых правил развития и применения передовых систем искусственного интеллекта.

Правовые аспекты безопасности современного искусственного интеллекта

Как отмечалось в Декларации Хиросимского процесса (2023г.)[118], потенциальные преимущества генеративного ИИ сопряжены с определенными рисками. Способность генеративного ИИ усугублять проблемы дезинформации и манипулирования мнениями рассматривается как одна из основных угроз, исходящих от генеративного ИИ, наряду с рисками нарушения прав интеллектуальной собственности и неприкосновенности частной жизни. Ответственное использование генеративного ИИ, борьба с дезинформацией, защита прав интеллектуальной собственности и управление генеративным ИИ являются одними из приоритетов и требуют международного сотрудничества. Другие неотложные и важные вопросы включают конфиденциальность и управление данными, прозрачность, справедливость и предвзятость, права человека и фундаментальные права, безопасность и надежность систем искусственного интеллекта, а также влияние на функционирование демократии.

[118]G7 Hiroshima Process on Generative Artificial Intelligence (AI): Towards a G7 Common Understanding on Generative AI, 7 September 2023, OECD 2023 // http://www.oecd.org/termsandconditions (дата обращения 15.11.2023)

Примечательно, что в качестве дополнительных рисков были также выделены угрозы безопасности (включая кибербезопасность), манипулирование данными и ненадлежащее использование данных, а также угрозы правам человека. Выделяются несколько основных категорий риска генеративного ИИ: (1) дезинформация (манипуляция); (2) нарушение авторских прав и иных прав интеллектуальной собственности; (3) нарушения неприкосновенности (тайны) частной жизни; (4)усиление предвзятости и дискриминация;(5) риски безопасности, включая кибербезопасность;(6)противоправная деятельность (мошенничество, и др.) (см. рис. 1).

Проблема безопасности ИИ сформулирована и обсуждается сравнительно недавно, но ее столь широкое правовое оформление на международном уровне сделано впервые. Безопасность искусственного интеллекта представляет собой состояние защищенности от угроз для человека при использовании ИИ, во взаимодействии с ИИ и в системе социальной и биосферы человечества, где ИИ уже стал значимым фактором, оказывающим самостоятельное влияние на общественные отношения, на самого человека. ИИ переходит от стадии инструмента, созданного человеком, к самостоятельной операционной системе, существующей по особым правилам и законам, техническим стандартам, и все чаще на базе машинного обучения (ML) и нейронных сетей. Об этом свидетельствует множество публикаций, например [1-12].

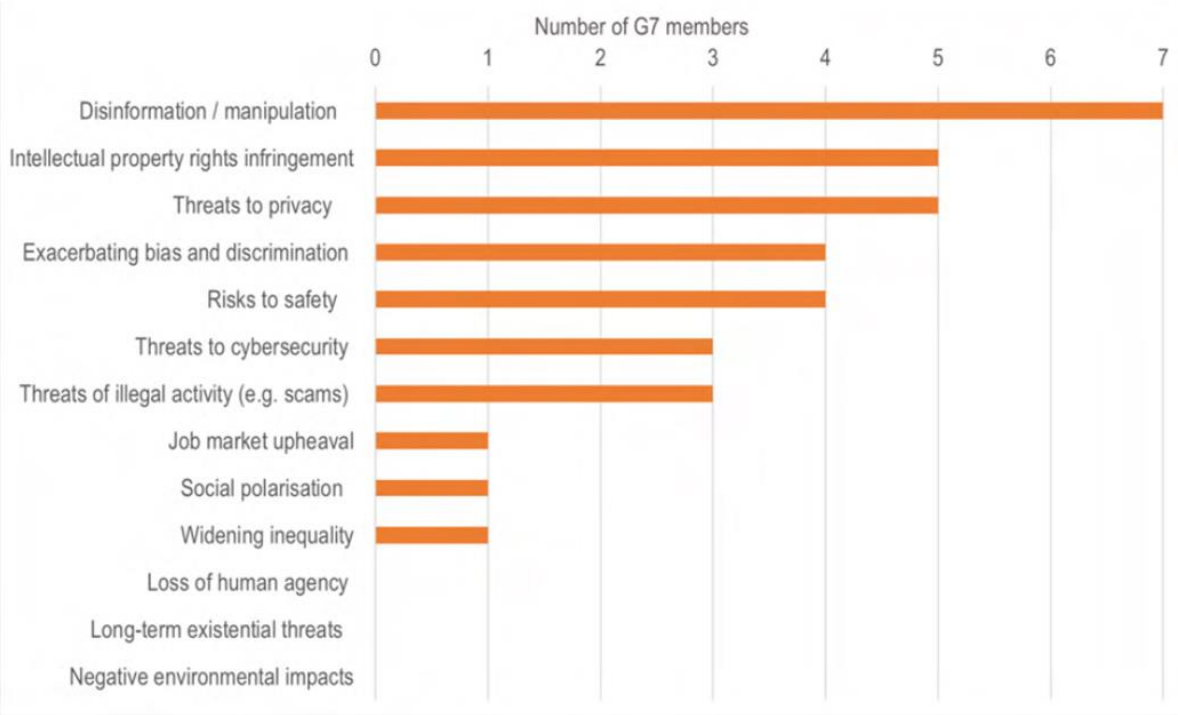


Рис.1. Пять основных рисков применения генеративного искусственного интеллекта *(G7 Hiroshima Process on Artificial Intelligence (AI).*

В связи с этим, технологии ИИ классифицируются в трех разных аспектах: *методы*, применяемые при создании ИИ (например, машинное обучение); *функциональные приложения* (например, обработка речи и компьютерное зрение); и *области применения* этих технологий (например, связь, транспорт)[119].

[119] WIPO Technology Trends 2019, Artificial Intelligence. https://www.theblockchaintest.com/uploads/resources/WIPO%20-%20Technology%20Trends%202019-Artificial%20Intelligence%20-%202019.pdf

Стоит отметить, что термин "искусственный интеллект" не относится к какой-либо конкретной технологии, как отмечают эксперты, - скорее, это собирательный термин для множества технологий использования математико-статистических методов для моделирования когнитивных способностей. Технологии искусственного интеллекта работают на основе анализа большого объема неструктурированных данных *(Big Data)* по специально разработанному алгоритму для выявления определенных закономерности данных и получения на их основе конкретного вывода с использованием нейронной сети, алгоритмы и структура которых основаны на функциональных принципах человеческого мозга, где большое количество отдельных алгоритмов работают вместе во взаимосвязанном и взаимозависимым образом, отражающим функционирование сети синапсов в человеческом мозге.

Сложные нейронные сети с несколькими уровнями обработки (со множеством соединенных последовательно и влияющих друг на друга алгоритмов) называются глубокими нейронными сетями *(Deep Neural Networks)*. В сложных ("глубоких") нейронных сетях способ взаимодействия отдельных алгоритмов друг с другом больше не определяется разработчиком, поскольку количество определяемых параметров слишком велико. Вместо этого подходящие обучающие данные (т. е. обучающие данные, специально отобранные и предназначенные для использования по назначению) передаются в нейронную сеть для обработки в автоматических циклах обучения. Нейронная сеть использует процессы статистической оптимизации для определения наиболее подходящих настроек (параметризация), например, для автономной идентификации лица на снимках. Этот процесс автоматической параметризации нейронной сети известен как глубокое обучение (*Deep Learning*). Качественный уровень технологии ИИ зависит от его архитектуры, обучения и качества обучающих данных, поскольку структура нейронной сети, ее настройки должны быть адаптированы к конкретной цели, на которую нацелен ИИ (например, распознавание речи или изображений, генерация текста и т. д.). В идеале приложение искусственного интеллекта должно быть способно идентифицировать в большом объеме данных (например, в потоке данных камеры наблюдения) тип шаблона, для которого оно было обучено (например, лица, номерные знаки и т. д.), за очень короткое время. Фактический показатель успешности приложений искусственного интеллекта во многом зависит от структуры нейронной сети, способа ее обучения и качества используемых обучающих данных [13].

Единообразие подходов при определении ИИ, общие определения для ИИ на международном уровне и в разных секторах его применения способны обеспечить инклюзивный диалог, устраняя различия между юрисдикциями и способствуя междисциплинарным коммуникациям и сотрудничеству. Эти усилия могут опираться на Концепцию ОЭСР по классификации систем искусственного интеллекта[120]. Концепция определяет, что модель искусственного интеллекта – это вычислительное представление всей внешней среды системы искусственного интеллекта или ее части, охватывающее, например, процессы, объекты, идеи, людей и/или взаимодействия, которые происходят в этой среде. Модели искусственного интеллекта используют данные и/или экспертные знания, предоставляемые людьми и/или автоматизированными инструментами, для представления, описания и взаимодействия с реальной или виртуальной средой. Основные характеристики включают технический тип, способ построения модели (с использованием экспертных знаний, машинного обучения или того и другого) и способ использования модели (для каких целей и с использованием каких показателей эффективности).

Определение модели ИИ важен для государственной политики, поскольку ключевые свойства моделей ИИ – степень прозрачности и/или объяснимости, надежность и последствия для прав человека, неприкосновенности частной жизни и справедливости – зависит от типа модели, а также от процессов построения модели и логического вывода. Например, системы, использующие нейронные сети, часто рассматриваются как потенциально способные обеспечить сравнительно более высокую точность, но менее объяснимые, чем системы других

[120] https://www.oecd.org/publications/oecd-framework-for-the-classification-of-ai-systems-cb6d9eca-en.htm

типов. Объяснимость часто связана со сложностью системы; чем сложнее модель, тем труднее ее объяснить. Степень, в которой модель эволюционирует в ответ на данные, имеет отношение к государственной политике и режимам защиты прав потребителей, особенно для систем искусственного интеллекта, которые могут извлекать уроки из итераций и эволюционировать с течением времени. Понимание того, как была разработана и/или поддерживается модель, является еще одним ключевым фактором при распределении ролей и обязанностей в рамках процессов управления рисками. Субъекты искусственного интеллекта в этом измерении включают разработчиков и моделистов, которые создают и используют модели, а также проверяют и валидизируют их.

В связи с этим, важно определить **современное понимание искусственного интеллекта.** Обычно, *Генеративный (созидательный) искусственный интеллект (AI)* на основе машинного обучения использует нейронные сети и другие алгоритмы для создания новых данных или контента, похожих на исходные данные. Этот подход отличается от дескриптивного AI, который анализирует и классифицирует данные, но не создает новых данных. Генеративный AI может иметь огромное значение для различных отраслей, таких как медиа, искусство, развлечения, реклама и образование. Однако, он также может вызывать определенные угрозы в связи с нарушением авторских прав, распространением ложной или дискриминационной информации и потери контроля над созданным контентом.

Дескриптивный искусственный интеллект (AI) на основе машинного обучения используется для анализа, классификации и предсказания на основе необработанных данных и определяет структуру, зависимости и тенденции данных, не создавая новых данных. Дескриптивный AI может быть использован для различных целей, таких как: (a) Классификация, т.е. разделение данных на группы на основе их характеристик или признаков (классификация электрокардиограмм (ЭКГ) на нормальные и аномальные, диагностика заболеваний и др.); (б) регрессия, т.е. предсказание неизвестных значений на основе известных данных (прогноз погоды, биржевых котировок и др.); (c) кластеризация, т.е. разделение данных на группы на основе схожести между элементами (моделирование бизнес-процессов и др.); (d) анализ тенденций, т.е. определение тенденций и зависимостей в данных для получения информации о будущих событиях или изменениях. Дескриптивный AI является основой для многих современных технологий, таких как рекомендательные системы, системами автоматической обработки звука и изображений, системами контроля качества и системами управления рисками. Хотя дескриптивный AI не создает новых данных, он может предоставить важную информацию и знания, которые могут быть использованы для принятия решений, планирования и стратегического планирования.

Системы генеративного искусственного интеллекта (ИИ) создают новый контент в ответ на запросы, основанные на их обучающих данных. Недавний рост и распространение систем генеративного искусственного интеллекта высветили возможности искусственного интеллекта, включая, например, ChatGPT и BARD для текста; Midjourney и Stable Diffusion для изображений; WaveNet и DeepVoice для аудио; Make-A-Video и Synthesia для видео; и мультимодельные системы, объединяющие несколько типов медиа, языковые модели ИИ. Генеративный искусственный интеллект (ИИ) создает новый контент в ответ на запросы, предлагая преобразующий потенциал во многих секторах, таких как образование, развлечения, здравоохранение и научные исследования. Однако эти технологии также создают критические социальные и политические проблемы: потенциальные изменения на рынках труда, неопределенность в отношении прав интеллектуальной собственности; риск, связанный с возможностью злоупотреблений при создании дезинформации и манипулируемого контента, распространением ложной информации (*deep fake*).

В итоге могут формироваться негативные социальные, политические и экономические последствия, включая дезинформацию по ключевым научным вопросам, создание стереотипов и дискриминации, искажение общественного дискурса, создание и распространение теорий заговора и другой дезинформации, влияние на политические выборы, искажение рынков и даже подстрекательство к насилию. Это, тем не менее, не отрицает преобразующую природу

генеративного ИИ и значимости международные дискуссии о стремлении к инклюзивному и заслуживающему доверия ИИ[121].

В настоящее время особое внимание приковано в генеративному ИИ. Генеративный искусственный интеллект – это тип искусственного интеллекта, который может создавать новый контент и идеи, включая разговоры, истории, изображения, видео и музыку. Как и любой искусственный интеллект, генеративный ИИ основан на моделях машинного обучения – очень больших моделях, предварительно обученных на огромных объемах данных и обычно называемых базовыми моделями (FM). Базовые модели (FM), обученные работе с огромными наборами данных, представляют собой крупные нейронные сети с глубоким обучением, которые изменили подход специалистов по работе с данными к машинному обучению (ML). Вместо того чтобы разрабатывать искусственный интеллект с нуля, специалисты по работе с данными используют базовую модель в качестве отправной точки для разработки моделей ML, позволяющих быстрее и экономичнее поддерживать новые сферы применения.

Термин *«базовая модель»* был придуман исследователями для описания моделей ML, обученных на широком спектре обобщенных и немаркированных данных и способных выполнять широкий спектр общих задач, таких как понимание языка, генерирование текста и изображений и общение на естественном языке. Технологии искусственного интеллекта пытаются имитировать человеческий интеллект в таких нетрадиционных вычислительных задачах, как распознавание изображений, обработка естественного языка (NLP) и перевод. Генеративный искусственный интеллект – это следующий шаг в разработке искусственного интеллекта[122].

Генеративный ИИ быстро вошел в общественный дискурс. Стремительный прогресс в области генеративного искусственного интеллекта обусловлен его ожидаемым потенциалом для повышения производительности, поощрение инноваций и предпринимательства и поиск решений глобальных проблем, а также в решении социальных проблем, таких как улучшение здравоохранения и помощь в разрешении климатического кризиса и достижении Целей устойчивого развития (ЦУР).

Литература

1. Ващекин А.Н., Ващекина И.В. Искусственный интеллект в судебной системе: задачи и методы // Правовая информатика. 2023. № 3. С. 65-74.
2. Гаврилов Д.А. Нормативно-технические вопросы разработки безопасных автоматизированных интеллектуальных систем // Вопросы кибербезопасности. 2020. № 6 (40). С. 63-71.
3. Гарбук С.В. Задачи нормативно-технического регулирования интеллектуальных систем информационной безопасности // Вопросы кибербезопасности. 2021. № 3 (43). С. 68-83.
4. Карцхия А.А. Искусственный интеллект как средство управления в условиях глобальных рисков // Мониторинг правоприменения. 2020. № 1 (34). С. 45-50.
5. Карцхия А.А. Новые элементы национальной безопасности: национальный и международный аспект // Вопросы кибербезопасности. 2020. № 6 (40). С. 72-82.
6. Карцхия А.А., Макаренко Г.И., Сергин М.Ю. Современные тренды киберугроз и трансформация понятия кибербезопасности в условиях цифровизации системы права // Вопросы кибербезопасности. 2019. № 3 (31). С. 18-23.
7. Карцхия А.А., Макаренко Д.Г. Правовые аспекты статуса и рисков искусственного интеллекта. В сборнике: «Безопасные информационные технологии». Сборник трудов Десятой международной научно-технической конференции. М.: МГТУ им. Н.Э.Баумана, 2019. С. 167-171.
8. Кибербезопасность цифровой индустрии. Теория и практика функциональной устойчивости к кибератакам / Под ред. Зегжда Д.П. и др. М.: Горячая линия, 2021. 560 с

[121] Initial Policy Considerations for Generative Artificial Intelligence, OECD Artificial Intelligence Papers, September, 2023. http://www.oecd.org/termsandconditions

[122] Initial Policy Considerations for Generative Artificial Intelligence, OECD Artificial Intelligence Papers, September, 2023. http://www.oecd.org/termsandconditions

9. Марков А.С. Актуальные вопросы оценки соответствия интеллектуальных средств защиты информации. Материалы трудов Конгресса «Русский инженер» (Москва, 30 октября - 3 ноября 2023). М.: МГТУ им. Н.Э.Баумана, 2023.

10. Степанов О.А. Правовое регулирование отношений в сфере безопасного функционирования и развития систем искусственного интеллекта: доктринальные аспекты // Правовая информатика. 2019. № 1. С. 56-63.

11. Хуноян А.С. Моделирование применения технологии искусственного интеллекта в судебной системе // Правовая информатика. 2022. № 4. С. 76-86.

12. Чечкин А.В. Элементы искусственного интеллекта умных систем // Правовая информатика. 2022. № 1. С. 15-23.

13. S. Klaus, C. Jung. Legal Aspects of «Artificial Intelligence» (AI) // Information and Communication Technology Newsletter, 2019, N10. URL: www.swlegal.com/media/filer_public/ce/e4/cee498cc-910d-4af8-a020-5b4063662b35/sw_newsletter_october_i_english.pdf

Legal Perspectives of Artificial Intelligence Technologies

Kartskhia A.A.[123], Makarenko G.I.[124], Makarenko D.G.[125]

Abstract. The accelerated spread of artificial intelligence technologies puts a number of right-wing issues on the agenda. This paper attempts to address the risks associated with the misuse of opportunities offered by artificial intelligence that may arise from potential intentional misuse or unintentional control issues of advanced AI, with cybersecurity, biotechnology, and disinformation risks of particular concern.

Keywords: cyberattacks, security, control, risks, privacy threats, key principles, increased accountability.

[123] Alexander A. Kartskhia, Dr.Sc.(Law), Professor, Gubkin Russian State University of Oil and Gas, Moscow. E-mail: arhz50@mail.ru

[124] Grigory I. Makarenko, Senior Researcher, National Center for Strategic Studies under the Ministry of Justice of the Russian Federation, Moscow, E-mail: t7920518@yandex.com

[125] Dmitry G. Makarenko, Expert of the Federal Institute for Certification and Evaluation of Intellectual Property and Business, Moscow. E-mail: d.g.makarenko@gmail.com

УДК 681.3.06 (075.32)

Человеко-машинный интерфейс для прогнозирования и рационального управления рисками в системной инженерии

Нистратов А.А.[126]

Перспективная системная инженерия охватывает широкий спектр областей функционального применения систем, ориентирована на компьютерные системы, становящиеся более интеллектуальными. Учитывая это, в работе рассмотрены вопросы разработки человеко-машинного интерфейса для поддержки прикладных решений, ориентированных на прогнозирование и рациональное управление рисками в жизненном цикле систем. В качестве рассматриваемых систем могут выступать: органы управления, информационная инфраструктура (учитывающая инженерную, транспортную, энергетическую, коммуникационную инфраструктуры), компьютеризированные машины и механизмы, процессы и пр. Примерами типовых задач, подлежащих решению, являются: прогнозирование рисков; обоснование допустимых рисков; выявление существенных угроз; обоснованию мер, направленных на достижение целей и противодействие угрозам; определение сбалансированных решений при средне- и долгосрочном планировании; обоснование предложений по совершенствованию и развитию систем. Приведен вариант предлагаемого человеко-машинный интерфейс для прогнозирования и рационального управления рисками.

Ключевые слова: интерфейс, риск, система, системная инженерия, управление

Введение

Под системной инженерией согласно ISO/IEC/IEEE 15288 (в России ГОСТ Р 57193) понимается сосредоточение междисциплинарных научно-технических и организационных усилий, требуемых для преобразования ряда потребностей заинтересованных сторон, ожиданий и ограничений в прикладные решения и для поддержки этих решений в жизненном цикле системы. Система определена как комбинация взаимодействующих элементов, упорядоченная для достижения одной или нескольких поставленных целей. В свою очередь под риском понимается сочетание вероятности нанесения ущерба и тяжести этого ущерба.

Подразумеваются сложные системы, создаваемые человеком для любой области приложений: в интересах органов государственной власти и корпораций, энергетических, финансово-экономических, страховых и промышленных структур (включая отдельные предприятия, строительные, нефтегазовые и транспортные комплексы, объекты опасного производства), предприятия авиационно-космической отрасли, служб по чрезвычайным ситуациям, жилищно-коммунального хозяйства и др. Системы должны создаваться с использованием эффективных инструментариев, реализующих инновации для поддержания необходимой конкурентоспособности. В настоящей работе предлагается человеко-машинный интерфейс, ориентированный на прогнозирование и рациональное управление рисками с использованием авторских моделей [1-12], доведенных до реализации в стандартах системной инженерии ГОСТ Р 59329 – ГОСТ Р 59357, охватывающих защиту информации в системных процессах.

Предлагаемый человеко-машинный интерфейс

Предлагаемый вариант логического представления определенных системных интересов высшего мета-уровня для решения задач системной инженерии представлен на рис. 1. В общем случае для достижения конкретных целей системы с учетом разнородных угроз, различных ограничений и условий решению подлежат задачи, связанные с анализом рисков. Исходя из этого на рис. 2 предлагается логическое представление системы для построения программно-

[126] Нистратов Андрей Андреевич, к.т.н., Федеральный исследовательский центр «Информатика и управление» Российской академии наук, Москва, e-mail: andrey.nistratov.job@yandex.ru

технологических инструментариев, ориентированных на достижение ожидаемых прагматических эффектов.

Рис. 1. Предлагаемый вариант логического представления определенных системных интересов высшего мета-уровня

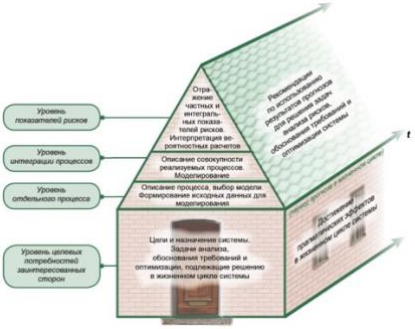


Рис. 2. Логическое представление системы для построения программно-технологических инструментариев, ориентированных на достижение эффектов

В качестве исходных данных для моделирования может выступать не только статистика, но и данные, формируемые в режиме реального времени, например, в системе дистанционного контроля промышленной безопасности (для чего используются дополнительные специальные средства обработки телеметрической информации) – по ГОСТ Р 58494. Вариант предлагаемого человеко-машинного интерфейса применительно к структуре сложной системы (на примере технологической схемы обогатительной фабрики) представлен на рис. 3.

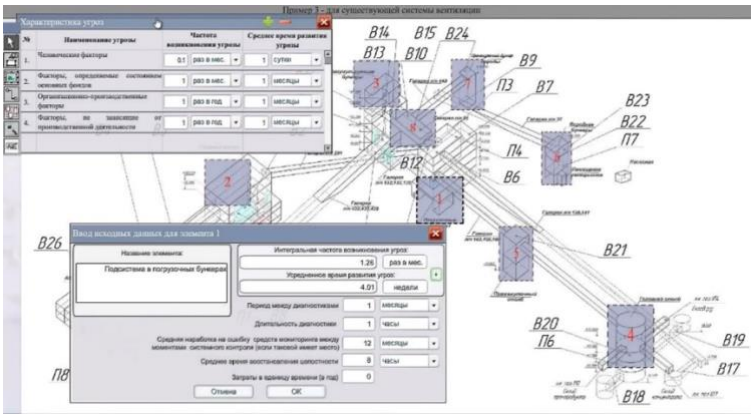


Рис. 3. Вариант предлагаемого человеко-машинного интерфейса

Нумерация в архитектурном представлении означает номер подсистемы в формальной структуре моделируемой системе для последовательно-параллельного объединения. При прогнозировании рисков в терминах функций распределения используются элементы логики «И», «ИЛИ». Значения о состоянии анализируемых объектов могут быть взяты из статистики, а также могут поступать от систем дистанционного контроля, автоматизированных систем управления, датчиков, сенсоров. В итоге моделирования осуществляется прогнозирование рисков, связанных с критичными сущностями рассматриваемой системы в терминах вероятности «успеха» и/или риска «неудачи». Получаемые рекомендации предназначены для использования лицами, принимающими решение, в целях выработки упреждающих мер противодействия угрозам и достижения прагматических эффектов. Предложенный человеко-машинный интерфейс на формальном уровне способен охватить системы любой области приложения. Их применение обеспечивает аналитическую прослеживаемость интегрального и частных рисков от влияющих факторов. Это предоставляет возможности для поиска эффективных решений в системной инженерии с использованием непрерывного аналитического прогнозирования рисков и обоснования способов их снижения или удержания в допустимых пределах [3, 4].

Заключение

Учитывая перспективы развития системной инженерии в условиях разнородных неопределенностей для систем различного функционального назначения в настоящей работе предложены:

- вариант логического представления определенных системных интересов высшего мета-уровня для решения задач системной инженерии с применением методов прогнозирования и управления рисками;
- логическое представление системы для построения программно-технологических инструментариев, ориентированных на достижение прагматических эффектов;
- человеко-машинный интерфейс применительно к структуре сложной системы для моделирования с привязкой к фотографии, скану или иному изображению бумажного документа.

Охватывая системы любой области приложения, предложенные решения обладают аналитической новизной, за счет чего их применение обеспечивает прослеживаемость прогнозных рисков от влияющих факторов. Это предоставляет возможности для поиска эффективных решений в системной инженерии.

Выводы

Предложенный человеко-машинный интерфейс применим для любого рода систем согласно ГОСТ Р 58494, ГОСТ Р 59329–ГОСТ Р 59357 и ориентирован на:

- прогнозирование рисков, связанных с критичными сущностями рассматриваемой системы в терминах вероятности «успеха» и/или риска «неудачи»;
- определение существенных угроз и условий, способных при любом развитии событий в жизненном цикле негативно повлиять на безопасность системы;
- обоснование упреждающих мер противодействия угрозам и условий, обеспечивающих желаемые свойства системы при задаваемых ограничениях в задаваемый период прогноза;
- обоснование предложений по обеспечению и повышению качества и безопасности системы.

Литература

1. Костогрызов А.И., Степанов П.В. Инновационное управление качеством и рисками в жизненном цикле систем – М.: Изд.”Вооружение, политика, конверсия”, 2008. – 404 с.
2. Kostogryzov A., Nistratov G., Nistratov A. Some Applicable Methods to Analyze and Optimize System Processes in Quality Management. Total Quality Management and Six Sigma, InTech, 2012, pp. 127-196, http://www.intechopen.com/books/total-quality-management-and-six-sigma/some-applicable-methods-to-analyze-and-optimize-system-processes-in-quality-management
3. V. Artemyev, A. Kostogryzov, Ju. Rudenko, O. Kurpatov, G. Nistratov, A. Nistratov. Probabilistic methods of estimating the mean residual time before the next parameters abnormalities for monitored critical systems. Proceedings of the 2nd International Conference on System Reliability and Safety (ICSRS), Milan, Italy, December 20-22, 2017, pp. 368-373.
4. V. Kershenbaum, L. Grigoriev, P. Kanygin and A. Nistratov. Probabilistic modeling in system engineering. Probabilistic modeling processes for oil and gas systems. IntechOpen, 2018, P. 55-79. http://dx.doi.org/10.5772/intechopen.74963
5. Probabilistic modeling in system engineering. / By ed. Kostogryzov A. InTechOpen, 2018, - 279p.
6. Kostogryzov A., Grigoriev L., Golovin S., Nistratov A., Nistratov G., Klimov S. (2018). Probabilistic Modeling of Robotic and Automated Systems Operating in Cosmic Space. Proceedings of the International Conference on Communication, Network and Artificial Intelligence (CNAI), Beijing, China. DEStech Publications, Inc., 298-303.
7. A. Kostogryzov and V. Korolev, Probabilistic Methods for Cognitive Solving of Some Problems in Artificial Intelligence Systems. Probability, Combinatorics and Control, InTechOpen, 2020. DOI: http://dx.doi.org/10.5772/intechopen.89168
8. Нистратов А.А. Аналитическое прогнозирование интегрального риска нарушения приемлемого выполнения совокупности стандартных процессов в жизненном цикле систем высокой доступности. Часть 1. Математические модели и методы // Системы высокой доступности. 2021. Т.17 №3, с. 16-31,

9. Нистратов А.А. Аналитическое прогнозирование интегрального риска нарушения приемлемого выполнения совокупности стандартных процессов в жизненном цикле систем высокой доступности. Часть 2. Математические модели и методы // Системы высокой доступности. 2022. Т.18 №2, с. 42-57.

10. Костогрызов А.И. О моделях и методах вероятностного анализа защиты информации в стандартизованных процессах системной инженерии // Вопросы кибербезопасности. 2022, №6 (52), с.71-82.

11. Нистратов А.А. О математических, программно-технологических и методических решениях, ориентированных на рациональное управление рисками в системной инженерии. Сборник материалов Всероссийской научно-практической конференции «Россия в XXI веке в условиях глобальных вызовов: проблемы управления рисками и обеспечения безопасности социально-экономических и социально--политических систем и природно-техногенных комплексов», 26-27.04.2022, Президиум РАН. Под общ. ред. Проф. Я.Д. Вишнякова. – М.: Государственный университет управления. 2022. С. 251-255

12. Kostogryzov A., Makhutov N., Nistratov A., Reznikov G. Probabilistic predictive modeling for complex system risk assessments. Time Series Analysis - New Insights. IntechOpen, 2023, pp.73-105. http://mts.intechopen.com/articles/show/title/probabilistic-predictive-modelling-for-complex-system-risk-assessments

About probabilistic methods of system engineering

Nistratov Andrey[127]

Abstract. Advanced system engineering covers a wide range of areas of system functional application, is focused on computer systems that are becoming more intelligent. Taking this into account, the paper considers the issues of developing a human-machine interface to support application solutions focused on prediction and rational risk management in the life cycle of systems. The systems under consideration can be: management bodies, information infrastructure (taking into account engineering, transport, energy, communication infrastructure), computerized machines and mechanisms, processes, etc. Examples of typical tasks to be solved are: risk prediction; rationale of acceptable risks; identification of significant threats; rationale of measures aimed at achieving goals and countering threats; determination of balanced solutions for medium- and long-term planning; justification of proposals for improving and developing systems.

Keywords. Interface, modeling, risk, system.

[127] Andrey A. Nistratov, PhD, Senior Researcher, Federal Research Center "Informatics and Control" of the Russian Academy of Sciences. Moscow, Russia. E-mail: andrey.nistratov.job@yandex.ru

УДК 004.056

К вопросу о способах дешифрования классических шифров

Марков Я.А.[128]

Аннотация. Работа посвящена исследованию стойкости классических шифров. Рассмотрены три способа взлома шифра Цезаря. Показаны ограничения частотного анализа при дешифровании фраз. Сделан вывод об эффективности эвристического способа дешифрования с помощью часто используемых фраз.

Ключевые слова: криптоанализ, шифр Цезаря, взлом, дешифрование

Введение

Особенность работы состоит в том, что в ней исследуются не вопросы шифрования и расшифрования классических шифров, а вопросы их криптостойкости (дешифрования). В качества объекта исследования рассмотрен обобщенный шифр Цезаря [1-4]. Несмотря на известность шифра Цезаря, вопросы его исследования в литературе представлены лаконично. Например, в elibrary.ru было найдено 23 научные публикации, которые касались исследования классических шифров[129]. Однако большинство публикаций предоставляют только краткую аннотацию без текста исследования, поэтому невозможно оценить, что в реальности в них сделано. Полные тексты научных работ приведены только в [6-13]. Так, в работе [6] представлено описание программы шифрования Цезаря для MS Excel 2019. В [7, 8] представлены программа и схема шифрования по методу Цезаря исключительно для латиницы. В [9-11] прорекламированы лишь экранные формы обучающих программ по шифрованию и расшифрованию. В [12] представлена лишь блок-схема алгоритма шифрования. В [13] представлена программа (на алгоритмическом языке) полного перебора для шифра Цезаря. Указанное послужило причиной провести собственное исследование.

Суть метода Цезаря

Как известно, Цезарь использовал сдвиг на три символа на латинице (рис. 1), а обобщенный алгоритм допускает различные алфавиты и сдвиги.

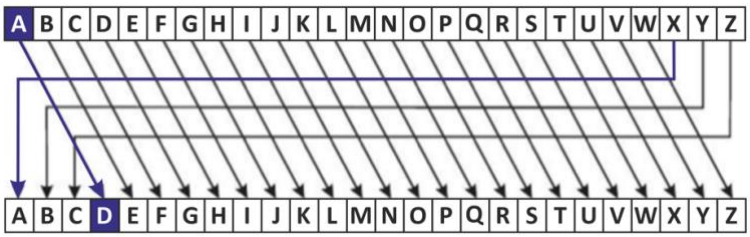


Рис.1. Демонстрация шифра Цезаря

Несмотря на античность, подход Цезаря до сих пор востребован. В музее криптографии представлены экспозиции его использования для коротких сообщений американскими шпионами, многие вычислительные системы его используют для скрытия кода, например, устройства CISCO и др. Шифр Цезаря широко используется при обучении во многих предметах, например, в логике, кибернетике, информационной безопасности, информатике.

Методы дешифрования

В литературе описаны несколько методов дешифрования [3, 4]. В работе исследовано три, а именно:

- прямой перебор (brute force attack);
- дешифрование по известной фразе;
- частотный анализ.

[128] Марков Ярослав Алексеевич, НИЯУ МИФИ, предуниверситарий, Москва, cyberbugz@yandex.ru

[129] https://www.elibrary.ru/keyword_items.asp?id=9844820

1. Прямой перебор является самым простым, но самым длительным. Суть его состоит в переборе всевозможных ключей, в данном случае сдвигов. Считается, что эффективность любых других способов дешифрования (взлома) оценивается относительно эффективности прямого перебора.

2. Дешифрование по известной фразе упрощает ручной анализ прямого перебора, облегчая жизнь криптоаналитика. Такой способ имеет исторические корни, например, описаны способы взлома, если предполагали, что в зашифрованном тексте есть известная фраза, например, приветствие или обращение. Наиболее известна методика взлома немецких шифров времен II мировой войны - «Eins-алгоритм». Данный алгоритм предложил математик Алан Тьюринг, заметив, что в немецких шифровках наиболее часть используется немецкое слово один (eins).

3. Считается, что частотный анализ позволяет дешифровать любой классически шифр[130]. Суть частотного анализа состоит в том, что собирается статистика по использованию букв алфавита, а при дешифровании символы зашифрованного текста заменяются в соответствии с частотой их использования. К примеру, в интернет доступны словари частотности русских букв[131] (рис. 2) и других символов[132]. В интернет представлено интересное исследование метода частотного анализа на сайте www.habr.com [5], выполненное в сравнении с информацией, данной в Википедии[133], однако и в нем есть недостатки (учтены лишь буквы русского языка, не рассмотрен способ использования частотного анализа при переборе - не был просчитан пробел).

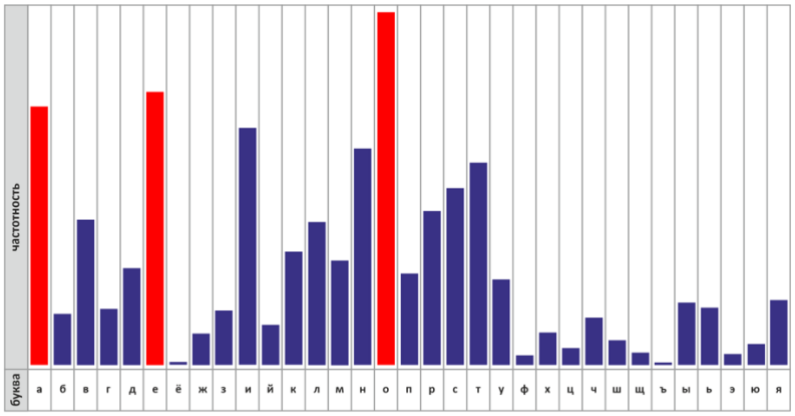


Рис. 2. Статистика русских букв согласно исследованию

Практическая реализация

В рамках исследования были написаны программы на языке Python 3 (платформы PyCharm, IDLE). Программы можно посмотреть на авторском сайте по QR-коду (рис. 3).

Рис. 3. QR-коды для шифрования, расшифрования и дешифрования

[130] Метод упоминается в книгах Конан Дойля и Жюль Верна для расшифровки различной тайнописи.
[131] https://ru.wikipedia.org/wiki/Частотность
[132] https://www.bckelk.org.uk/words/etaoin.html
[133] https://ru.wikipedia.org/wiki/Частотный_анализ

Исследование методов дешифрования

Проведенный эксперимент показал следующее:

1. Прямой перебор взламывает шифр Цезаря, а объем перебора зависит от длины алфавита.

2. В работе был предложен оригинальный вариант взлома по часто используемым фразам. В программе использовались следующие подстроки: «привет», «здравст», «пока», «задал», «задани», «пиши», «досвид» «до свид», «домаш», «контрольн», «шифр», «qwerty», «1234», «пароль», «roblox», «cs2», «counter», «strike», «terraria». Выбор указанных подстрок был определен анализом школьного чата. Это значит, что под любой чат надо формировать набор подстрок, используемый сообществом.

3. Эксперимент с частотным анализом показал, что короткие фразы затруднительно расшифровать частотным анализом. Например, если расшифровывать всю переписку, то вероятность расшифровки существенно повышается. Однако противостоять этому можно, меняя (по заранее заданным правилам) ключ. В процессе исследования было выявлен существенный недостаток частотного анализа для смешанного текста (в данном случае сочетание русского и английского языка), когда буквы имеют одинаковое написание (Aa-Аа, Bb-Вв, Cc-Сс, Ee-Ее, Kk-Кк, Mm-Мм и др.).

Еще очень важный момент, который был впервые обнаружен в данном исследовании, - это то, что в литературе обычно приводят статистику только по буквам, однако для малых текстов самым используемым (как показал эксперимент) является символ пробел! Данное исследование привело к выводу, что частотный анализ для шифра Цезаря использовать следует иначе, чем представлено в литературе, а именно как средство уменьшения прямого перебора, когда достаточно угадать один символ, а по нему провести сдвиг!

Заключение

В работе были разработаны программы по дешифрованию шифра Цезаря тремя способами. При этом вариант интеллектуального (эвристического) дешифрования с использованием подобранных часто используемых фраз исследован впервые.

В рамках исследования были сделаны следующие выводы:

1. Было подтверждено, что шифр Цезаря взламывается путем прямого перебора. Сложность взлома зависит от размера алфавита.

2. Предложенный в работе интеллектуальный (эвристический) способ дешифрования по известным фразам повышает скорость дешифрования. Эффективность метода зависит от правильности подобранных подстрок, таких как: приветствия, имена, типовые запросы в комьюнити и пр.

3. Несмотря на то, что частотный метод считается универсальным для взлома классических шифров, эксперимент показал, что частотный анализ малоэффективен при дешифровании небольших сообщений. В то же время впервые предложен вариант повышения эффективного частотного анализа шифров, основанных на сдвиге, например, путем угадывания пробела.

Список литературы

1. Математические основы информационной безопасности / Басараб М.А., Булатов В.В., Булдакова Т.И. и др.; Под. ред. В.А.Матвеева. М.: НИИ РиЛТ МГТУ им. Н.Э.Баумана, 2013. 244 с.
2. Орлов, В. А. Теория чисел в криптографии. / В. А. Орлов, Н. В. Медведев, Н. А. Шимко, А. Б. Домрачева - М.: МГТУ им. Н.Э. Баумана, 2011. - 223 с.
3. Фомичёв, В. М. Криптографические методы защиты информации. Системные и прикладные аспекты. / В. М.Фомичёв, Д. А.Мельников: В 2-х ч. - М.: «ЮРАЙТ», 2019. Ч. 2. 245 с.
4. Свейгарт, Э. Криптография и взлом шифров на Python. / Э. Свейгарт. - М.: «Диалектика», 2020. - 512 с.
5. Wadik69, В. Дешифровка текста методом частотного анализа. / В. Wadik69 // Криптография. Шифрование и криптоанализ, 2020. - [Электронный ресурс]. – Режим доступа: https://habr.com/ru/articles/513926/
6. Михаэлис, В. В. Шифрование в среде MS Excel для безопасной передачи и хранения данных / В. В. Михаэлис, С. И. Михаэлис // Современная наука: актуальные проблемы теории и практики. Серия: Естественные и Технические Науки. - 2023. - №04/2. - С. 99-102. - DOI: 10.37882/2223-2966.2023.04-2.22.
7. Карпенкова, Н. В. Использование модулярной математики в криптографии // Электронный научно-практический журнал Культура и образование. 2015. № 1 (17). -С. 26.
8. Кузьминых, Е. С. Анализ симметричных методов шифрования, проблемы и пути возможного их решения / Е. С. Кузьминых, М. А. Маслова // Научный результат. Информационные технологии. - 2023. - Т. 8. - № 1. - С. 38-45. - DOI: 10.18413/2518-1092-2022-8-1-0-3.
9. Ачекеев, К. С. Создание компьютерной программы для шифрования текстовой информации / К. С. Ачекеев, У. Т. Керимов, А. Б. Салижанов, У. Б. Салижанова // Известия ВУЗов Кыргызстана. - 2022. - № 2. - С. 45-47.
10. Лепшокова, А. Р. Разработка интерактивного приложения для наглядного представления шифра Цезаря / А. Р. Лепшокова // В сборнике: Актуальные проблемы методики обучения информатике и математике в современной школе. Материалы Международной научно-практической интернет-конференции. – М.: МПГУ, 2020. - С. 493-498.
11. Шарейко, В. В. Использование программы с реализацией алгоритмов симметричного шифрования для олимпиадных заданий / В. В. Шарейко // В сборнике: Информационные технологии в образовательном процессе вуза и школы. Материалы XIV Всероссийской научно-практической конференции. – Воронеж: ВГПУ, 2020. - С. 384-388.
12. Адаев, Р. Б. Программная реализация шифрования текстовых фраз / Р. Б. Адаев // Инженерный вестник Дона. 2021. № 11 (83). С. 172-180.
13. Гумерова, Л. З. Взлом шифра Цезаря методом «грубой силы» / Л. З. Гумерова, Г. Н. Аглямзянова, Е. С. Маисеева // В сборнике: Лучшие практики общего и дополнительного образования по естественно-научным и техническим дисциплинам. материалы II Всероссийской научно-практической конференции, посвященной памяти академика РАН К.А. Валиева. – Казань: Казанский (Приволжский) федеральный университет, 2022. - С. 157-163.

Научный руководитель: Троицкий Игорь Иванович, к.т.н., заместитель заведующего кафедрой ИУ8 МГТУ им. Н.Э.Баумана, iitroickiy@mail.ru

On the Question of Decryption Methods of Classical Ciphers

Markov Y.A.

Abstract. The paper is devoted to the study of the strength of classical ciphers. Three methods of decryption of Caesar cipher are considered. The limitations of frequency analysis are shown. It is concluded about the efficiency of heuristic method of decryption with the help of frequently used phrases.

Keywords: cryptanalysis, Caesar cipher, breaking, decryption

СОДЕРЖАНИЕ

Марков А.С. *Современные тенденции безопасных информационных технологий* 5
Арустамян С.С. , Антипов И.С. *Интеллектуальные методы фаззинг-тестирования в рамках цикла безопасной разработки программ* 11
Белгородцев С.К.*Разработка методики эмуляции сетевой активности для анализа вредоносного обеспечения в изолированной среде* 16
Бердюгин А.А. , Ревенков П.В. *Квантовые вычисления и квантовые компьютеры: развитие, проблемы и перспективы* 22
Быков А.Ю., Сысоев В.В. *Модель выбора атрибутов при многофакторной аутентификации на основе игры с нулевой суммой* 29
Васютин Р.Р., Ключарёв П.Г. *Разработка SAT-решателя для криптоанализа алгоритмов симметричного шифрования* 34
Васютина А.П., Ключарёв П.Г. *Оптимизация постквантового криптографического протокола, основанного на изогениях суперсингулярных эллиптических кривых* 40
Гарбук С.В. *Задачи информационной безопасности систем искусственного интеллекта* 44
Гурина Л.А. *Анализ киберугроз для интеллектуальных инверторов, используемых при управлении микросетями* 48
Дорофеев А.В. *Симуляционное обучение специалистов по кибербезопасности в стиле сотрудничества* 52
Еськов Н.В. , Ключарёв П.Г. *Обеспечение конфиденциальности пользователей блокчейн сетей* . 55
Жуков И.Ю. , Муравьев С.К., Комаров Т.И., Чепик Н.А. *Состояние и перспективы развития защищенного встроенного программного обеспечения* 61
Жуков Д.А. *Об одной методике преподавания преобразований Адамара и их приложений* 64
Зеленецкий А.С., Ключарев П.Г. *Постквантовые механизмы инкапсуляции ключа на решетках* 67
Карташова Ж.К. , Медведев Н.В. *Идентификация и аутентификация при обеспечении кибербезопасности гражданского воздушного судна* 72
Козачок А.В. , Ерохина Н.С. *Подходы к повышению эффективности мутаций сложноструктурированных данных при фаззинг-тестировании JavaScript интерпретаторов* 75
Козлов С.В. *Процессные аспекты обеспечения интероперабельности в автоматизированных системах, создаваемых на основе информационных и когнитивных технологий* 80
Корнеев Н.В. *Российская индустрия искусственного интеллекта в решении актуальных проблем информационной безопасности* 89
Костогрызов А.И. *О вероятностных методах системной инженерии* 93
Костогрызов А.И. *Интерпретация вероятностных рисков для анализа упреждающих мер противодействия угрозам в системах с искусственным интеллектом* 98
Лемешко Д.В., Басараб М.А. *Предложение подхода к переходу на модель разграничения доступа на основе атрибутов в информационной системе SAP* 110
Марков Г.А. *Концептуальный подход к разработке сценариев компьютерных атак* 117
Маркова И.Д. *Концептуальные вопросы защиты информации безопасного города* 120
Олифиров А. В., Маковейчук К.А. *Организационно-технические меры информационной безопасности цифровой валюты центрального банка* 124
Петренко А.С. *Методика обеспечения квантовой устойчивости блокчейн в условиях атак с применением квантового компьютера* 130
Ромашкина Н.П. *Спутниковые информационные технологии в период кризиса* 135
Тихонов А.М. *Deception Platform как часть эшелонированной системы защиты* 141
Царегородцев А.В. *Кадры решают всё: назад в будущее* 146
Чепик П.И. *Обезличивание персональных данных как способ повышения их защиты при обработке в информационных системах* 150
Карцхия А.А., Макаренко Г.И., Макаренко Д.Г. *Правовые перспективы технологий искусственного интеллекта* 154
Нистратов А.А. *Человеко-машинный интерфейс для прогнозирования и рационального управления рисками в системной инженерии* 161
Марков Я.А. *К вопросу о способах дешифрования классических шифров* 166

ISBN 978-5-6045553-8-5

Издательство ООО «Мастерская Печати Идей»
Россия, Москва, 129226, ул. Сельскохозяйственная, д. 12а, стр.7.
Тел. (499) 404-64-74
Подписано в печать 29.11.2023 Заказ 215
Формат 60х90.8. Гарнитура Times New Roman
Усл. печ. 29.11.2023 Тираж 100 экз.